Izbrana poglavja iz informatike

izr. prof. dr. Denis Trček

denis.trcek@fri.uni-lj.si

Namen predmeta

- Je osredotočen na e-poslovanje.
- Podaja komplementarna („infrastrukturna“) znanja k temeljnim znanjem s področja e-poslovanja:
  - varovanje informacijskih sistemov;
  - varovanje zasebnosti.
- Pokrivanje tehnoloških in org. vidikov.
- Praktična izvedba znanj pri vajah.
- Tržna uporabnost znanj (svetovalci, skrbniki varnosti, razvijalci, analitiki,...).

Struktura predmeta

- Pregled strukture predavanj:
  - Uvod in osnovne definicije.
  - Standardizacija področja.
  - Varnostni mehanizmi in varnostne storitve.
  - Uvod v formalne metode.
  - Infrastruktura javnih ključev in elementi celovite varnostne infrastrukture.
  - Sistemi za overjanje, avtorizacijo in obračunavanje.
  - Organizacijski vidiki infomracijske varnosti (revizija inf. sistemov).
  - Temeljni zakonski vidiki.

Načrt in namen vaj

- Namen vaj je
  - uporaba in administracija temeljnih rešitev za zagotavljanje varnosti in zasebnosti v informacijskih sistemih;
  - razvoj enostavnih rešitev za omogočanje varovanja in zasebnosti v IS;
  - *integracija znanj in praktična uporabnost pridobljenih znanj za potrebe informacijske varnosti, to je vzpostavitve varnostne politike v organizacijah in / ali revizijo IS*;
  - spodbujanje samoiniciativnosti.

Namen predmeta

- Namen predmeta kot celote je, da na osnovi zadostnega poznavanja ustreznega segmenta informacijskih tehnologij študenta usposobi za
  - obvladovanje organizacijskih vidikov,
  - upoštevanje zakonodajnih elementov ter
  - uporabo revizijskih in akreditacijskih postopkov

  na področju zagotavljanja informacijske varnosti v organizacijah.

Režim pri predmetu

- Tematika predavanj je osnova za izpit.
- Režim pri vajah določi asistent - študent mora pred pristopom k pisnemu izpitu imeti opravljen seminar pri vajah.
- Preizkusi znanj (izpiti):
  - Pisni izpit – vprašanja vključujejo tematike, ki so bile podane na predavanjih.
  - Ustni izpit – javni nastop, predstavitev poljubne tematike s področja predmeta (prosojnice dostopne prek omrežja), dolžina nastopa 7 minut, vprašanje 2 minuti.

Režim pri predmetu

- Strukturo pisnega izpita pogojuje namen le-tega:
  - Preveriti poznavanje temeljnih konceptov in zmožnost samostojnega sklepanja.
  - Spodbuditi povezovanje (integracijo) znanj z drugimi področji.
  - "Vprašanje za najboljše" (občasno).
- Ustni izpit:
  - Spodbuditi samoiniciativnost (samostojno iskanje tematike).
  - Navaditi slušatelja na učinkovito posredovanje sporočila množici (nastop pred avditorijem, časovna omejitev).

Režim pri predmetu

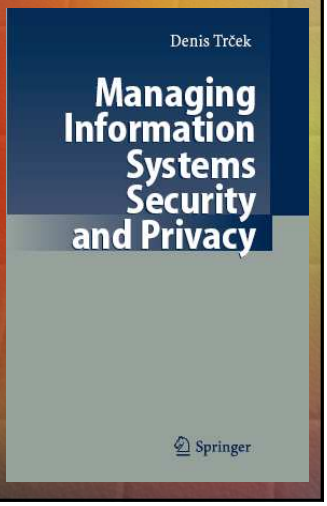
- Preizkusi znanj (izpiti):
  - Glavnino končne ocene doprinese pisni izpit (ustni izipt le v omejenem obsegu).
  - Kolokvijev ni.
- Diplomska dela in magisteriji.
  - Izdelava dispozicije na eno do dveh straneh A4, ki vsebuje izhodišče teme in predvideno delo študenta (format PDF).
  - Izdelava trinivojskega kazala in navedba osnovne literature.
- Govorilne ure.
- Razno (stik s perspektivnimi študenti).

Režim pri predmetu

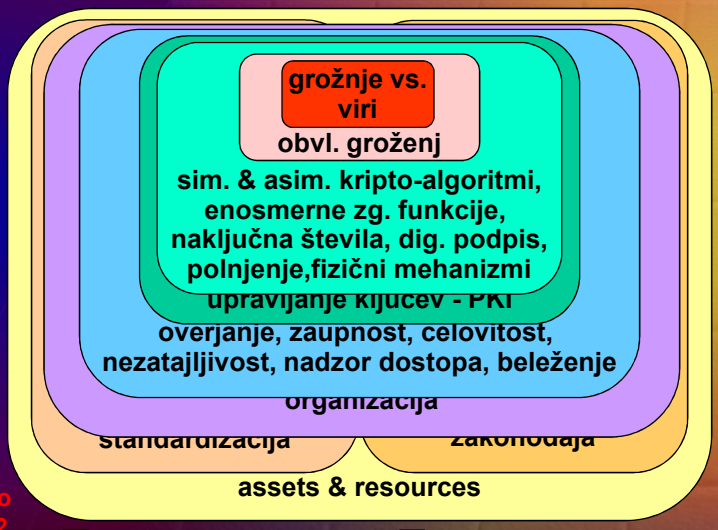
- Področja za možne teme diplomskih, magistrskih in doktorskih del (podano v angleščini za lažje iskanje literature).
  - E-business, security, trust management, privacy, identity management.
  - Bolj specifično opredeljena področja so: services oriented architecutres (SOAs), web services, security protocols design, formal techniques, PKI issues, operational security policies, economics of security, human-factor modelling, embedded and ubiquitous computing, digital forensics.

Literatura

- Temeljna literatura:
  - Trček D., Managing IS Security and Privacy, Springer, Heidelberg / New York, 2006.
  - Kopije prosojnic.
- *Dopolnilna literatura:*
  - *Nakhjiri M., Nakhjiri M., AAA and Network Security for Mobile Access, J. Wiley & Sons, 2005.*
  - *Chandra P., Bulletproof Wireless Security, Elsevier, Amsterdam, 2005.*

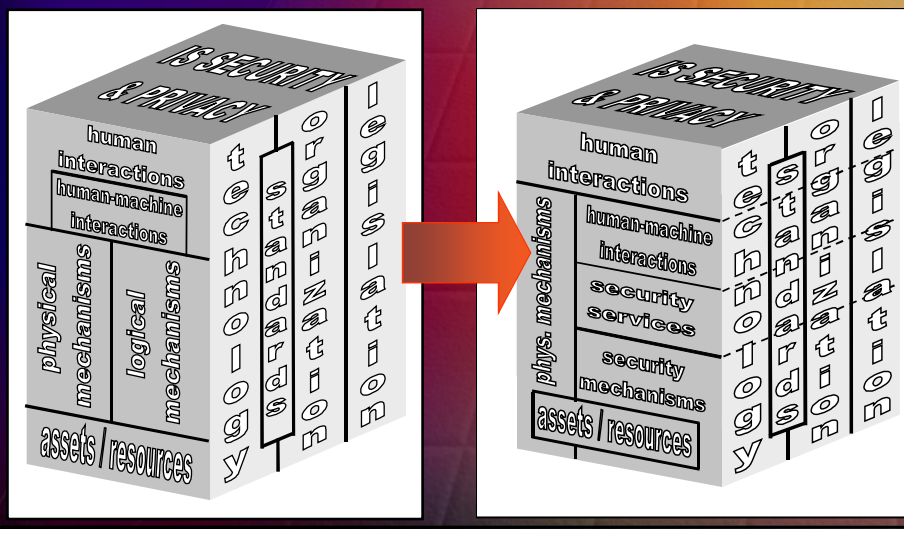


Celovito obvladovanje računalniško-infor. varnosti



povzeto po ISO 7498-2

Obvladovanje varnosti IS - koncepti in modeli

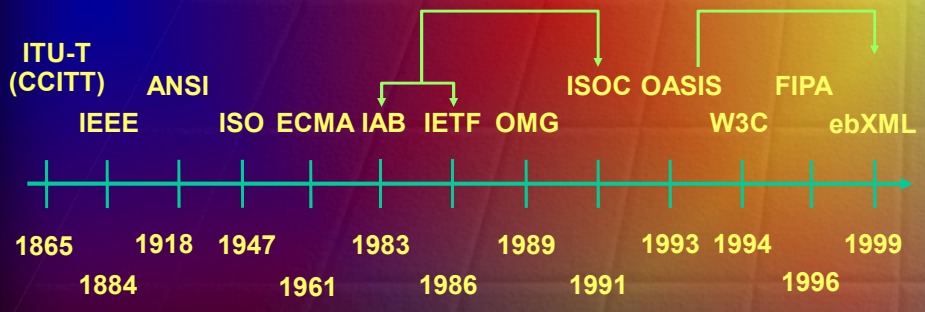


Varnost in standardizacija

- Namen standardizacije.
- Zgodovinski pregled standardizacije.
- Organizacije za standardizacijo.
- *De jure* in *de facto* standardi.
- Relevantnost posameznih organizacij:
  - Četudi ISO standardizira kaj v zvezi z infrastrukturo javnih ključev, ima večinoma IETF prioriteto.
  - Karkoli standardiziramo med transportnim in aplikacijskim slojem, “dejstvo” ostaja SSL.
  - Šibka prisotnost standardov ECMA.
  - Ozko specializirani standardi, npr. FIPA.

Varnost in standardizacija

- Glavna standardizacijska telesa:
  - kronološki pregled in
  - nekatere povezave.



Varnost in standardizacija - pregled organizacij

- ITU-T.
  - Do leta 1956 se je imenovala International Telecommunication Union - ITU, potem se preimenuje v CCITT (Comite Consultatif International Telegraphique et Telepho-nique). Leta 1993 se preimenuje v ITU-T.
  - Standardizira področje telekomunikacij.
  - Spočetka je to pomenilo telegrafijo, nato telefonijo, danes rač. komunikacije, vseskozi pa tudi radijske komunikacije.

Varnost in standardizacija - pregled organizacij

- ITU-T.
  - Ima več vrst članic: države, sektorske članice, (npr. privatne operatorje kot so AT&T, MCI, BT) in druge zainteresirane člane (npr. proizvajalce opreme in raziskovalne organizacije).
  - Priporočila izdelajo študijske skupine, ki se sestoje iz delovnih teles z eksperti.
  - Financiranje s t.i. “contributory units” - CU = 250k $ (velike države plačajo do 30 CU, majhne in revne 1/16 CU).
  - Poznana priporičila: V.24 (RS 232), X.25.

Varnost in standardizacija - pregled organizacij

- ISO.
  - International Standards Organization je bila ustanovljena leta 1946, članstvo je prostovoljno, članice pa so nacionalne organizacije s področja standardizacije.
  - Organizarana je v tehnične komiteje (angl. Technical Committees - TCs), ti pa se naprej členijo v podkomiteje (angl. subcommittees - SCs) in ti v delovne skupine (angl. working groups - WGs).
  - ISO ima ~ 200 TC-jev, od katerih se TC97 ukvarja izključno z računalništvom in s procesiranjem informacij.

Varnost in standardizacija - pregled organizacij

- ISO.
  - ISO sodeluje z ITU-T na področju telekomunikacij in je tudi članica ITU-T.
  - Proces standardizacije:
    - nacionalna organizacija da pobudo;
    - tvori se dolovna skupina, ki napiše t.i. Committee Draft - CD;
    - CD gre v obravnavo za pridobitev komentarjev;
    - ko ga večina članic TC/SC potrdi, postane t.i. Draft International Standard (DIS);
    - DIS zopet kroži za obravnavo in po popravkih gre v okviru TC/SC skozi postopek volitev, da postane standard.

Varnost in standardizacija - pregled organizacij

- ANSI.
  - American National Standards Institute je privatna, nedržavna in neprofitna organizacija.
  - Ustanovljen je l. 1918 s strani petih inženirskih združenj in treh državnih agencij.
  - Članice so proizvajalci, vršilci storitev in druge zainteresirane stranke.
  - Je glavno standardizacijsko telo v ZDA, ima približno 70 zaposlenih in proračun v višini 18 mio USD.

Varnost in standardizacija - pregled organizacij

- NIST.
  - National Institute of Standards and Technology je agencija v okviru US Dept. of Commerce.
  - Skrbi za standarde, ki so obvezni za nabave za delo vladnih služb (izjema je Dept. of Defense).
- IEEE.
  - Institute of Electrical and Electronics Engineers je največja profesionalna organizacija.
  - Pripravlja standarde s področja elektro in računalniške stroke in se neposredno povezuje z ISO, ANSI, ITU-T.

Varnost in standardizacija - pregled organizacij

- IAB.
  - Internet Activities Board (IAB) je bil ustanovljen 1983 z namenom, da določa smernice razvoja Interneta.
  - Sestavljen je bil iz delovnih teles, zadolženih za specifična področja in izdajanje standardov na teh področjih.
  - Leta 1989 nastaneta Internet Research Task Force za delovanje na dolgoročnem razvoju in Internet Engineering Task Force za delovanje na kratkoročnih inženirskih problemih (standardi RFC).
  - IRTF in IETF sta podrejena IAB.

Varnost in standardizacija - pregled organizacij

- IAB - IETF.
  - IETF deluje v delovnih skupinah, ki se ukvarjajo s specifičnimi področji.
  - Delovne skupine so rezultat pobude za rešitev novega tehničnega problema, ki naj bi bil standardiziran.
  - Ko je ideja razdelana, dokumentirana in sprejeta postane to t.i. predlog standarda.
  - Če obstajata vsaj dve delujoči implementaciji, je predlog “povišan” v osnutek standarda (Draft Standard).
  - Če je IAB prepričan v idejo, standard izglasuje kot veljavni standard RFC.

Varnost in standardizacija - pregled organizacij

- ISOC.
  - Internet Society je profesionalno združenje z več kot 150 organizacijami in 16.000 posamezniki iz skoraj 200 držav.
  - ISOC obravnava problematiko, povezano z bodočnostjo Interneta: možnosti dostopa, cenzura, e-poslovanje, avtorske pravice, varnost, zasebnost, javna politika, socialna vprašanja (t.i. digital divide), neželena pošta (angl. spam).
  - Je krovna organizacija za IAB (in IETF).

Varnost in standardizacija - pregled organizacij

- ECMA.
  - European Computer Manufacturing Association je bila ustanovljena 1961 in je sedaj mednarodni konzorcij na področju industrijske standardizacije.
  - Konkretno področje je informacijska in komunikacijska tehnologija ter sistemi.
  - Generalna skupščina rednih članov je vrhovno telo.
  - Operativno delo izvajajo tehnični komiteji in delovne skupine, ki jih nadzira koordinacijski odbor.

Varnost in standardizacija - pregled organizacij

- W3C.
  - WWW Consortium je bil ustanovljen 1994 z namenom razvoja in promocije svetovnega spleta in zagotavljanja njegove interoperabilnosti.
  - Ima okoli 400 organizacij članic.
  - Svetovalni odbor (vrhovno telo W3C) se sestoji iz po enega predstavnika vsake organizacije članice.
  - Predstavniki članic sodelujejo v delovnih skupinah, interesnih in koordinacijsjkih skupinah.

Varnost in standardizacija - pregled organizacij

- W3C.
  - Delovne skupine izdelajo tehnična poročila (del. osnutke), ki so lahko povzdignjena v priporočila (kar pomeni W3C standard).
  - Postopek sprejemanja standarda:
    - objava delovnega osnutka,
    - poziv za pripombe,
    - poziv za implementacije,
    - poziv za popravke,
    - objava (sprejem) priporočila.

Varnost in standardizacija - pregled organizacij

- OMG.
  - Object Management Group je leta 1989 ustanovilo 11 podjetij kot neodvisno in neprofitno organizacijo, ki ima približno 800 članov.
  - OMG ustvarja standarde za softversko industrijo, najbolj znana standarda sta CORBA in UML.
- FIPA.
  - Foundation for Intelligent Physical Agents se ukvarja s standardizacijo inteligentnih agentov in agentnih sistemov.
  - Ima okrog 100 članov iz komercialne in akademske ter raziskovalne domene.
  - Standardizacija poteka v okviru tehničnih komitejev. Ostale dejavnosti se opravljajo v okviru delovnih in interesnih skupin.

Varnost in standardizacija - pregled organizacij

- OASIS.
  - Je neprofitni globalni konzorcij za razvoj, konvergenco in uveljavljanje standardov na področju e-poslovanja (ust. l. 1993).
  - Delo poteka v tehničnih odborih - TO, ki se osnujejo na osnovi predlogov članic.
  - Obstaja poseben TO na področju varnosti, ki se osredotoča zlasti na spletne storitve.
  - TO opravljajo tehnično delo na nevtralen in demokratičen način, ki ne preferira posameznega proizvajalca.
  - Člani so VISA, SAP, Sun, HP, IBM, Microsoft, Oracle...

Varnost in standardizacija - pregled organizacij

- ebXML.
  - To je iniciativa iz leta 1999, ki sta jo spočeli UN/CEFACT in OASIS.
  - Ta iniciativa deluje na področju petnivojskega nabora standardov: za poslovne procese, za ključne komponente, za protokole sodelovanja, za sporočanje in standardov za registracijo / imenike.
  - ebXML je modularen nabor, ki organizacijam omogoča poslovanje prek interneta ne glede na velikost ali geografsko lokacijo.

Zagotavljanje varnosti

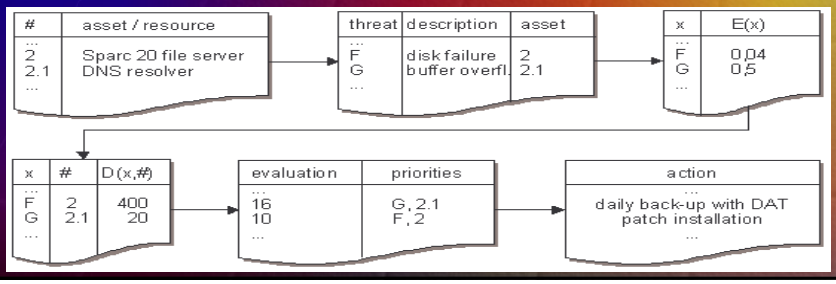
- Problematika varnosti v omrežjih (dinamika rasti, pomen varnosti).
- Definicije varnosti in ranljivosti:
  - Varnost pomeni minimizacijo ranljivosti virov in resursov.
  - Ranljivost pomeni kakršnokoli slabost sistema, ki bi bila lahko izkoriščena proti sistemu samemu ali pa podatkom, ki se na njem nahajajo.
- Problem absolutne varnosti.

Zagotavljanje varnosti

- Primeri (klasičnih) groženj:
  - prisluškovanje,
  - prestrezanje sporočil,
  - zavračanje storitev,
  - napade od znotraj,
  - izogibanje nadzoru dostopa,
  - uporabo stranskih vrat (Trojanski konj),
  - arhitekturno specifične (npr. v WWW), itd.
- Primeri novih groženj:
  - kraja medija (brezžična omrežja),
  - kraja identitete.

Obvladovanje varnosti IS - Tehnike

- Tehnike analize tveganj - kvantit. pristop.
  - Postavljanje prioritet glede na pričakovano škodo:
    - Identifikacija groženj z upoštevanjem motivacije napadalca in človeškega dejavnika.
    - Za vsako grožnjo in vir določi verjetnost učinkovanja E(x) in škodo v primeru realizacije D(x).
    - Določi verjetne stroške D(x)*E(x), postavi prioritete.



Obvladovanje varnosti IS - Tehnike

- Tehnike analize tveganj - kvalit. pristop.
  - Matrike s predefiniranimi vrednostmi - tu določimo vrednostni nivo vsakega vira. Podobno določimo nivoje grožnje, za podnivoje pa ranljivost virov.
  - Oceno grožnje predstavlja ustrezno mesto v matriki.

threat description	level of threat	Low			medium			high		
	vulnerability level	L	M	H	L	M	H	L	M	H
level of asset value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Obvladovanje varnosti IS - Tehnike

- Tehnike analize tveganj - kvalit. pristop.
  - Tabele ocenjenih frekvenc in ocen škode:
    - Najprej določimo pričakovano frekvenco škodnega dogodka.
    - Zatem iz druge tabele preberemo ocenjen nivo škode glede na vrednost sredstva.

level of threat	Low			Medium			High		
vulnerability level	L	M	H	L	M	H	L	M	H
estimated frequency	0	1	2	1	2	3	2	3	4

resource value level / freq. estimation	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Obvladovanje varnosti IS - Tehnike

- Tehnike analize tveganj - kvalit. pristop.
  - Ocena sprejemljivih in nesprejemljivih tveganj (poenostavljena različica predhodne metode) - tu gre le za določitev ločnice med sprejemljivimi in nesprejemljivimi tveganji.

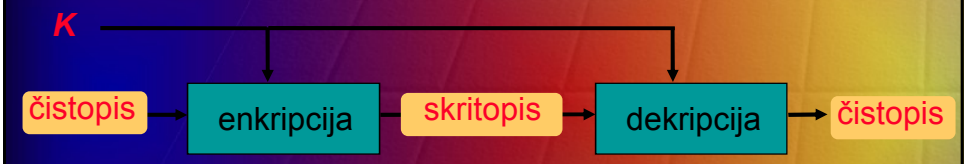
stopnja vrednosti vira	0	1	2	3	4
ocena frekvence					
0	S	S	S	S	S
1	S	S	N	N	N
2	N	N	N	N	N
3	N	N	N	N	N
4	N	N	N	N	N

Zagotavljanje varnosti

- Zagotavljanje varnostnih storitev.
  - Tajnopisni sistemi:
    - simetrični sistemi (DES, IDEA), kjer pošiljatelj in prejemnik uporabljata isti ključ;
    - asimetrični sistemi (RSA, El Gamal), kjer en udeleženec uporablja en ključ za enkripcijo, drugi pa komplementarni ključ za dekripcijo;
    - enosmerne zgoščevalne funkcije, ki predstavljajo neke vrste prstni odtis dokumenta.
  - Večja dolžina ključa načeloma zagotavlja večjo varnost.

Zagotavljanje varnosti

- Model simetričnega sistema (en ključ).



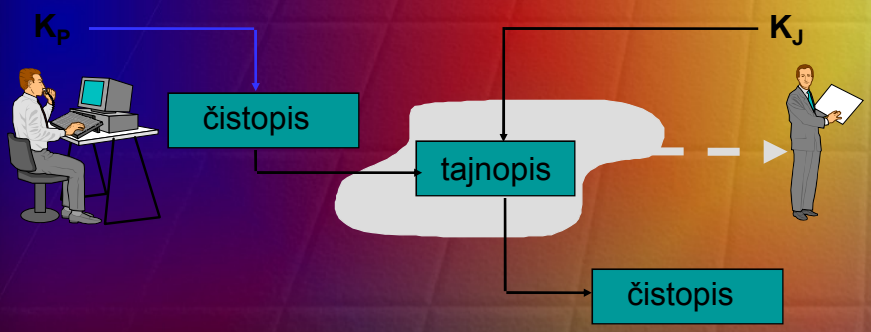
- Model asimetričnega sistema (2 ključa).

Zagotavljanje varnosti

- Simetrični sistemi:
  - relativno procesorsko nezahtevni,
  - število potrebnih ključev narašča s kvadratom števila udeležencev.
- Asimetrični sistemi:
  - procesorsko zahtevni,
  - število potrebnih ključev narašča proporcionalno številu uporabnikov,
  - omogočajo digitalni podpis,
  - zahtevajo uvedbo agencije za certificiranje.

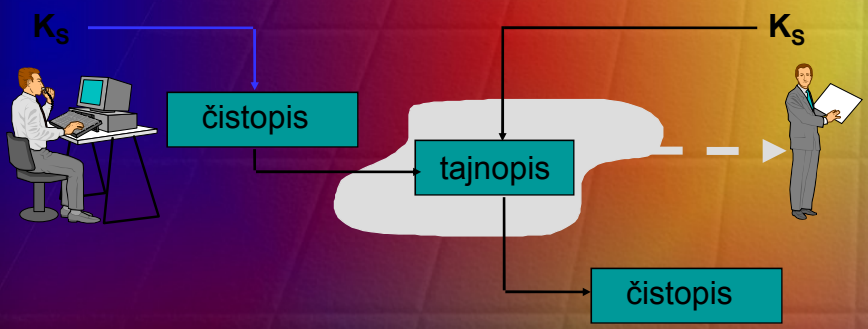
Zagotavljanje varnosti - primeri varnostnih storitev

- Overjanje s pomočjo asim. postopka.



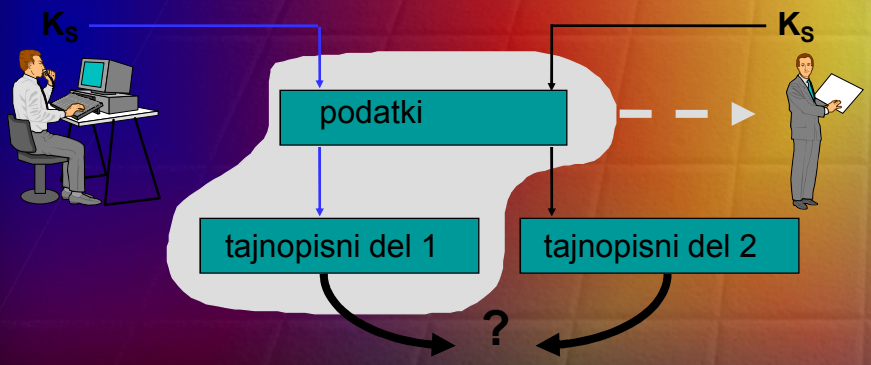
Zagotavljanje varnosti - primeri varnostnih storitev

- Zaupnost s pomočjo sim. postopka.



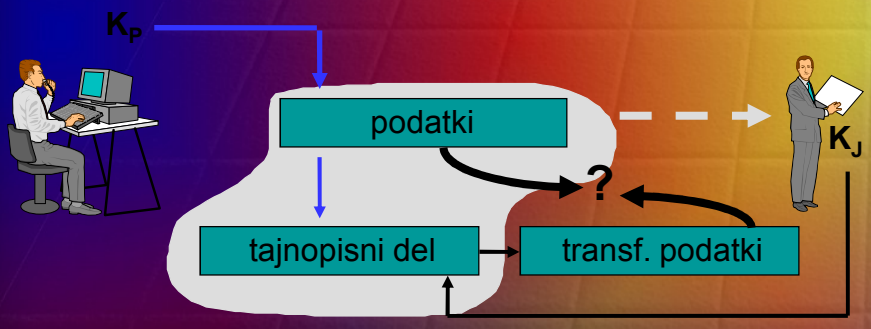
Zagotavljanje varnosti - primeri varnostnih storitev

- Celovitost s pomočjo sim. postopka.



Zagotavljanje varnosti - primeri varnostnih storitev

- Nezatajljivost s pomočjo asimetričnega postopka (digitalnega podpisa).



Zagotavljanje varnosti - temeljni problem

- Relacije med overjanjem, zaupnostjo, celovitostjo in nezatajljivostjo.
  - Katere storitve tvorijo “bazo”, oz. katere so osnova in katere lahko izpeljemo?
    - Izhodišče je overjanje - a če ni celovitosti, overjanja ne more biti.
    - Podobno velja za zaupnost - ta nima pravega smisla brez overjanja.
    - Vendar, ni močnega overjanja (KZOS!) brez predhodne zaupnosti (izmenjava skrivnih ključev za KZOS).
    - Kaj pa nezatajljivost?

Zagotavljanje varnosti - temeljni problem

- Relacije med overjanjem, zaupnostjo, celovitostjo in nezatajljivostjo.
  - Overjanje, zaupnost in celovitost tvorijo sklopljen nabor, ki obstaja sočasno, ali pa ga ni.
  - Sklopljenost na nivoju implementacije, “ortogonalnost” na nivoju definicije:
    - overjanje, zaupnost in celovitost so na nivoju neposredne definicije ločeni med sabo;
    - nezatajljivost ni ločena niti na nivoju definicije.
  - Pomen logičnega ločevanja storitev.

Zagotavljanje varnosti

- Upravljanje ključev je kreiranje, hranjenje, porazdeljevanje in preklicevanje ključev.
- Temeljne razlike med simetrično in asimetrično kriptografijo:
  - rast števila potrebnih ključev glede na število udeležencev;
  - kompleksnost računskih operacij,
  - “trade-off” je osnova za odločitev za posamezno družino .

Zagotavljanje varnosti

- V vsakodnevni uporabi kombinacije obeh vrst šifriranj:
  - asimetrična za izvajanje overjanja (vzpostavitev sej),
  - simetrična za šifriranje velikih množin podatkov (podatkov seje same).
- Temeljni problem upravljanja ključev: *Kako zagotoviti, da določen (javni) ključ res pripada tistemu osebku, ki naj bi mu pripadal?*

Zagotavljanje varnosti

- Kreiranje - simetrični postopki.
  - Tu služi poljuben naključen niz kot ključ.
  - Problem je, da ljudje izberejo ključe, ki so lahko uganljivi:
    - osebne podatke (imena, inicialke, ipd.);
    - besede iz enciklopedij, slovarjev...;
    - variacije zgornjih metod (uporaba velikih in malih črk, zamenjava “O”-ja z “0”, idr...);
    - uporaba besed iz tujih jezikov.
  - Pri nekaterih raziskavah so na podlagi zgornjih principov ugotovili do 60% gesel.
  - Zakaj relacija ključi - gesla?

Zagotavljanje varnosti

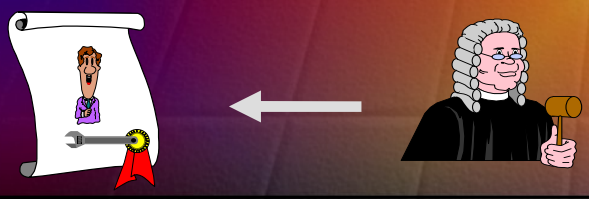
- Kreiranje - simetrični postopki.
  - Naključni nizi (vsak bit ključa mora biti enako verjeten):
    - generator naključnih števil;
    - generator psevdo - naključnih števil;
    - uporaba enosmerne zgoščevalne funkcije in inicialne vrednosti (semena, angl. seed);
    - metanje kovanca.
- Porazdeljevanje - simetrični postopki.
  - Šifriranje šifrirnih ključev.
  - Uporaba paralelnih kanalov.

Zagotavljanje varnosti

- Hranjenje - simetrični postopki:
  - pomnjenje najboljši, a najtežji način;
  - hranjenje s pomočjo elektronskih vezij (t.i. pametnih kartic s PIN-i).
- Preklicevanje:
  - pri centraliziranem porazdeljevanju se obvesti center o izgubi ključa;
  - v primeru komunikacije brez centra je potrebno o tem obvestiti vse udeležence.
- Uničevanje.

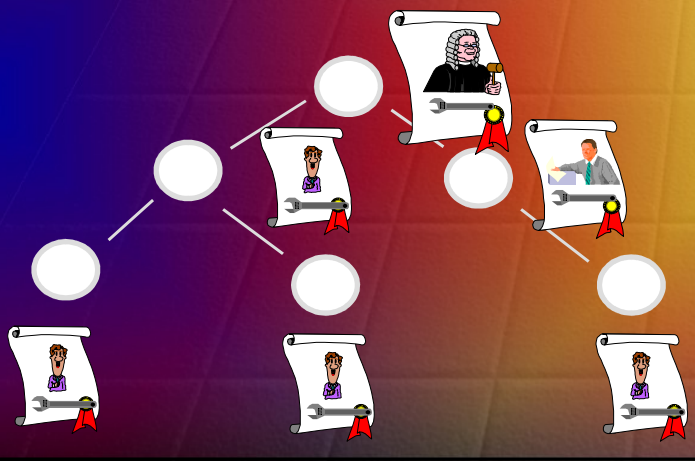
Zagotavljanje varnosti

- Generiranje - asimetrični postopki:
  - podvrženi matematičnim zakonitostim.
- Porazdeljevanje - asimetrični postopki.
  - Postavitev strukture overiteljev (angl. certification authoritites ali CAs) in uvedba overjenih dig. potrdil (angl. certificates).



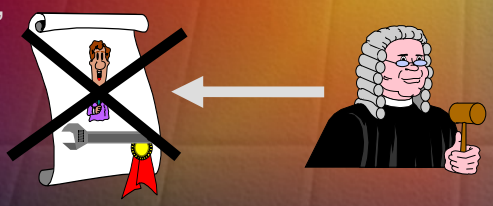
Zagotavljanje varnosti

- Porazdeljevanje - asimetrični postopki.



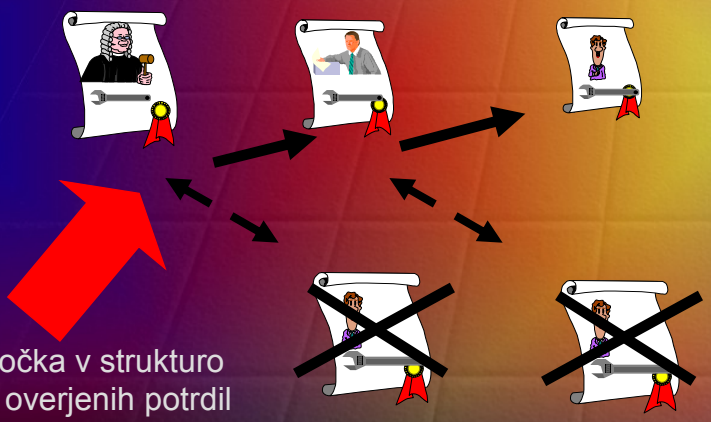
Zagotavljanje varnosti

- Preklicevanje poteka prek seznamov preklicanih potrdil (angl. certificate revocation lists).
- Razlogi za preklicevanje:
  - staranje kriptografskega materiala,
  - skrivni ključ razkrit,
  - zloraba pooblastil.



Zagotavljanje varnosti

- Preverjanje veljavnosti digitalnih potrdil.



vstopna točka v strukturo
digitalnih overjenih potrdil

Upravljanje ključev - overjena digitalna potrdila

- ISO/IEC 9594-8 (ITU-T X.509).

```
Certificate ::= SIGNED { SEQUENCE {
  version [0] Version DEFAULT v1,
  serialNumber CertificateSerialNumber,
  signature AlgorithmIdentifier,
  issuer Name,
  validity Validity,
  subject Name,
  subjectPublicKeyInfo SubjectPublicKeyInfo,
  issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,
  subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,
  extensions [3] Extensions OPTIONAL
Version ::= INTEGER { v1(0), v2(1), v3(2) }
CertificateSerialNumber ::= INTEGER
AlgorithmIdentifier ::= SEQUENCE {
  algorithm ALGORITHM.&id ({SupportedAlgorithms}),
  parameters ALGORITHM.&Type ({SupportedAlgorithms}{ @algorithm}) OPTIONAL }
```

Upravljanje ključev - overjena digitalna potrdila

- ISO/IEC 9594-8 (ITU-T X.509).

```
Validity ::= SEQUENCE {
  notBefore Time,
  notAfter Time }
SubjectPublicKeyInfo ::= SEQUENCE {
  algorithm AlgorithmIdentifier,
  subjectPublicKey BIT STRING }
Time ::= CHOICE {
  utcTime UTCTime,
  generalizedTime GeneralizedTime }
Extensions ::= SEQUENCE OF Extension
Extension ::= SEQUENCE {
  extnId EXTENSION.&id ({ExtensionSet}),
  critical BOOLEAN DEFAULT FALSE,
  extnValue OCTET STRING
ExtensionSet EXTENSION ::= { ... }
```


Upravljanje ključev – infrastruktura javnih ključev

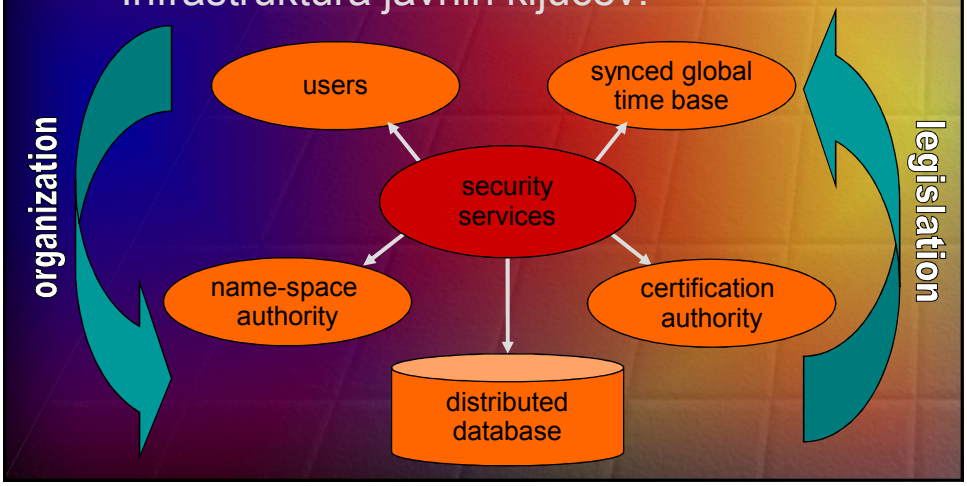
- Relevantni de jure standardi:
  - ITU-T, Public-key and Attribute Certificate Frameworks, Recommendation X.509 v4, Geneva 2001.
  - IETF PKIX Working Group standardi:
    - približno 20 RFC-jev;
    - približno 20 osnutkov;
    - so utemeljeni na certifikatih X.509 (delno tudi iz zgodovinskih razlogov).
- Razširjen de facto standard je PGP.

Upravljanje ključev – infrastruktura javnih ključev

- Varnostne storitve potrebujejo podporo za upravljanje ključev (npr. S/MIME, SSL, IPSec).
- Temeljni problem je zagotoviti, da določen javni ključ v resnici pripada tisti osebi, ki naj bi ji pripadal:
  - digitalna potrdila povežejo identiteto in vlogo entitete z javnim ključem;
  - uvedba digitalnih overjenih potrdil zahteva podporni sistem, imenovan infrastruktura javnih ključev ali IJK (angl. PKI).

Upravljanje ključev – infrastruktura javnih ključev

- Infrastruktura javnih ključev.



Upravljanje ključev – infrastruktura javnih ključev

- IJK - preverjanje digitalnega podpisa:
  - S pomočjo certifikata prejemnik preveri podpis, to je povezanost z identiteto v dokumentu navedene entitete.
  - Prejemnik preveri podpise pripadajočega in vseh drugih ustreznih certifikatov.
  - Prejemnik preveri veljavnost vseh certifikatov.
  - Prejemnik preveri, če je podpisnik avtoriziran za omenjeni podpis.

Upravljanje ključev – IETF PKIX

- Področja IETF PKIX - 5 področij.
  - Tipi (profiles) certifikatov X.509 in seznamov preklicanih certifikatov:
    - opis osnovnih polj in razširitvenih polj;
    - problematika validacije certifikatov;
    - podpora kriptografskih algoritmov.
  - Protokoli za upravljanje (inicializacija, registracija,…):
    - potrebne predpostavke in omejitve;
    - definicija podatkovnih struktur za potrebna sporočila, ter postopkov izmenjave sporočil;
    - definicija funkcij za skladne izvedbe.

Upravljanje ključev – IETF PKIX

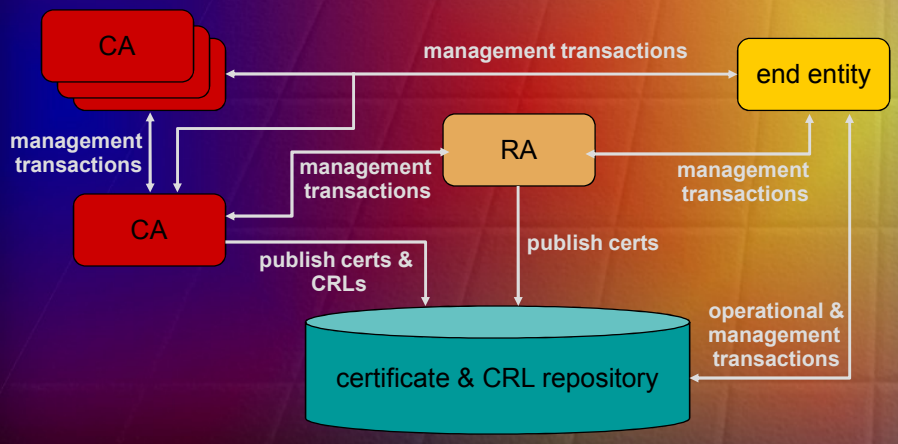
- Področja IETF PKIX - 5 področij.
  - Izvedbeni protokoli - uporaba npr. FTP ali HTTP za podporo PKI.
  - Politike in uporabljane prakse:
    - vzpostaviti povezavo med certifikatom in politiko oz. prakso uporabe le tega (angl. Certificate Policy Statements);
    - zagotoviti elemente, ki omogočajo to povezavo.
  - Časovni žigi in validacija certifikatov:
    - definicija arhitekture zaupanja vredne entitete in kreiranja časovnih žigov;
    - definicija storitev za podporo gornje naloge in za validacijo digitalno podpisanih dokumentov.

Upravljanje ključev – IETF PKIX

- Funkcionalnost PKIX:
  - Registracija, inicializacija, certificiranje, generiranje ključa, rekonstrukcija ključa, ažuriranje ključa, potek veljavnosti ključa, razkritje ključa, križno certificiranje, preklic.
  - Komponente PKI po PKIX:
    - overitelji digitalnih potrdil (angl. CAs),
    - pooblaščene osebe za registracijo, ki preverijo povezavo med ključem in entiteto (angl. RAs);
    - klienti, ki potrdijo podpise;
    - direktoriji za porazdeljevanje certifikatov in seznamov preklicanih certifikatov.

Upravljanje ključev – IETF PKIX

- Funkcionalnost PKIX.



Upravljanje ključev

- IJK in infrastruktura za upravljanje privilegijev - IUP (angl. privilege management infrastructure - PMI).
  - To je komplement IJK za obvladovanje certifikatov atributov (angl. attribute certificates - ACs).
  - Običajni certifikati zagotavljajo povezavo med entiteto in pripadajočim javnim ključem, certifikati atributov pa služijo nadzoru dostopa.

Upravljanje ključev

- IJK in IUP.
  - Certifikati atributov so podobni običajnim, a nudijo večjo fleksibilnost:
    - to so podpisani digitalni dokumenti (certifikati), vendar brez javnega ključa;
    - vsebujejo pomembne atribute, kot so pripadnost skupinam, vloge v sistemu, itd.
  - Gornjih informacij ne damo v certifikat, ker
    - so tipično krajšega roka veljavnosti,
    - in ker sam javni ključ ni neposredno povezan z avtorizacijo.

Upravljanje ključev – časovni žigi

- Časovno žigosanje je del IJK.
- Za razliko od osnovne funkcionalnosti IJK (digitalno podpisovanje dokumentov) časovno žigosanje služi dokazu obstoja dokumenta ob določenem trenutku.
- Protokol za časovno žigosanje je Time Stamp protocol (RFC 3161).
- Pri nas imamo v okviru SIGOV-CA strežnik SI-TSA.

Upravljanje ključev – časovni žigi

- Potek protokola za časovno žigosanje.
  - Entiteta, ki želi dokaz obstoja določenih podatkov (dokumenta) kreira izvleček teh podatkov (dokumenta).
  - Izvleček pošlje strežniku za žigosanje (ta je tipično na voljo kot spletna storitev).
  - Strežnik podpiše izvleček in ga podpisanega vrne pošiljatelju.
- V kakšnem odnosu je časovno žigosanje z digitalnim podpisom?

Upravljanje ključev – IETF OAKLEY

- Opis protokola.
  - OAKLEY je generičen protokol v smislu tega, da nima specificiranih formatov.
  - Je protokol za določitev ključev in je osnovan na protokolu Diffie-Hellman, vendar z odpravljenimi pomanjkljivostmi.
  - Glavne lastnosti:
    - Omogoča pogoditev o parametrih.
    - Uporablja naključne vrednosti za preprečevanje napadov s ponovitvami.
    - Uporablja piškotke za preprečevanje napadov s preobremenitvijo (clogging attacks).
    - Omogoča overjanje za preprečevanje napadov "z napadalcem vmes" (angl. man in the middle).

Upravljanje ključev – IETF OAKLEY

- Opis protokola.
  - OAKLEY je generičen protokol v smislu tega, da nima specificiranih formatov.
  - Je protokol za določitev ključev in je osnovan na protokolu Diffie-Hellman, vendar z odpravljenimi pomanjkljivostmi.
  - Glavne lastnosti:
    - Omogoča pogoditev o parametrih.
    - Uporablja naključne vrednosti za preprečevanje napadov s ponovitvami.
    - Uporablja piškotke za preprečevanje napadov s preobremenitvijo (clogging attacks).
    - Omogoča overjanje za preprečevanje napadov "z napadalcem vmes" (angl. man in the middle).

Upravljanje ključev – IETF OAKLEY

- Podrobnosti protokola:
  - Napad s preobremenitvijo:
    - Napadalec pošlje žrtvi javni ključ z napačnim (izmišljenim) naslovom uporabnika.
    - Napadeni strežnik izračuna skrivni ključ za sejo in ga vrne na gornji naslov - intenzivno ponavljanje te operacije povzroči izrabo virov.
  - Preprečitev z uporabo piškotkov:
    - V inicialnem sporočilu mora biti piškotek, to je naključno število, ki ga druga stran potrdi.
    - To vrednost nato iniciator vključi v sporočilo za generiranje sejnega ključa.
    - Če je posredi napad, bo napadalec brez pravega piškotka. Kaj pa ostale možnosti?

Upravljanje ključev – IETF OAKLEY

- Podrobnosti - uporaba različnih grup.
  - Definicija dveh globalnih parametrov in ID algoritma (za DH):
    - računanje s 768-bitnim modulom:
      $q = 2^{768} - 2^{704} - 1 + 2^{64} * (\lfloor 2^{638} * \pi \rfloor) + 149686$, $\alpha = 2$
    - računanje s 1024-bitnim modulom:
      $q = 2^{1024} - 2^{960} - 1 + 2^{64} * (\lfloor 2^{894} * \pi \rfloor) + 129093$, $\alpha = 2$
    - računanje s 1024-bitnim modulom in prosto določljivimi parametri;
    - grupe na osnovi eliptičnih krivulj nad 2^{155}, generator X=7B, Y=1C8 (hex), in parametra A=0, Y=7338F (hex).
    - grupe na osnovi el. krivulj nad 2^{185}, generator X=18, Y=D (hex), parametra A=0, Y=1EE9.

Upravljanje ključev – IETF OAKLEY

- Podrobnosti protokola - overjanje:
  - Uporaba digitalnih podpisov - vsaka entiteta kriptira zgoščeno vrednost parametrov z lastnim privatnim ključem.
  - Uporaba asimetrične kriptografije - izmenjani parametri so kriptirani s pošiljateljevim privatnim ključem.
  - Uporaba simetričniega tajnopisja - simetrični ključ je posredovan “izven pasu” (angl. out-of-band).

Upravljanje ključev – IETF OAKLEY

- Podrobnosti protokola - primer:
  - Iniciator *A* pošlje piškotek, grupo in svoj javni DH ključ. Iniciator navede sprejemljive algoritme za javno kriptografijo, zgoščevalne funkcije, algoritme za overjanje, vključi identifikatorja *A* in *B*, ter naključno vrednost za ta korak. S privatnim ključem *A* podpiše ID, naključno vrednost, grupo, javni DH ključ in ponujene algoritme.
  - *B* preveri podpis z javnim ključem *A*-ja za podpisovanje. Potrdi prejem, s tem da v odgovoru pošlje *A*-jev piškotek, ID, naključno število in grupo. *B* vključi lasten piškotek, lasten DH ključ, izbrane algoritme, lasten ID in naključno vrednost. *B* podpiše identifikatorja, obe naključni vrednosti, grupo, oba DH ključa in izbrane algoritme.
  - *A* preveri podpis na prejetem sporočilu, kjer naključne vrednosti preprečujejo napada s ponovitvijo. *A* pošlje potrditev, da ima *B* zagotovilo, da je *A* prejel njegov javni ključ.

Upravljanje ključev – IETF OAKLEY

- Podrobnosti protokola - primer:
  - $A \rightarrow B$: CKY_A, *OK_KEYX*, *GRP*, g^x, *EHAO*, *NIDP*, ID_A, ID_B, N_A, $S_{KA}[ID_A \,||\, ID_B \,||\, N_A \,||\, GRP \,||\, g^x \,||\, EHAO]$
  - $B \rightarrow A$: CKY_B, CKY_A, *OK_KEYX*, *GRP*, g^y, *EHAS*, *NIDP*, ID_B, ID_A, N_B, N_A, $S_{KB}[ID_B \,||\, ID_A \,||\, N_B \,||\, N_A \,||\, GRP \,||\, g^y \,||\, g^x \,||\, EHAS]$
  - $A \rightarrow B$: CKY_A, CKY_B, *OK_KEYX*, *GRP*, g^x, *EHAS*, *NIDP*, ID_A, ID_B, N_A, N_B, $S_{KA}[ID_A \,||\, ID_B \,||\, N_A \,||\, N_B \,||\, GRP \,||\, g^x \,||\, g^y \,||\, EHAS]$
  - *CKY* (piškotki), *OK_KEYX* (tip sporočila za izmen. ključev), *GRP* (oznaka DH grupe), *EHAO* / *EHAS* (encryption, hash, authentication functions, offered / selected), g^x / g^y (javna ključa *A* in *B*), *NIDP* (indikator, da je preostanek sporočila nekriptiran), *ID* (identifikatorji), *N* (naključne vrednosti, angl. nonces), $S_K[X]$ (podpis *X* s privatnim ključem $K_{A\,/\,B}$).

Upravljanje ključev – Digitalna ovojnica

- Podrobnosti generičnih principov:
  - *A* izbere naključen sejni ključ *S*.
  - *A* kriptira tekst z *S*: $e_S(tekst)$.
  - *A* kriptira *S* z *B*-jevim javnim ključem E_B: $e_{E_B}(S)$.
  - *A* pošlje *B*-ju $e_S(tekst)$ in *S* kriptiran z javnim ključem *B*-ja: $e_{E_B}(S)$ to *B*.
  - *B* dekriptira sejni ključ s svojim privatnim ključem: $d_{P_B}(e_{E_B}(S))$.
  - *B* dekriptira sporočilo, da dobi čistopis *text*: $d_S(e_S(tekst))$.

Upravljanje ključev – IETF ISAKMP

- ISAKMP določa postopke in formate paketov za upravljanje varnih povezav - VP (angl. security associations, SA).
- Vzpostavitev VP dosežemo z ustrezno koristno vsebino (angl. payload) za izmenjavo podatkov, s katerimi opravimo overjanje in generiramo ključe.
- Formati koristne vsebine so neodvisni od posameznega protokola za izmenjavo ključev, tajnopisnega algoritma ali protokola za overjanje.

Upravljanje ključev – IETF ISAKMP

- Format glave - polja:
  - Piškotek pobudnika (iniciatorja) vzpostavitve, oznanitve ali razdrtja VP.
  - Piškotek partnerja, ki se odzove pobudniku (v prvem sporočilu pobudnika je nastavljen na vrednost *null*).
  - Naslednja koristna vsebina, ki podaja tip prve koristne vsebine v sporočilu.
  - Glavna verzija, ki podaja glavno verzijo trenutno uporabljanega ISAKMP.
  - Podverzija, ki podaja podverzijo trenutno uporabljanega ISAKMP.

Upravljanje ključev – IETF ISAKMP

- Format glave - polja:
  - Tip menjave, ki podaja vrsto menjave.
  - Zastavice, ki podajajo posamezne opcije, npr. bit za enkripcijo je TRUE, če je vsa koristna vsebina kriptirana, bit za jamstvo je TRUE, ko želimo zagotovitev, da se kriptiran material ne vroči pred zaključkom vzpostavitve varnostne povezave.
  - ID sporočila, ki enolično opredeljuje le-to.
  - Dolžina, ki podaja celotno dolžino v B (glava in koristna vsebina).

Upravljanje ključev – IETF ISAKMP

- Glava in gener. glava koristne vsebine.

Upravljanje ključev – IETF ISAKMP

- Vsaka koristna vsebina (angl. payload) se prične z generično glavo:
  - Next payload je postavljen na 0 za zadnjo koristno vsebino sporočila, sicer je nastavljen na tip naslednje koristne vsebine;
  - Payload length polje podaja dolžino dotične koristne vsebine vključno s pripadajočo glavo (podano v oktetih).

ISAKMP - tipi koristne vsebine

- Tipi koristne vsebine.
  - Varnostne povezave (SA):
    - Parametri: domena interpretacije, situacija.
    - Opis: Parametra služita za pogajanje glede varnostnih atributov in opredelitev konteksta, v okviru katerega poteka pogajanje.
  - Predlogi (P):
    - Parametri: zaporedna št., ID protokola, velikost indikatorja varnostnih parametrov, indikator varnostnih parametrov (angl. security parameter indicator - SPI), št. transformov in navedba transformov samih.
    - Opis: Parametri služijo pogajanju pri vzpostavitvi VP, to je, kateri protokoli in transformi bodo uporabljani in koliko jih bo.

oznaka tipa

ISAKMP - tipi koristne vsebine

- Tipi koristne vsebine.
  - Transformi (T):
    - Parametri: ID transforma, atributi varnostne povezave.
    - Opis pomena parametrov: Služijo za pogajanje o varnostni povezavi in pripadajočih transformih (npr. 3DES / ESP ali HMAC-SHA-1 / AH).
  - Koristna vsebina za izmenjavo ključev (angl. key exchange - KE):
    - Parametri: podatki za izmenjavo ključev.
    - Opis pomena parametrov: Podpora različnim tehnikam za izmenjavo ključev, npr. Diffie-Helman.

ISAKMP - tipi koristne vsebine

- Tipi koristne vsebine.
  - Certifikati (CERT):
    - Parametri: vrsta kodiranja certifikata, certifikat.
    - Opis: Služijo prenosu digitalnih overjenih potrdil in drugih relevantnih informacij (kodiranja).
  - Prošnja za certifikat (certificate req.- CR):
    - Parameter: tipi certifikatov in število tipov, sami certifikati, število overiteljev in navedba le-teh.
    - Opis: Služijo temu, da entiteta lahko zaprosi za certifikat, opredeli njihovo število in tip.
  - Podpis (SIG):
    - Parametri: digitalni podpis.
    - Opis: vrednost izračunanega dig. podpisa.

ISAKMP - tipi koristne vsebine

- Tipi koristne vsebine.
  - Identifikacija koristne vsebine (ID):
    - Parametri: identifikatorji vsebin in tipi le-teh.
    - Opis: Služijo izmenjavi potrebnih podatkov za določitev in uporabo identifikatorjev.
  - Zgoščena vrednost (HASH):
    - Parametri: zgoščena vrednost sporočil.
    - Opis: vsebujejo izhod enosmernih zgoščevalnih funkcij, kjer je vhod ustrezno sporočilo.
  - Naključna vrednost (NONCE):
    - Parametri: enkratna naključna vrednost.
    - Opis: vsebuje naključno vrednost.

ISAKMP - tipi koristne vsebine

- Tipi koristne vsebine.
  - Naznanilo (angl. notification - N):
    - Parametri: domena interpretacije (angl. DOI), ID protokola (Protocol-ID), indeks varnostnih parametrov (SPI) in njegova velikost, tip naznanila, sami podatki naznanila.
    - Opis pomena parametrov: Prenos naznanil, npr. pogojev, ob katerih se proglasi napaka.
  - Odstranitev (D):
    - Parametri: DOI, Protocol-ID, število in velikost SPI, ter sami SPI.
    - Opis pomena parametrov: Podaja oz. opredeli tisto varnostno povezavo, ki se razveljavi.

Vrste poteka ISAKMP

- ISAKMP podaja
  - okvir za izmenjavo sporočil,
  - ki je zasnovan okrog koristne vsebine.
  - Osnovna izmenjava - ta omogoča hkratno izmenjavo podatkov za overjanje in ključev.
    - Prvi dve sporočili preneseta piškotka in vzpostavita varnostno povezavo z dogovorjenimi protokoli in transformi, obe entiteti pa uporabljata naključne vrednosti za preprečevanje napadov s ponovitvami.
    - Zadnji dve sporočili preneseta podatke za ključe, identifikatorje uporabnikov, koristno vsebino za overjanje ključev (AUTH), ter naključne vrednosti iz prvih dveh sporočil.

Vrste poteka ISAKMP

- Osnovna izmenjava (angl. basic mode).
  (*A* je pobudnik, *B* je sogovornik):
  - *A*→ *B*: SA; NONCE

  (začni pogajanje za varnostno povezavo)
  - *B* → *A*: SA; NONCE

  (osnovna VP določena)
  - *A* → *B*: KE; ID_A; AUTH

  (ključ na strani B generiran, pobudnik je overjen s strani sogovornika)
  - *B* → *A*: KE; ID_B; AUTH

  (sogovornik overjen s strani pobudnika, ključ pri A je generiran, VP vzpostavljena).

Vrste poteka ISAKMP

- Izmenjava s ščitenjem identitete.
  - Je nadgradnja osnovne izmenjave, kjer dodatno zaščitimo identiteto udeležencev.
  - Prvi dve sporočili vzpostavita varnostno povezavo, drugi dve sporočili služita izmenjavi ključa, kjer je napad s ponovitvami preprečen z naključnimi vrednostmi.
  - Po izračunu sejnega ključa se izmenjajo kriptirana sporočila s podatki za overjanje (npr. digitalnimi podpisi in certifikati).

Vrste poteka ISAKMP

- Izmenjava s ščitenjem identitete.
  - $A \rightarrow B$: SA
  - $B \rightarrow A$: SA
  - $A \rightarrow B$: KE; NONCE
  - $B \rightarrow A$: KE; NONCE
  - $A \rightarrow B$: ID_A; AUTH } kriptirana koristna vsebina
  - $B \rightarrow A$: ID_B; AUTH }
- Informativna izmenjava.
  - Služi le enosmerni izmenjavi podatkov za VP (napaka, razpustitev, status).
    - $A \rightarrow B$: N / D } kriptirana koristna vsebina

Vrste poteka ISAKMP

- Izmenjava, ki omogoča izključno le overjanje.
  - Zagotavlja le overjanje entitet brez izmenjave sejnega ključa.
  - Prvi dve sporočili vzpostavita varnostno povezavo, kjer sogovornik v drugem sporočilu posreduje lasten ID in izvede overjanje nad sporočilom.
  - V tretjem sporočilu pobudnik pošlje lasten ID, ki ga overi. Potek:
    - $A \rightarrow B$: SA; NONCE
    - $B \rightarrow A$: SA; NONCE; ID_B; AUTH
    - $A \rightarrow B$: ID_A; AUTH

Vrste poteka ISAKMP

- Agresivna izmenjava.
  - Minimizira število izmenjav, a ne ščiti identitete.
  - V prvem sporočilu pobudnik predlaga varnostno povezavo (protokole in transforme). Istočasno začne z izmenjavo ključa in posreduje lasten ID.
  - Sogovornik v drugem sporočilu naznani sprejeto varnostno povezavo (protokol in transform), zaključi izmenjavo ključa in opravi overjanje.
  - V tretjem koraku sogovornik pošlje še podatke za overjanje podatkov iz predhodnjega koraka, ki jih kriptira s sejnim ključem.
    - $A \rightarrow B$: SA; KE; NONCE; ID_A
    - $B \rightarrow A$: SA; KE; NONCE; ID_B; AUTH
    - $A \rightarrow B$: AUTH } kriptirana koristna vsebina

IP Sec

- IPSec je standard za varnostno nadgradnjo protokola IP v4 in v6.
- IPSec omogoča varno komunikacijo prek lokalnih in globalnih omrežij.
- Prednosti IPSec:
  - Omogoča overjanje, nepovezavno celovitosti, zaupnosti, nadzor dostopa, delno zaupnost prometa in preprečuje napade s ponovitvami.
  - Je transparenten za običajne uporabnike.
  - Omogoča posamično (selektivno) zaščito.

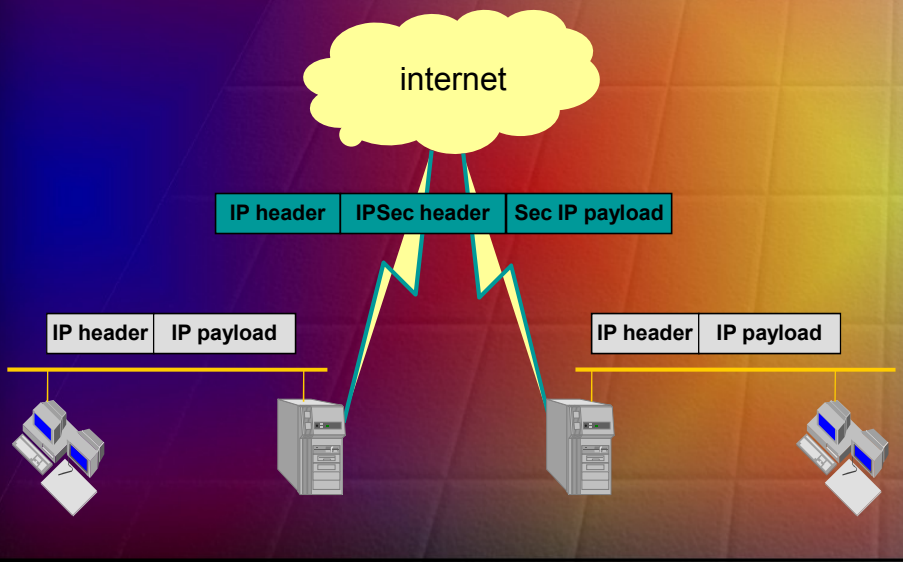
IP Sec

- IPSec - določen je s sedmimi skupinami standardov:
  - Arhitektura: splošni koncepti, varnostne zahteve, definicije, mehanizmi.
  - Authentication Header (AH): format paketa in splošna vprašanja povezana z overjanjem paketa.
  - Encapsulated Security Payload (ESP): format paketa in splošna vprašanja povezana z enkripcijo (in opcijsko z overjanjem).

IP Sec

- IPSec - sedem skupin standardov:
  - Enkripcijski algoritmi: načini uporabe različnih algoritmov za ESP.
  - Algoritmi za overjanje: načini uporabe različnih algoritmov za overjanje AH in ESP (opcijsko).
  - Upravljanje ključev: opis protokolov za upravljanje ključev za tajnopisne mehanizme.
  - Domena interpretacije: opis vrednosti potrebnih za povezave in druge dokumente (identifikatorji algoritmov, operativni parametri).

Tipičen scenarij IPSec



IP Sec

- Varnostna povezava - VP (angl. security association - SA):
  - Je enosm. povezava med pošiljateljem in prejemnikom z določenimi var. storitvami.
  - Obojestranska povezava zahteva dve VP.
  - VP enolično identificirajo trije parametri:
    - SPI (sec. par. index), ki je niz bitov, pridružen povezavi in vključen v glave AH in ESP, da prejemnik določi podrobnosti za procesiranje.
    - IP namembna adresa, kjer so trenutno dovoljena le usmerjena oddajanja (angl. unicast addresses).
    - Identifikator varnostnega protokola: AH ali ESP.

IP Sec

- VP in drugi parametri, ki jo določajo.
  - Sequence Number Counter (SNC) - je 32-bitna vrednost, vnešena v ustrezno polje v glavah AH in ESP.
  - Sequence Counter Overflow - zastavica, ki naznani, če je prišlo do preliva (angl. overflow) pri vrednosti SNC.
  - Anti-Replay Window - služi preprečevanju ponovitev paketov AH / ESP (angl. replay).
  - AH information - določa algoritme, ključe, njihovo življenjsko dobo in druge potrebne parametre za izvedbo AH.

IP Sec

- VP in drugi parametri, ki jo določajo.
  - ESP information - določa algoritem za zaupnost, algoritem za overjanje, ključe, njihovo življenjsko dobo in druge potrebne parametre za protokol ESP.
  - Lifetime of this SA - časovni interval v katerem je dano VP potrebno zaključiti in vzpostaviti novo.
  - IPSec Protocol Mode - načini delovanja, kjer poznamo tuneliranje, transportni način in t.i. wildcard način (angl. wildcard = slo. nadomestni znak).
  - Path MTU - maksimalna velikost paketa, ki ni fragmentiran.

IP Sec

- Selektorji VP (angl. SA Selectors).
  - Za podporo VP rabimo ustrezni podatkovni bazi: bazo varnostnih politik (angl. Security Policy DB - SPD) in varnostnih povezav (angl. Security Association DB - SAD).
  - SPD vsebuje vnose z naslovi IP in kazalci na VP za dotične naslove ter t.i. selektorje.
- Procesiranje izhodnega paketa IP:
  - Primerjaj vrednost selektorja v paketu in poišči ustrezno VP v bazah (če obstaja).
  - Izvedi zahtevano procesiranje paketa (ali ESP ali AH).

IP Sec

- Selektorji VP, ki določajo vnos v SPD:
  - Namembna adresa IP: ta je lahko ena sama, seznam več adres ali nadomestni znak (angl. wildcard) - zadnji služita pož. zidom.
  - Izvorna adresa IP: enako kot zgoraj.
  - UserID: ID uporabnika, ki je posredovan s strani operacijskega sistema.
  - Data Sensitivity Level: opredeljuje varnostni nivo (npr. zaupno, neklasificirano).
  - Protokol transportnega nivoja: oznaka posameznega ali več protokolov, ki so dobljeni iz ustreznih polj glav IPv4 in IPv6.

IP Sec

- Selektorji VP, ki določajo vnos v SPD:
  - IPSec protokol (AH, ESP, AH / ESP): če obstaja, je dobljen iz polja Protocol glave IPv4, oz. polja Next Header glave IPv6.
  - Izvorna in ponorna vrata: številke vrat za protokola TCP in UDP (možne posamezne številke, nizi ali pa nadomestni znak).
  - Razred IPv6: ta vrednost je dobljena iz glave IPv6 in je lahko točno določena vrednost ali pa nadomestni znak.
  - Oznaka (pre)toka IPv6 (angl. Flow Label): vrednost iz ustreznega polja glave IPv6 (je lahko posamična, ali pa nadomestni znak).
  - Vrsta storitve IPv4 (angl. Type of Service): vrednost iz ustreznega polja glave IPv4 (je lahko posamična, ali pa nadomestni znak).

IP Sec

- Transportni in tunelski način (angl. transport and tunnel mode).
  - Tako AH kot ESP podpirata transportni in tunelski način delovanja.
  - Značilnosti transportnega načina:
    - Zagotavlja zaščito predvsem višjenivojskim protokolom (TCP, UDP, ICMP).
    - Služi za povezave “od konca do konca” (angl. end-to-end communication).
    - AH v tem načinu overi celotno koristno vsebino IP, a le del glave IP.
    - ESP v tem načinu kriptira in opcijsko overi koristno vsebino, nič pa glave IP.

IP Sec

- Transportni in tunelski način.
  - Tunelski način:
    - Zagotavlja zaščito celotnega paketa IP.
    - Po dodajanju polj AH ali ESP se cel paket skupaj z varnostnimi polji obravnava kot koristna vsebina nove povezave navzven, zato se doda nova glava IP. Notranji paket je tako za usmerjevalnike nedostopen oz. neviden.
    - Ta novi paket ima lahko od originalnega paketa različne naslove IP (primerno za požarni zid).
    - ESP v tunelskem načinu kriptira (zaupnost!) in opcijsko overi ves tunelirani paket, medtem ko AH overi celoten paket in opcijsko izbrane dele zunanjega paketa.

IP Sec

koda za overitev sporočila

vrednost preverjanja neokrnjenosti

- Overilna glava - OG (angl. authentication header - AH).
  - Podpira overjanje in celovitost paketov IP z uporabo vrednosti MACs in ICV. Polja OG:
    - Next Header - identificira naslednjo glavo.
    - Payload Length - dolžina OG v 32-bitnih besedah, zmanjšana za 2.
    - Reserved - za bodočo uporabo.
    - Security Parameters Index (SPI) - določa VP.
    - Sequence Number - monotono naraščajoča vrednost (števec zaporednih vrednosti).
    - Authentication Data: vsebuje ICV ali MAC za dani paket.

IP Sec

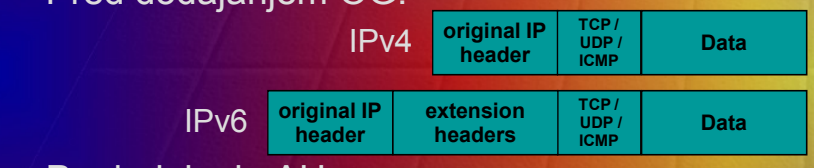
- Overilna glava.

0	8	16	24	31
Next Hdr	Payload Lngth	RESERVED		
Security parameters index / SPI				
Sequence Number				
Authentication Data (variable)				

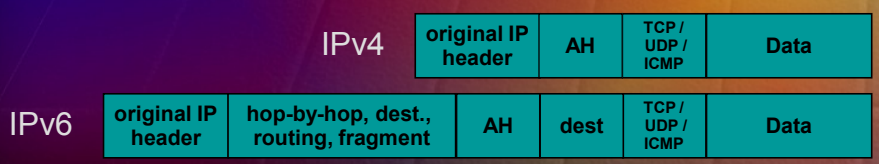
- Monotono rastoče zaporedne številke služijo preprečevanju napadov s ponovitvijo (angl. replay attacks).

IP Sec

- Overilna glava - transportni način.
  - Pred dodajanjem OG:



  - Po dodajanju AH (transportni način, celoten paket je overjen, razen spremenljivih polj).



IP Sec

- Overilna glava - tunelski način.
  - Pred dodajanjem OG:

IPv4

original IP header	TCP	Data

IPv6

original IP header	extension headers	TCP	Data

  - Po dodajanju OG (tunelski način, celoten paket je overjen, razen spremenljivih polj).

IPv4

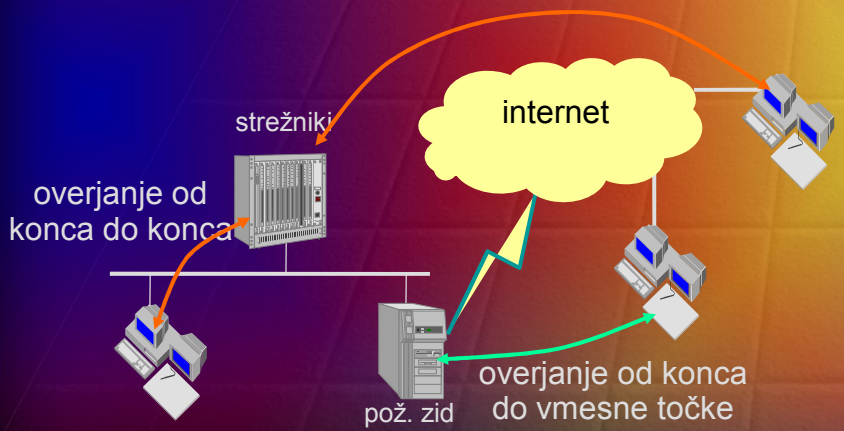
new IP header	AH	original IP header	TCP	Data

IPv6

new IP header	ext headers	AH	orig. IP header	ext headers	TCP	Data

IP Sec scenarij

- OG - transportni in tunelski način.



IP Sec

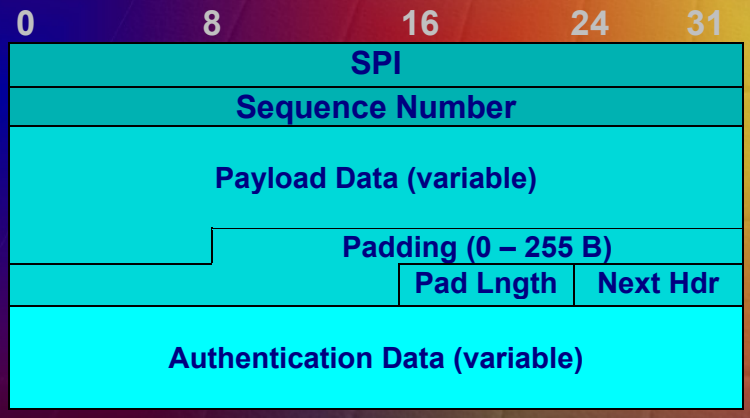
- Varovanje koristne vsebine z inkap-sulacijo (angl. Encapsulating Security Payload - ESP).
  - Ta različica omogoča zaupnost, delno ščitenje nadzora prometa in opcijsko iste storitve overjanja kot OG.
  - Podpira 3DES (s tremi ključi), RC5, IDEA, 3IDEA (s tremi ključi), CAST, Blowfish.
  - Format ESP:
    - SPI - identificira VP.
    - Sequence number – je monotono naraščajoča številka niza za preprečevanje ponovitev.
    - Payload data – je spremenljivo polje, ki vsebuje segment transportnega nivoja pri transportnem načinu, pri tunelskem pa paket IP.

IP Sec

- Varovanje koristne vsebine (angl. payload) z inkapsulacijo (VKSI).
  - Format VKSI:
    - Padding – je polje potrebno za kripto-algoritme.
    - Pad Length – je številno zapolnjevalnih oktetov (angl. pad octets), ki se nahajajo neposredno pred tem poljem.
    - Next Header - določa tip podatkov v polju koristne vsebine tako, da indetificira prvo glavo koristne vsebine.
    - Authentication Data – je polje spremenljive dolžine z ICV, ta pa je izračunan prek paketa ESP brez polja Authentication Data.

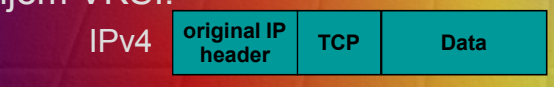
IP Sec

- Struktura paketa VKSI.

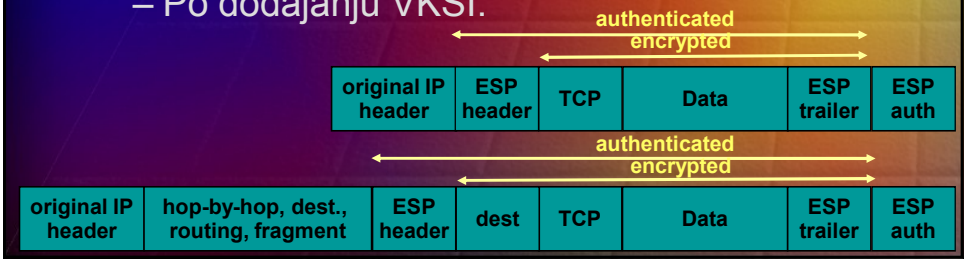


IP Sec

- VKSI - transportni način.
  - Pred dodajanjem VKSI:

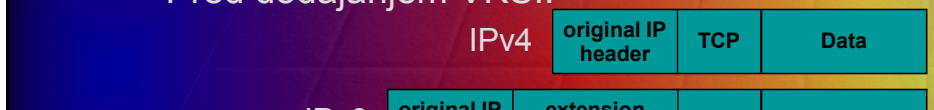


  - Po dodajanju VKSI:

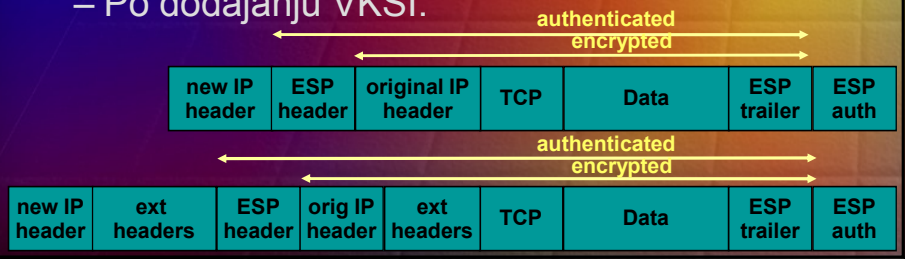


IP Sec

- VKSI - tunelski način.
  - Pred dodajanjem VKSI:



  - Po dodajanju VKSI:



IP Sec

- VKSI - transportni način.
  - Ta način uporabljamo za enkripcijo in opcijsko overjanje podatkov v paketu IP (ki so lahko tipa TCP, UDP ali ICMP).
  - Delovanje:
    - Iz segmenta transportnega sloja tvorimo podatkovni blok, dodamo VKSI zaključek in vse kriptiramo - to nadomesti originalne podatke.
    - Opcijsko dodamo overjanje.
    - Paket pošljemo prek omrežja.
    - Prejemnik procesira glavo IP in njene razširitve - skladno s poljem SPI v glavi dekriptira paket.

IP Sec

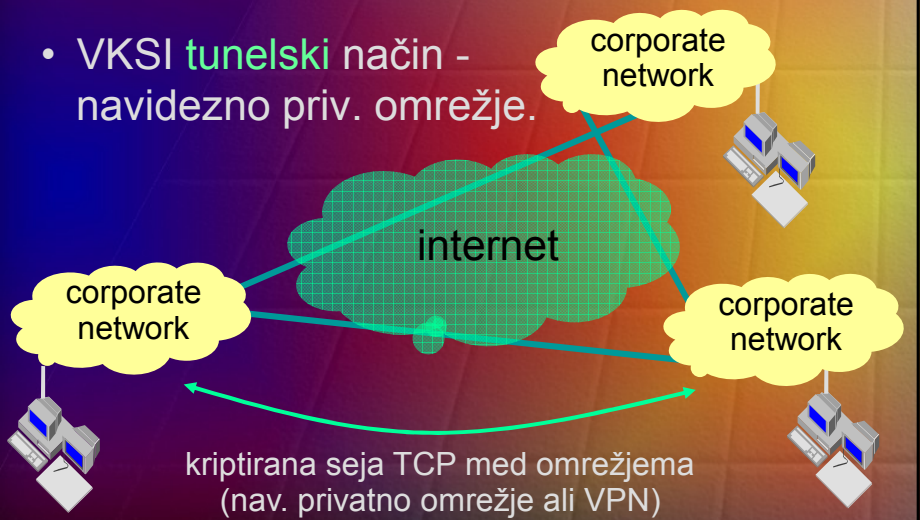
- VKSI - tunelski način.
  - Ta način uporabljamo za kriptiranje celotnega paketa in zagotovitev zaupnosti prometa - zato je potrebna nova glava.
    - Osnovni paket na začetku dopolnimo z VKSI glavo, na koncu pa z VKSI začeljem (angl. trailer). Rezultat inkapsuliramo s pomočjo nove glave IP.
    - Nov paket usmerjamo do požarnega zidu.
    - Požarni zid sprocesira zunanjo glavo in eventuelne razširitve, nato pa na podlagi SPI in VKSI glave opravi dekripcijo ter prvotni paket preda na notranje omrežje.

IP Sec

- VKSI transportni način - komunikacija "od točke do točke".

IP Sec

- VKSI tunelski način - navidezno priv. omrežje.



Standardi za IPSec, Oakley in ISAKMP

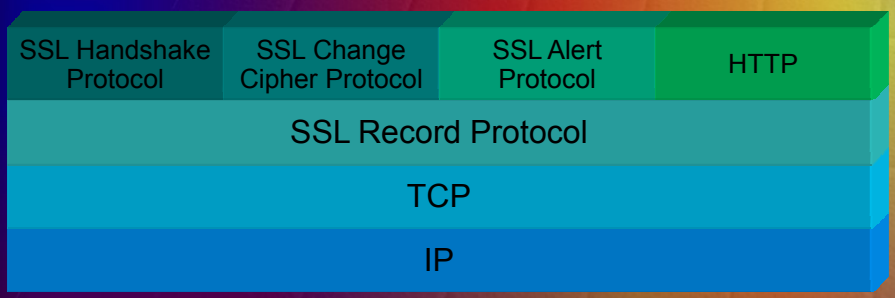
- Standardi Request for Comments (RFCs):
  - Harkins D., Carrel D., The Internet Key Exchange (IKE), RFC 2409, November 1998.
  - Maughan D., Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, IETF, November 1998.
  - Orman H., The OAKLEY Key Determination Protocol, RFC 2412, November 1998.
  - Kent S., Atkinson R., Security Architecture for the Internet Protocol, RFC 2401, November 1998.
  - Kent S., Atkinson R., IP Authentication Header, RFC 2402, November 1998.
  - Kent S., Atkinson R., IP Encapsulating Security Payload (ESP), RFC 2406, November 1998.
  - Drugi podrejeni standardi RFCs.

Sloj varnostnih vtičnic (Secure Sockets Layer - SSL)

- Standard SSL.
  - SSL so razvili pri podjetju Netscape, danes dominira različica št. 3.
  - Je najbolj razširjen (de facto) standard, ki pa je v postopku standardizacije prišel samo do nivoja osnutka standarda.
  - Standardizirani naslednik je Transport Layer Security-TLS, ki je nekako SSL v 3.x.
  - SSL zagotavlja varnost aplikac. sloju.
  - SSL specifikacija vključuje nabor več protokolov: SSL Record Protocol, SSL Handshake, SSL Alert in SSL Change Cipher Spec Protocol.

Sloj varnostnih vtičnic

- SSL in izgled protokolne podatkovne enote ali PPE (angl. Protocol Data Unit).



Sloj varnostnih vtičnic

- Sloj varnostnih vtičnic.
  - Povezava SSL:
    - To je (psevdo)transportna povezava med soležnima osebkoma pridružena eni seji – vsaka povezava pripada eni seji.
  - Seja SSL:
    - To je zveza med strežnikom in odjemalcem.
    - Ta zveza (seja) se vzpostavi s protokolom predstavitve (angl. handshake protocol) in je definirana s kriptografskimi parametri, ki si jih lahko deli tudi z drugimi povezavami.
    - Seje služijo minimizaciji potrebnih pogajanj okrog paramterov, ker to zahteva veliko virov.

Sloj varnostnih vtičnic

- Sloj varnostnih vtičnic.
  - Stanje seje SSL definirajo parametri:
    - Session identifier, ki je poljubno zaporedje oktetov, ki jih določi strežnik.
    - Peer certificate, to je certifikat X.509 v3 soležnega osebka.
    - Compression method, ki določa algoritem stiskanja pred izvajanjem tajnopisja.
    - Cipher spec, ki določa sejno kriptiranje in EZF za izračun KOS.
    - Master secret, ki je 48 B vrednost, ki si jo delita strežnik in odjemalec.
    - ”Is resumable” - zastavica, ki označuje, ali dano sejo lahko uporabimo za zagon nove seje.

Sloj varnostnih vtičnic

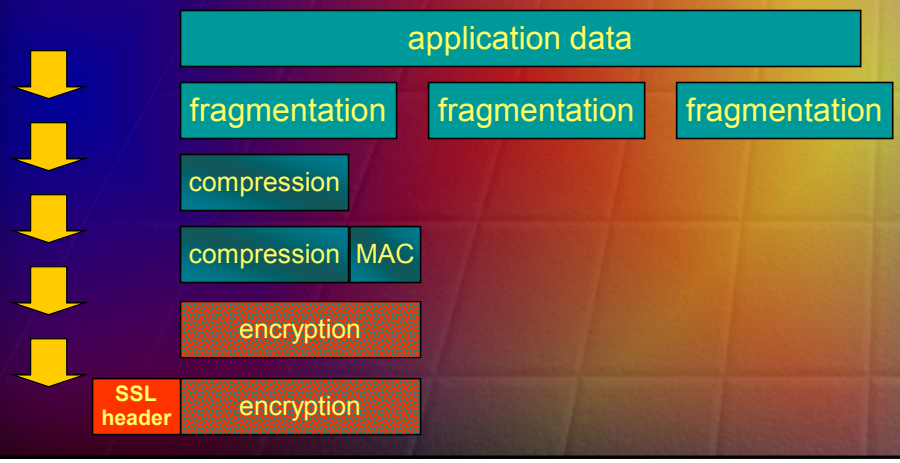
- Sloj varnostnih vtičnic.
  - Stanje povezave SSL definirajo parametri:
    - Server and client random: naklj. zaporedja, ki jih izbereta strežnik in odjemalec za povezavo.
    - Server write MAC secret: skrivni ključ za izračun KOS (MAC), ki ga pošlje strežnik.
    - Client write MAC secret: skrivni ključ za izračun vrednosti KOS, ki ga pošlje odjemalec.
    - Server write key: simetrični ključ, ki ga uporablja strežnik.
    - Client write key: simetrični ključ, ki ga uporablja odjemalec.
    - Inicializacijski vektorji za bločno šifriranje.
    - Številke niza - te so z intervala 0 od 2^{64}-1.

Sloj varnostnih vtičnic

- Protokol SSL Record.
  - Omogoča zaupnost in celovitost.
  - S protokolom predstavitve (angl. handshake protocol) vzpostavi skrivni ključ za zaupnost in skrivni ključ za izračun kode za overovitev sporočil - KOS (angl. MAC).
  - Delovanje protokola: fragmentiranje aplikacijskih podatkov, kompresija podatkov, izračun KOS, enkripcija, dodajanje glave SSL, prenos v segmentu protokola TCP.

Sloj varnostnih vtičnic

- Delovanje protokola SSL Record.



Sloj varnostnih vtičnic

- Podrobnosti protokola SSL Record.
  - Fragmentacija aplikacijskih podatkov tako da imajo po največ 2^{14} oktetov.
  - Kompresija je opcijska, a mora biti brezizgubna ter ne sme povečati dolžine za več kot 1024 B (tovrstna neučinkovitost se pojavlja pri kratkih blokih).
  - Izračun KOS:
    - hash [shared_secret_key || pad2 || hash (shared_secret_key || pad1 || seq_number || compression_type || compressed_length || compressed_fragment)]

Sloj varnostnih vtičnic

- Podrobnosti protokola SSL Record.
  - Podprti simetrični tajnopisni postopki:

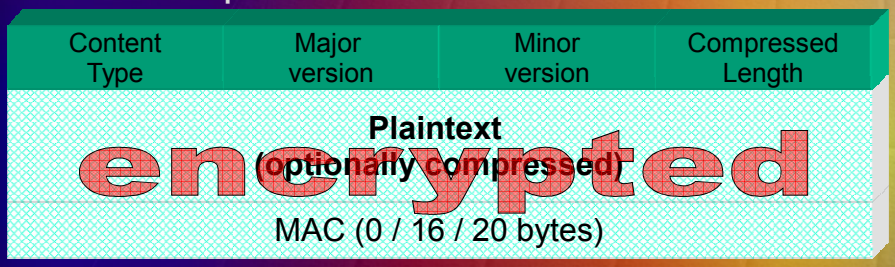
Block cipher		Stream cipher	
algorithm	key size	algorithm	key size
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

Sloj varnostnih vtičnic

- Podrobnosti protokola SSL Record.
  - Dodajanje glave SSL, ki se sestoji iz polj:
    - Content Type - oznaka višjenivojskih protokolov, ki procesirajo dotični fragment.
    - SSLMajor version - indikator glavne različice protokola SSL.
    - SSLMinor version - indikator podrejene različice SSL.
    - Compressed length - v oktetih podana dolžina stisnjenega fragmenta (ali čistopisa, če kompresije nismo uporabili).

Sloj varnostnih vtičnic

- Format protokola SSL Record.



- Change Cipher Spec protokol:
  - To je najenostavnejši protokol v družini SSL, saj le kopira obstoječo povezavo v trenutno aktivno povezavo.
  - Sestoji se iz enega samega sporočila, kjer je ustrezen bit postavljen na vrednost 1.

Sloj varnostnih vtičnic

- Protokol SSL Alert.
  - Služi pošiljanju opozoril soležni entiteti.
  - Opozorila so komprimirana in kriptirana, kot to določa trenutna seja.
  - Vsako sporočilo se sestoji iz 2 B, kjer prvi pomeni “warning” ali “fatal”, drugi oktet pa ga dopolnjuje:
    - Če je prvi “fatal”, se povezavo takoj razpusti.
    - Ostale povezave se lahko nadaljujejo, vendar novih povezav v okviru dane seje ni dovoljeno vzpostaviti.
    - Vrste sporočil “warning”: unexpected_message, bad_record_MAC, decompression_failure, handshake_failure, illegal_parameter.

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Ta protokol omogoča strežniku in odjemalcu obojestransko overjanje in pogajanje glede podrobnosti za izvajanje tajnopisnih postopkov.
  - Ta protokol se, razumljivo (?), odvija pred začetkom same izmenjave podatkov, ki so predmet ščitenja.
  - Format sporočil protokola:

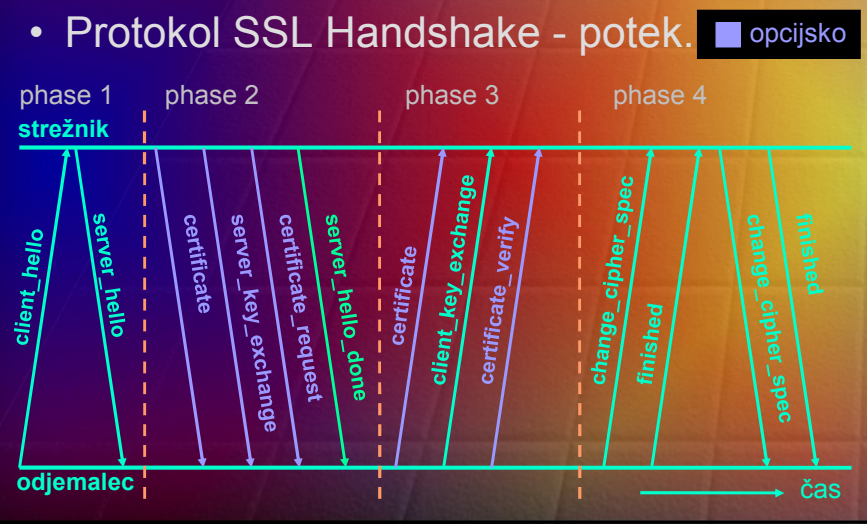
Type (1B)	Length (3)	Content >=0B (parameters)

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Posamezni tipi in pripadajoči parametri:
    - hello_request / null;
    - client_hello / version, random, session id, cipher suite, compression method;
    - server_hello / version, random, session id, cipher suite, compression method;
    - certificate / X.509 v3 certificate chain;
    - server_key_exchange / parameters, signature;
    - certificate_request / type, authorities;
    - server_done / null;
    - certificate_verify / signature;
    - client_key_exchange / parameters, signature;
    - finished / hash value.

Sloj varnostnih vtičnic

- Protokol SSL Handshake - potek.



Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Faza 1: Tu iniciiramo logično povezavo z opredelitvijo varnostnih opcij, ki jih odjemalec pošlje v sporočilu “client_hello”:
    - Version-najvišja različica razumljiva odjemalcu.
    - Random - naključen niz, ki ga generira odjemalec in služi za preprečitev napadov s ponovitvami med izmenjavo ključev.
    - Session ID - vrednost nič naznanja, da želi odjemalec vzpostaviti novo povezavo znotraj nove seje, od nič različna vrednost pa naznanja, da odjemalec želi nove parametre obstoječe povezave ali pa novo povezavo v okviru obstoječe seje.

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Faza 1:
    - Cipher Suite - seznam protokolov za izmenjavo ključev in tajnopisnih postopkov, ki jih podpira odjemalec. Protokoli za izmenjavo ključev so RSA encrypted secret key, fixed DH, ephemeral DH, anonymous DH, Fortezza, tajnopisni postopki pa podajajo tajnopisne algoritme, tipe uporab (tekoča ali bločna), algoritme za KOS, dolžino zgoščenih vrednosti, niz bitov za generiranje sejnih ključev, inicializacijski vektor za enkripcijo CBC.
    - Compression Method: podprte metode za kompresijo.

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Faza 2:
    - Certificate - če je zahtevan (to ni primer pri npr. anonimnem DH), pošlje strežnik certifikat.
    - Server_key_exchange sledi opcijsko v primeru
      - anonimnega DH in vsebuje globalni vrednosti DH skupaj s strežnikovim javnim DH ključem;
      - t.i. “ephemeral” (kratkotrajni) DH, kjer so potrebni parametri (anonimnega DH) digitalno podpisani;
      - izmenjavo s pomočjo RSA, kjer strežnik poseduje privatni ključ le za podpisovanje, zato kreira začasni par ključev RSA, pošlje javni del tega začasnega para in ga podpiše s privatnim ključem za podpisovanje.
      - Fortezza.

signature (hash) includes not only DH / RSA parameters, but also nonces from initial hello messages

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Faza 2:
    - Certificate_request vsebuje dva parametra: *Certificate_type* parameter, ki opredeljuje PK algoritem in njegovo uporabo, npr.
      - RSA (samo za podpis, ali za fiksni DH,…),
      - DSS (samo za podpis, za kratkotrajni DH,..),
      - Fortezza.

      Drugi parameter je certificate_v *Certificate_authorities*, ki vsebuje seznam sprejemljivih CA in pripadajočih certifikatov.
    - Server_done sporočilo označuje zaključek druge faze (zaključi del, ki je bil začet s danim sporočilom server_hello in pripadajočimi sporočili).

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Faza 3: V tej fazi odjemalec preveri strežnikov certifikat in sprejemljivost ponujenih parametrov:
    - Če je strežnik zahteval certifikat, potem se ta faza začne s certifikatom.
    - Nato sledi Client_key_exchange z
      - odjemalčevimi javnimi parametri za anonimni ali kratkotrajni DH;
      - v primeru fiksnega DH so bili parametri posredovani v sporočilu s certifikaton, zato je takrat vsebina tega sporočila prazna;
      - za RSA s t.i. “premaster secret”, ki je kriptirana z strežnikovim javnim (ali začasnim javnim) ključem;
      - parametri za Fortezza algoritem.

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Faza 3: Sporočilo certificate_verify opcijsko pošljemo za eksplicitno preverjanje odjemalčevega certifikata.
    - Sporočilo pošljemo le, če odjemalec zna izračunavati digitalni podpis.
    - To sporočilo vsebuje podpis nad enosmerno zgoščeno vrednostjo, ki je dobljena na podlagi predhodnih sporočil (vključno z zapolnjevalnimi biti), sporočil predstavitve in glavne skrivnosti (angl. master secret).

Sloj varnostnih vtičnic

- Protokol SSL Handshake.
  - Faza 4: ta faza zaključi vzpostavitev varne povezave (v bistvu je to protokol Change CipherSpec).
    - Odjemalec pošlje change_cipher_spec in kopira veljavno CipherSpec v trenutno aktualno CipherSpec vrednost.
    - Odjemalec takoj pošlje sporočilo finished_message dobljeno z novimi algoritmi, ključi in skrivnostmi - s tem sporočilom zagotovimo, da je bilo overjanje in izmenjava ključev uspešna.
    - V odzivu strežnik pošlje lastno sporočilo change_cipher_spec in kopira veljavno CipherSpec v aktualno CipherSpec vrednost.

Sloj varnostnih vtičnic

- Kriptografski izračuni - glavna skrivnost.
  - Glavna skrivnost (48B)-služi za parametre:
    - V primeru RSA odjemalec tvori t.i. “pre-master secret” (PMS), vrednost kriptira s strežnikovim javnim ključem in jo pošlje strežniku.
    - V primeru DH je PMS dobljena enako kot sicer sejni ključ po DH.
    - Iz PMS tvorimo glavno skrivnost, kot sledi:

master_secret = MD5 (PMS || SHA(‘A’|| PMS ||
ClientHello.random || ServerHello.random)) ||
MD5 (PMS || SHA(‘BB’ || PMS ||
ClientHello.random || ServerHello.random)) ||
MD5 (PMS || SHA (‘CCC’ || PMS ||
ClientHello.random || ServerHello.random))

nonces from hello messages

Sloj varnostnih vtičnic

- Kriptografski izračuni.
  - Generiranje kriptografskih parametrov:
    - Skladno s CipherSpecs je potrebno zagotoviti odjemalčev in strežnikov ključ za KOS, odjemalčev in strežnikov ključ za kriptiranje ter odjemalčevo in strežnikovo inic. vrednost IV.
    - Te vrednosti dobimo iz glavne skrivnosti:

key_block = MD5 (MS || SHA(‘A’|| MS ||
ServerHello.random || ClientHello.random)) ||
MD5 (MS || SHA(‘BB’ || MS ||
ServerHello.random || ClientHello.random)) ||
MD5 (MS || SHA (‘CCC’ || MS ||
ServerHello.random || ClinetHello.random)) || ...

tvorimo, dokler ne dobimo dovolj dolgega niza

Varnostne aplikacije - S/MIME

- Običajna e-pošta (SMTP / RFC 822).
  - RFC 822 je najbolj razširjen format, ki je vezan na protokol SMTP (RFC 821).
  - RFC 822 definira format tekstovnih sporočil za e-pošto.
  - Vsako e-pošta po tem standardu tvorita glava in telo, ki sta ločena s prazno vrstico.
  - Glava se sestoji iz vrstic s ključnimi besedami / argumenti, ki so ločeni z dvopičjem.
  - Najpogostejša polja so FROM, TO, SUBJECT, DATE, MESSAGE-ID.

Varnostne aplikacije - S/MIME

- Pomanjkljivosti SMTP/RFC 822.
  - Pošta SMTP je omejena na 7-bitne znake ASCII in zato z njo ni moč prenašati neangleških znakov, programov,...
  - Strežniki SMTP lahko zavrnejo preobsežna sporočila.
  - Strežniki SMTP imajo lahko težave s preslikavami, npr. med ASCII in EBCDIC.
- MIME (RFC 2045 - 2049).
  - Pet dodatnih polj v glavi.
  - Določeni so novi formati vsebine pošte.
  - Določena so nova prenosna kodiranja.

Varnostne aplikacije - S/MIME

- Polja glave pošte MIME.
  - MIME-Version – indikator različice.
  - Content-Type – opis podatkov v telesu pošte.
  - Content-transfer-Encoding – indikator vrste transformacije telesa sporočila.
  - Content-ID – enolično identificira objekte (entitete) MIME v različnih kontekstih.
  - Content-Description – tekstovni opis objekta v telesu (primerno kadar ta ni berljiv, npr. ko so to slikovni podatki).

Varnostne aplikacije - S/MIME

- Tipi vsebin MIME.
  - Tekstovni (angl. text) - vsebuje nize ASCII.
  - Glavni tip “multipart” s sledečimi podtipi:
    - mešani, kjer sta v telesu dva neodvisna in različna dela, ki morata biti vročena v danem vrstnem redu;
    - paralelni, kjer vrstni red vročitve posameznih delov ni določen;
    - alternativni, kjer so isti podatki predstavljeni v več delih telesa;
    - t.i. “digest”, ki je soroden mešanemu, le privzeti tip/podtip sta message/rfc822.

Varnostne aplikacije - S/MIME

- Tipi vsebin MIME.
  - Tip “Message” s podtipi:
    - rfc822, kjer je telo sporočila skladno z RFC 822;
    - delni (angl. partial), ki vsebuje fragmente (dele) večjega sporočila;
    - zunanji (angl. external-body), kjer je v sporočilu kazalec na objekt izven sporočila.
  - Tip “Image” (podtipa jpeg in gif).
  - Tip “Video” (podtip mpeg).
  - Tip “Audio” (podtip “basic”).
  - Tip “Application” (podtipa PS in octet-stream).

Varnostne aplikacije - S/MIME primeri MIME

```
From: Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Date: Sun, 21 Mar 1993 23:56:48 -0800 (PST)
Subject: Sample message
MIME-Version: 1.0
Content-type: multipart/mixed; boundary="simple boundary"

This is the preamble. It is to be ignored, though it is a handy place for
composition agents to include an explanatory note to non-MIME conformant readers.

--simple boundary

This is implicitly typed plain US-ASCII text.
It does NOT end with a linebreak.
--simple boundary
Content-type: text/plain; charset=us-ascii

This is explicitly typed plain US-ASCII text. It DOES end with a linebreak.

--simple boundary--

This is the epilogue.  It is also to be ignored.
```

```
From: Nathaniel Borenstein <nsb@nsb.fv.com>
To: Ned Freed <ned@innosoft.com>
Date: Fri, 07 Oct 1994 16:15:05 -0700 (PDT)
Subject: A multipart example
Content-Type: multipart/mixed;
              boundary=unique-boundary-1

This is the preamble area of a multipart message. Mail readers that understand multipart
format should ignore this preamble.
 If you are reading this text, you might want to consider changing to a mail reader that
understands how to properly display multipart messages.

--unique-boundary-1

... Some text appears here ...

[Blank between the boundary and the start of the text in this part means no header fields
were given and this is text in the US-ASCII character set. It could have been
done with explicit typing as in the next part.]

--unique-boundary-1
Content-type: text/plain; charset=US-ASCII

This could have been part of the previous part, but illustrates explicit versus implicit
typing of body parts.

--unique-boundary-1
Content-Type: multipart/parallel; boundary=unique-boundary-2

--unique-boundary-2
Content-Type: audio/basic

Content-Transfer-Encoding: base64

... base64-encoded 8000 Hz single-channel mu-law-format audio data goes here ...

--unique-boundary-2
Content-Type: image/jpeg
Content-Transfer-Encoding: base64

... base64-encoded image data goes here ...

--unique-boundary-2--

--unique-boundary-1
Content-type: text/enriched

This is <bold><italic>enriched.</italic></bold> <smaller>as defined in RFC 1896</smaller>

--unique-boundary-1
Content-Type: message/rfc822

From: (mailbox in US-ASCII)
To: (address in US-ASCII)
Subject: (subject in US-ASCII)
Content-Type: Text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: Quoted-printable

... Additional text in ISO-8859-1 goes here ...

--unique-boundary-1--
```


Varnostne aplikacije - S/MIME

- Vrste prenosnega kodiranja MIME.
  - 7 bit – podatki so predstavljeni kot kratke vrstice znakov ASCII.
  - 8 bit – podatki so predstavljeni z okteti, kjer je postavljeni bit MSB.
  - binary – podobno kot 8 bitno kodiranje, le da so dovoljene dolge vrstice.
  - quoted-printable – kodirano tako, da je večinoma tekst ASCII.
  - base64 – vhod razdelimo na 6-bitne bloke, za dobljeno vrednost poiščemo v tabeli Radix-64 pripadajoč znak, ki ga kodiramo kot ASCII in dodamo ničlo (MSB).
  - x-token – poljubno nestandardno kodiranje.

Varnostne aplikacije - S/MIME

- Pretvorba (algoritem) Base-64.
  - Izhod je nabor znakov, ki je univerzalno predstavljiv na vseh računalnikih.
  - Preslikovalna tabela se sestoji iz 65 natisljivih znakov, od katerih en znak služi zapolnjevanju (“=“).
  - Izključitev kontrolnih znakov omogoča nemoteno delovanje prenosnih poštnih sistemov (mailers).
  - Tabela Radix-64 vsebuje preslikave za 64 znakov, kar torej zadošča predstavitvi vseh možnih 6-bitnih vhodnih nizov.

Varnostne aplikacije - S/MIME

- Pretvorba Radix-64.

value	encoding	value	encoding	value	encoding	value	encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v	(pad)	=
14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		

The output stream must be represented in lines with max. 76 characters.

Varnostne aplikacije - S/MIME

- Radix-64 - primer pretvorbe.
  - Vhod:
    00100011 01011100 10010001
  - Pregrupiranje bitov vhodnega niza:
    001000 110101 110010 010001
    (8, 53, 50, 17 decimalno)
  - Prevedba s pomočjo tabele radix-64:
    I 1 y R
  - Kodiranje niza I1yR s pomočjo ASCII:
    01001001 00110001 01111001 01010010

Varnostne aplikacije - S/MIME

- Varna pošta MIME (S/MIME).
  - Varnostna nadgradnja MIME, ki omogoča zaupnost, celovitost, nezatajljivost in overjanje.
  - Vrste funkcionalnosti:
    - "enveloped data" - vsebuje kriptirano vsebino in ključe (digitalna ovojnica!);
    - "signed data" - digitalni podpis nad zgoščeno vrednostjo sporočila (podpis in sporočilo sta kodirana base-64);
    - "clear-signed data" - enako kot zgoraj, le da je samo podpis kodiran base-64;
    - "signed & enveloped" – kriptirani podatki so lahko podpisani in obratno (podpisani podatki so lahko kriptirani).

Varnostne aplikacije - S/MIME

- Kriptografski algoritmi za S/MIME.
  - Asimetrična kriptografija:
    - DSS (Digital Signature Standard),
    - El Gamal (to je variacija DH),
    - RSA.
  - Enosmerne zgoščevalne funkcije:
    - 128-bitna MD5,
    - 160-bitna SHA-1.
  - Simetrična kriptografija:
    - 3DES,
    - 40-bitni RC2.

Varnostne aplikacije - S/MIME

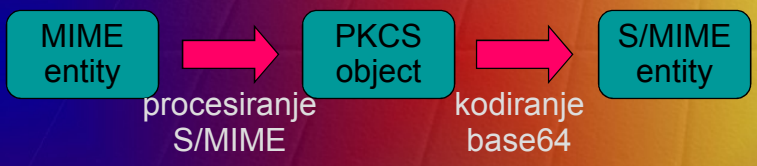
- Pošiljatelj (angl. User agent / UA) mora narediti sledeče:
  - Ugotoviti, ali je prejemnik sposoben opraviti dekripcijo - v kolikor ne, se mora odločiti, ali bo sploh poslal sporočilo.
  - Če ima pošiljatelj seznam preferiranih algoritmov s strani pošiljatelja, mora izbrati prvo od možnosti. Če tega seznama nima, mora izbrati ustrezne algoritme na podlagi že opravljene komunikacije.
  - Če nima nobene informacije v zvezi s tem, mora poskusiti s 3DES oz. RC 2 / 40.

Varnostne aplikacije - S/MIME

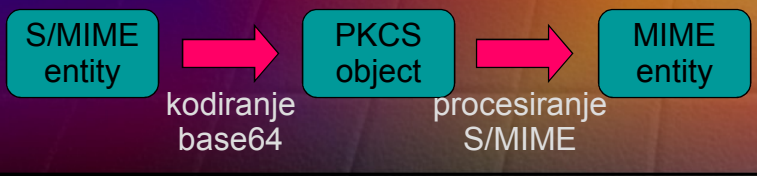
- Sporočila S/MIME.
  - S/MIME zaščiti objekt MIME, ki je lahko celotno sporočilo (izvzemši glavo RFC 822), ali del sporočila (če je “multipart”).
  - Objekti MIME s certifikati in identifikatorji algoritmov vred služijo tvorjenju objektov PKCS, ki jih obdelamo kot vsebino MIME (MIME wrapping).
  - V vseh primerih mora biti sporočilo pred pošiljanjem pretvorjeno v kanonično obliko.

Varnostne aplikacije - S/MIME

- Procesiranje S/MIME.
  - Pred pošiljanjem - prenosom:



  - Po pošiljanju, ob prejemu:



Varnostne aplikacije - S/MIME

- Nekateri tipi in podtipi vsebin S/MIME.

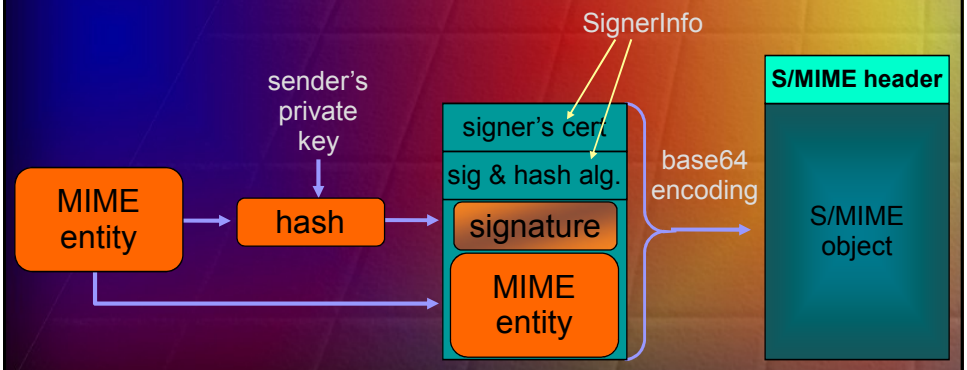
Type	Subtype	parameter	Description
Multipart	**signed**		One part is the message, the other is the signature.
Application	**pkcs7-mime**	**signedData**	A signed S/MIME entity.
	pkcs7-mime	**envelopedData**	An encrypted S/MIME entity.
	pkcs7-mime	**degenerate signedData**	An entity containing only PK certificates.
	pkcs7-signature	**–**	The content type of the signature subpart of multipart/signed message.
	pkcs10-mime	**–**	A certificate registration request.

Varnostne aplikacije - S/MIME

- S/MIME signedData.
  - To obliko lahko uporabljamo z enim ali večimi podpisniki.
    - Izberemo algoritem za izračun izvlečka sporočila (angl. message digest ali MD).
    - Kriptiramo izvleček s podpisnikovim privatnim ključem.
    - Pripravimo blok SignerInfo, ki vsebuje podpisnikov certifikat, identifikator algoritma za izračun izvlečka, identifikator algoritma za podpisovanje in sam podpis.
    - Dodamo lahko tudi niz potrebnih certifikatov.
    - Pred pošiljanjem opravimo kodiranje base-64.

Varnostne aplikacije - S/MIME

- Procesiranje pošte S/MIME, tip pošte signedData.

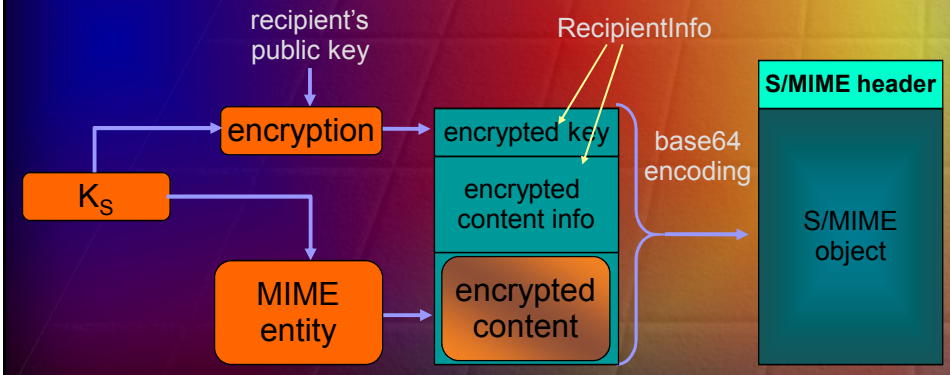


Varnostne aplikacije - S/MIME

- Pošta S/MIME, tip envelopedData.
  - Priprava oblike envelopedData:
    - Generiramo psevdo-naključen sejni ključ za izbran simetrični tajnopisni algoritem.
    - Za vsakega prejemnika kriptiramo ta ključ z njegovim javnim ključem RSA.
    - Za vsakega prejemnika tvorimo blok "RecipientInfo", ki vsebuje ID prejemnikovega certifikata, ID algoritma za dekripcijo sejnega ključa in sam kriptiran sejni ključ.
    - Celotno sporočilo (dobljeno vsebino) kriptiramo s sejnim ključem.

Varnostne aplikacije - S/MIME

- Procesiranje pošte S/MIME, tip pošte envelopedData.



Varnostne aplikacije - S/MIME

- Primer S/MIME SignedData.

```
Content-Type: application/pkcs7-mime;
        smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition:attachment;filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB97
7n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBghyHhHU
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8
```

- Primer S/MIME envelopedData.

```
Content-Type: application/pkcs7-mime;
        smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition:attachment;filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GI
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jHd
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHh6
```

Varnostne aplikacije - S/MIME

- Oblike S/MIME clearSigned.
  - Tip / podtip sta multipart / signed.
  - Prvi del je katerikoli tip MIME, drugi del pa je sam digitalni podpis.
  - S tem lahko sporočilo prikaže prejemnik, ki je sposoben procesirati MIME, ne pa tudi S/MIME.
  - Primer:

```
Content-Type: multipart/signed; protocol="application/pkcs7-signature";
                micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

This is a clear-signed message.

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition:attachment;filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF4674VQpfyF467
GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tb6
--boundary42--
```


Varnostne aplikacije - S/MIME

- Oblika S/MIME Registration Request.
  - Ta oblika tipa application/pkcs10 je namenjena pridobivanju (tudi izdajanju) certifikata in vključuje:
    - ustrezen blok RequestInfo,
    - identifikator asimetričnega algoritma,
    - podpis bloka RequestInfo s privatnim ključem, katerega pripadajoči javni ključ želimo overiti.
  - Blok RequestInfo vključuje enolično razločevalno ime nosilca certifikata in bitno predstavitev njegovega javnega ključa.

Varnostne aplikacije - S/MIME

- Pomembnejši standardi S/MIME:
  - S/MIME v3.1 Certificate Handling (RFC 3850),
  - S/MIME v 3.1 Message Specification (RFC 3851),
  - Cryptographic Message Syntax (CMS) (RFC 3852) ,
  - Cryptographic Message Syntax Algorithms (RFC 3370),
  - Use of the AES in CMS (RFC 3565),
  - Use of the IDEA Encryption Algorithm in CMS (RFC 3058),
  - Enhanced Security Services for S/MIME (RFC 2634),
  - Use of ECC Algorithms in CMS (RFC 3278),
  - Diffie-Hellman Key Agreement Method (RFC 2631),
  - Use of the KEA and SKIPJACK in CMS (RFC 2876),
  - Electronic Signature Policies (RFC 3125),
  - Electronic Sig. Formats for long term signatures (RFC 3126),
  - Securing X.400 Content with S/MIME (RFC 3854),
  - Transporting S/MIME Objects in X.400 (RFC 3855).

Kriptografski protokoli in poslovni procesi

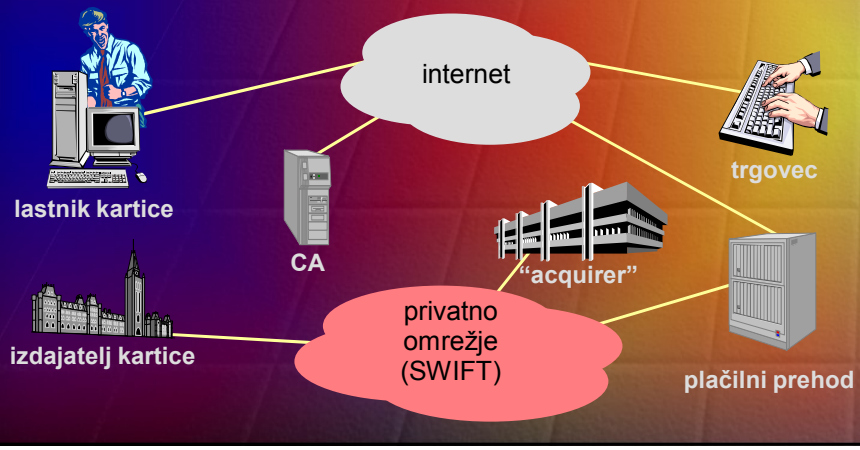
- Secure electronic transactions - SET.
  - To je standard za ščitenje finančnih transakcij prek omrežij, kjer uporabljamo kreditne in plačilne kartice - je v bistvu infrastruktura, ne toliko plačilni sistem.
  - Prva različica je bila definirana leta 1996 (v obsegu 63 strani), ki so jo sprejele organizacije Visa, MasterCard, IBM, MS, RSA, Netscape, Terisa, Verisign.
  - Prve implementacije leta1998.
  - Številka zadnje različice je 3, standard pa je obsegal skoraj 1000 strani.

Kriptografski protokoli in poslovni procesi

- Secure electronic transactions - SET.
  - Temeljne lastnosti.
    - Zaupnost podatkov: Podrobnosti o računu lastnika kartice in podrobnosti o plačilu so na omrežju ščitene in nedostopne tudi trgovcu.
    - Celovitost podatkov: Podatki, ki jih pošlje kupec trgovcu (naročilo, osebni podatki, navodila za plačilo) so zaščitene proti spremembam z dig. podpisi in KOS.
    - Overjanje kupca: Trgovec preveri identiteto plačnika z zagotovilom avtorizacije plačila.
    - Overjanje trgovca: Lastnik kartice lahko preveri identiteto trgovca in to, da je ta pooblaščen za izvedbo plačil s pomočjo kartic.

Kriptografski protokoli in poslovni procesi

- Arhitektura SET.



Kriptografski protokoli in poslovni procesi

- Entitete SET.
  - Lastnik kartice (angl. cardholder) – to je avtoriziran uporabnik plačilne oz. kreditne kartice.
  - Trgovec (angl. merchant) - prodajalec proizvodov ali storitev.
  - Izdajatelj kartice (issuer) - finančna institucija, ki izdaja kartice (tipično je to poslovna banka).

Kriptografski protokoli in poslovni procesi

- Entitete SET.
  - Realizator plačil (angl. acquirer) - finančna institucija, pri kateri ima trgovec račun in ki avtorizira plačila ter opravlja finančne transferje.
  - Plačilni prehod (angl. payment GW) - strojno - programski prehod za procesiranje sporočil trgovca.
  - Izdajatelj overjenih digitalnih potrdil (angl. certification authority) - izdajatelj overjenih potrdil (certifikatov) X.509 v3.

Kriptografski protokoli in poslovni procesi

- Visokonivojski pregled postopkov SET.
  - Na banki odpre kupec račun in dobi plačilno oz. kreditno kartico.
  - Kupec pri CA pridobi certifikat, ki njegovo identiteto poveže z javnim ključem in podrobnostmi kartice.
  - Trgovec dobi dva certifikata, enega za pod-pisovanje in enega za izmenjavo ključev.
  - Kupec pošlje naročilo z izbranimi postavkami, nakar trgovec odgovori s certifikatom in številko naročila.
  - Kupec preveri trgovčev certifikat.

Kriptografski protokoli in poslovni procesi

- Visokonivojski pregled postopkov SET.
  - Kupec pripravi plačilne podrobnosti in jih skupaj z naročilom pošlje prodajalcu, čemur doda svoj certifikat (tu plačilne podrobnosti prodajalcu niso vidne).
  - Prodajalec preveri certifikat in zaprosi za avtorizacijo plačila tako, da podrobnosti plačila posreduje plačilnemu prehodu.
  - Po avtorizaciji prodajalec vrne kupcu potrditev naročila in pošlje blago.
  - Prodajalec pošlje prošnjo za plačilo plačilnemu prehodu.

Kriptografski protokoli in poslovni procesi

- SET - mehanizem dvojnega podpisa.
  - Ta mehanizem poveže dve sporočili, ki sta namenjeni različnima prejemnikoma.
  - Osnovni scenarij: Kupec pošlje podatke naročila (*O=order*) trgovcu in plačilna navodila (*P=payment*) banki na način, ki banki onemogoča vpogled v naročilo, trgovcu pa ne v podrobnosti plačila.
  - Če bi poslali dve ločeni podpisani sporočili, bi lahko prišlo do situacije, ko bi npr. trgovec trdil, da je določeno naročilo povezano z nekimi drugimi plačilnimi navodili.

Kriptografski protokoli in poslovni procesi

- SET - mehanizem dvojnega podpisa S_D (indeks C označuje kupca, angl. customer).
  - Kupec izračuna izvleček H nad P in O.
  - Izvlečka stakne in izračuna končni izvleček.
  - Končni izvleček kriptira s priv. ključem K_C^{-1}:

    $$S_D = \{H(H(P) \,||\, H(O))\}K_C^{-1}$$

  - Nato trgovec dobi O, S_D, $H(P)$ in kupčev javni ključ K_C - izračuna lahko

    $$H(H(P) \,||\, H(O)) \text{ in } \{S_D\}K_C$$

  - Če se vrednosti ujemata, je podpis OK.

Kriptografski protokoli in poslovni procesi

- SET - mehanizem dvojnega podpisa.
  - Podobno banka, ko dobi S_D, $H(O)$, P in kupčev javni ključ K_C lahko izračuna
    $H(H(P) \,||\, H(O))$ in $\{S_D\}K_C$
  - Če se vrednosti ujemata, je podpis OK.
- Zgornji postopek zagotavlja, da
  - trgovec prejme O in lahko preveri podpis;
  - banka prejme P in lahko preveri podpis;
  - da sta P in O dokazljivo povezana med sabo prek dvojnega podpisa.

Kriptografski protokoli in poslovni procesi

- SET – faza nakupa.
  - Izmenjana sporočila:
    - "Initiate Request" omogoča kupcu pridobiti certifikate prodajalca in plačilnega prehoda skupaj z identifikatorjem (ID) te zahteve in naključnim številom. To zahtevo pošlje trgovcu skupaj z vrsto kartice.
    - "Initiate response" je odgovor trgovca, ki ga podpiše s svojim privatnim ključem, kjer se nahaja tudi naključna vrednost iz prvega sporočila, naključna vrednost trgovca, ID transakcije, trgovčev certifikat za podpise in certifikat prehoda za izmenjavo ključev.

Kriptografski protokoli in poslovni procesi

- SET – faza nakupa.
  - Izmenjana sporočila:
    - "Purchase request" pošlje kupec po preverjanju dobljenih certifikatov. Kupec pred tem tvori *O* in *P* ter jima pridruži od trgovca dobljen ID transakcije. Prav tako kreira simetrični ključ.
    - "Purchase response" sporočilo tvori trgovec za potrditev naročila in navede ustrezno referenčno številko transakcije - vse to podpiše s svojim privatnim ključem in skupaj s pripadajočim certifikatom to pošlje kupcu.

Kriptografski protokoli in poslovni procesi

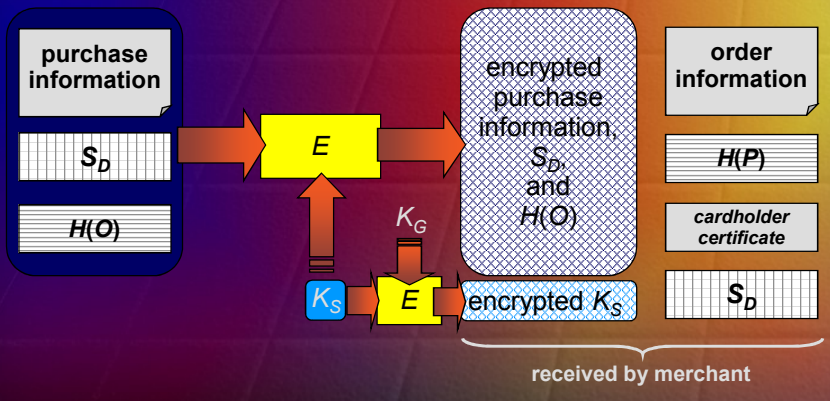
- SET – faza nakupa.
  - Struktura sporočila "Purchase request":
    - Vključuje podatke *P*, ki jih bo trgovec posredoval plačilnemu prehodu, dvojni podpis nad *P* in *O*, *H*(*O*) in simetrični ključ K_S v digitalni ovojnici, kriptiran z javnim ključem prehoda / banke K_G. Trgovec tega dela ne more brati.
    - Vključuje podatke o naročilu *O*, dvojni podpis nad *P* in *O* ter *H*(*P*).
    - Vključuje certifikat lastnika kartice, ki ga potrebujeta trgovec in plačilni prehod.

Kriptografski protokoli in poslovni procesi

- SET – faza nakupa.
  - Po prejemu sporočila “Purchase request” trgovec preveri kupčev certifikat, dvojni podpis, sprocesira naročilo in pošlje podrobnosti za plačilo plačilnemu prehodu. Zatem kupcu pošlje “Purchase response”.
  - Kot vidimo, SET potrebuje dve vrsti certifikatov (in skladno s tem dve vrsti privatnih / javnih ključev): eno vrsto za podpisovanje, drugo za izmenjavo simetričnih sejnih ključev.

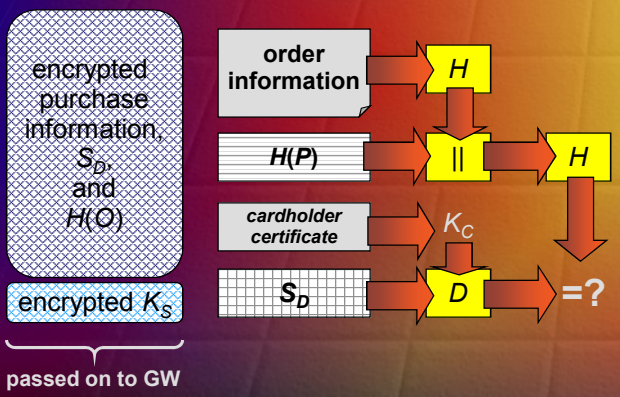
Kriptografski protokoli in poslovni procesi

- Procesiranje plačil pri SET - primer:
  - Struktura sporočila “Purchase Request”.



Kriptografski protokoli in poslovni procesi

- Procesiranje plačil pri SET - primer:
  - Preverjanje sporočila “Purchase Request”.



Kriptografski protokoli in poslovni procesi

- SET – faza avtorizacije.
  - Ta faza zagotavlja, da bo trgovec prejel plačilo; ima dve sporočili, “Authorization Request” in “Authorization Response”.
  - Trgovec pošlje prehodu sporočilo “Authorization Request”, ki vsebuje:
    - podatke o nakupu, dobljene od kupca (*P*, dvojni podpis prek *P* in *O*, *H*(*O*) in digitalno ovojnico);
    - trgovčeve podatke za avtorizacijo (kriptiran in od trgovca podpisan *ID* transakcije ter digitalno ovojnico z začasnim simetričnim ključem, ki ga bo uporabil plačilni prehod za avtorizacijo);
    - certifikate (kupčev in trgovčev cert. za podpisovanje in trgovčev cert. za izmenjavo ključev, ki ga potrebuje plačilni prehod).

Kriptografski protokoli in poslovni procesi

- SET – faza avtorizacije.
  - Plačilni prehod po prejemu sporočila "Authorization request" opravi sledeče:
    - preveri certifikate;
    - dekriptira digitalno ovojnico, da pride do podatkov za avtorizacijo;
    - preveri podpis na podatkih za avtorizacijo;
    - dekriptira digitalno ovojnico, da pride do ključa s katerim dostopi do plačilnih podatkov (ki jih je kreiral kupec);
    - preveri dvojni podpis in to da se *ID* transakcije trgovca in *ID* transakcije kupca ujemata;
    - posreduje izdajatelju kartice zahtevo za avtorizacijo.

Kriptografski protokoli in poslovni procesi

- SET – faza avtorizacije.
  - Sledi sporočilo "Authorization response".
    - Po potrditvi avtorizacije prehod tvori avtorizacijski blok in ga podpiše, kriptira to s simetričnim ključem in tvori digitalno ovojnico z uporabo trgovčevega javnega ključa.
    - Prehod doda še t.i. "Capture token data", ki služijo kasneje realizaciji plačila in jih sprocesira enako kot avtorizacijski blok. Trgovec teh podatkov ne procesira.
    - Prehod doda tudi lasten certifikat za podpise.
  - Po prejemu in preverjanju tega sporočila lahko trgovec pošlje blago.

Kriptografski protokoli in poslovni procesi

- SET – faza plačila.
  - Sledi “Payment capture” - za realizacijo plačila sta potrebni sledeči sporočili:
    - “Capture request” - trgovec generira blok z ID transakcije in višino plačila, to podpiše in kriptira. Doda tudi “Capture token data” iz predhodnjega koraka in lastna certifikata za podpise ter izmenjavo ključev.
    - “Capture response” - prehod dekriptira blok in preveri “Capture token data”. Če je vse OK, generira nalog za prenos sredstev in ga pošlje banki. zatem pošlje odgovor trgovcu, ki je podpisan in kriptiran ter mu doda lasten certifikat za podpisovanje.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Infrastruktura za overjanje, avtorizacijo in obračunavanje (OAB).
  - Služi omogočanju pooblaščenega dostopa do storitev v porazdeljenih omrežjih in
  - Služi beleženju dogodkov, ki so pomembni za zaračunavanje storitev, kar je prioritetno v komercialnih okoljih.
- Angleška okrajšava za te sisteme je AAA (auth., authorization, accounting).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Razvoj tovrstne infrastrukture sega v devetdeseta leta - Kerberos:
  - Ta sistem je bil razvit na MIT v okviru projekta Atena.
  - Služil je temu, da se je uporabnik le enkrat prijavil v sistem, nakar so mu bili dodeljeni viri skladno z avtorizacijsko politiko.
  - Problem Kerberosa je ta, da je koncipiran za omrežja LAN in ni razširljiv na omrežja, WAN.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Koncem devetdesetih let (z razvojem e-poslovanja) pride do potrebe po sistemih OAB za večja omrežja zaradi
  - povezav fizično oddaljenih omrežij, ki
  - pripadajo različnim administrativnim domenam, vendar
  - omogočajo poenoten pogled na uporabnika, vključno z zaračunavanjem.
- Prva tovrstna rešitev je bila RADIUS.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS (Remote Access Dial-In User Service).
  - Temelji na principu strežnik – odjemalec, kjer odjemalca RADIUS-a predstavlja t.i. strežnik omrežnega dostopa ali SOD (angl. Network Access Server, NAS).
  - Končni uporabnik, ki se prek NAS prijavlja v sistem torej ni mišljen kot odjemalec, ko govorimo o RADIUS-u:
    - uporabnik NAS (odjemalcu v Raidusu) posreduje ustrezne podatke,
    - ta pa jih prek zahtevkov pošlje strežniku RADIUS.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS (Remote Access Dial-In User Service).
  - Strežnik RADIUS na podlagi vzpostavljene politike odobri overjanje kot uspešno, ali pa zahteva dodatne korake ter vrne NAS ustrezne konfiguracijske podatke.
  - V primeru uspešnega overjanja odjemalec NAS spusti uporabnika do storitev.
  - NAS je odgovoren za beleženje podatkov o uporabi virov in poročanje strežniku.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Sporočila RADIUS-a.
  - Nabor sporočil je enostaven in se sestoji iz vsega osmih sporočil.
  - Le štiri od njih so podrobno definirana v osnovni specifikaciji.
    - Access Request: To sporočilo generira odjemalec RADIUS (NAS) in ga pošlje strežniku.
    - Access Challenge: To sporočilo strežnik RADIUS pošlje odjemalcu in služi kot vprašanje končnemu odjemalcu (za izziv, pogajanje, itd.).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Sporočila RADIUS-a.
  - Le štiri od njih so podrobno definirana v osnovni specifikaciji.
    - Access Accept – to sporočilo odjemalcu RADIUS (to je NAS) sporoči uspešno overjanje in da dovoljenje za dostop do sredstev.
    - Access Reject – sporočilo strežnika RADIUS, da mora NAS zavrniti dostop.
    - Accounting Request – to sporočilo strežniku pošlje NAS in vsebuje podatke za obračunavanje storitev.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Sporočila RADIUS-a.
  - Le štiri od njih so podrobno definirana v osnovni specifikaciji.
    - Accounting response – s tem sporočilom strežnik potrdi podatke beleženja in poda tudi druge rezultate.
    - Status Server – to je eksperimentalne narave (prvenstveno služi podajanju stanja strežnika).
    - Status Client – tudi to sporočilo je eksperimentalne narave in služi podajanju stanja strežnika.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Sporočila RADIUS-a.
  - Informacije se prenašajo kot t.i. atributi.
  - Format atributov je tip-dolžina-vrednost (type-length-value, TLV):
    - tip atributa je podan z enim oktetom;
    - dolžina atributa je podana v oktetih in obsega celotno koristno vsebino, to je tip in samo polje za dolžino;
    - vrednost atributa je sama informacija sporočila RADIUS.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Sporočila RADIUS-a.
  - Celoten paket tvori glava in vsaj en atribut:
    - Glava ima polja, kjer je prvo polje tip sporočila (access request, response, ...), drugo polje identifikator ID (kateremu izzivu je pridružen nek odziv), tretje je dolžina (celotna dolžina paketa) in četrto polje služi overjanju (authenticator).
    - Glavi sledi en ali več atributov – ti atributi omogočajo razširljivost RADIUS-a in so lahko specifični za posameznega proizvajalca (v osnovni specifikaciji je podanih ~40 atributov).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in zanesljivost prenosa.
  - RADIUS je v bistvu protokol aplikacijskega sloja, ki za prenos uporablja protokol UDP.
  - UDP je bil izbran zaradi večje učinkovitosti (vzpostavitev povezave TCP je draga).
  - Odločitev za UDP pomeni, da je prenos nezanesljiv in v omrežjih slabe kakovosti postane RADIUS neprimeren.
  - Izbira UDP ima tudi negativne posledice za samo varnost.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - Zelo elementarna varnostna mehanizma – skrivanje atributov in pa overjanje sporočil.
  - Oba mehanizma slonita na MD5 in uporabi skupne deljene skrivnosti med strežnikom in NAS.
  - Overjanju služi polje „Authenticator“ v glavi sporočila in se deli na „Request authenticator“ (v Access Request) in „Response authenticator“ (v Access Challenge, Accept in Reject).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - „Request authenticator“:
    - Ta vsebuje 128-bitno naključno vrednost, ki jo generira odjemalec.
    - Nima nobenih dodatnih zaščit, zatorej celovitost (integriteta) te vrednosti ni zagotovljena.
    - Ta vrednost naj bi bila v določenem časovnem intervalu globalno enolična za preprečitev napadov s ponovitvami, vendar generirane vrednosti običajno vsebujejo malo entropije (razlog je ta, da pred desetimi leti s skupno skrivnostjo ščitenega gesla ni bilo lahko razkriti, dodatno preverjanje številk IP pa je bil dovolj dober dodaten varnostni mehanizem).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - „Request authenticator“ se zaradi opisanih slabosti nadomesti z atributom „Message Authenticator“.
    - Tu odjemalec izračuna MAC celotnega sporočila ob uporabi skupne deljene skrivnosti:

      $MD5_{sharedSecret}$(Code, Length, ID, Request Authenticator Attributes)
    - Uporaba tega mehanizma je opcijska, tako da lahko ostane v uporabi le šibek mehanizem skrivanja gesla (attribute hiding).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - „Response authenticator“:
    - Ta je ščiten podobno kot „Request authenticator“.
    - Tu je zaščita obvezna in vsebuje pri izračunu MAC še skupno deljeno skrivnost:

      $MD5_{sharedSecret}$(Code, Length, ID, Request Authenticator, Shared Secret)
    - ID v odzivu ustreza vrednosti ID v izzivu.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - Večina funkcionalnosti, ki jo omogoča RADIUS, je realizirana prek atributov.
  - Velik pomen skrivanja atributov (attribute hiding); najpomembnejše namembnost je za skrivanje gesla.
  - Postopek skrivanja gesla uporabnika (user password, P) sloni na uporabi deljene skrivnosti (SS) med strežnikom in NAS ter naključne vrednosti (R).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - Postopek skrivanja gesla:
    - NAS izračuna

      $B = MD5(SS \,||\, R),\ C = B \oplus P$

      in pošlje vrednost C kot atribut sporočila.
    - Če je geslo daljše od 16B, ga segmentira v 16B dolge nize in izračuna

      $B_1 = MD5(SS \,||\, R),\ C_1 = B_1 \oplus P_1$

      $B_2 = MD5(SS \oplus C_1),\ C_2 = B_2 \oplus P_2$

      ...
    - ter pošlje kot atribute $C_1, C_2, ..., C_n$.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - Skrivanje atributov je le na videz učinkovito – prva slabost:
    - Globalna enoličnost zahteva kakovosten vir z zadostno entropijo, da generira primerne (psevdo)naključne vrednosti R.
    - Glede na razpoložljivo procesno moč NAS velikokrat ne uspe zagotoviti tega pogoja.
  - Torej se bosta relativno hitro pojavili dve enaki vrednosti R in s tem B_1, kar pomeni, da...

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in varnost.
  - Skrivanje je le na videz učinkovito – druga slabost:
    - Skupna skrivnost SS je dolgoročna in relativno statična vrednost.
    - Napadalec pošlje ukaz za overjanje in podtakne geslo in nato prestreže C_1, C_2, ..., C_n.
    - Ker pozna podtaknjeno geslo, lahko z uporabo XOR dobi vrednosti B_1, B_2, ..., B_n.
    - Ker zaradi slabe entropije hitro pride do ponavljanja R, lahko napadalec iniciira overjanja, dokler se ne začne ponavljanje niza B_i, nakar napadalec začne ugibati geslo.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Preostale slabosti RADIUS-a.
  - Skupne skrivnosti so nastavljene ročno.
  - Pri veriženju odjemalcev NAS (proxies) je skrivnost deljena le med neposrednima sosedoma (in ne med prvim odjemalcem NAS ter strežnikom RADIUS).
  - Vrata fragmentov UDP in naslovi IP so lahko potvorjeni.
  - Skrivanje atributov je zaščita na aplikacijskem nivoju, pa še ta je slabo kriptiran.
- Rešitev je RADIUS prek IPSec.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

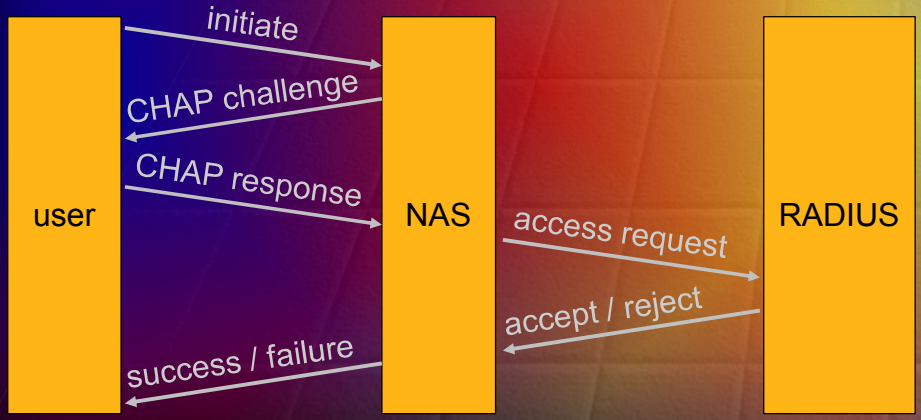
- RADIUS in podprti protokoli overjanja.
  - Overjanje pri PPP (Point to Point Protocol):
    - NAS od uporabnika zahteva uporabniško ime in geslo in s skrivanjem atributa kreira sporočilo „Access Request“.
    - V kolikor ni v določenem časovnem intervalu odziva na „Access Request“, ga pošlje ponovno istemu ali pa drugemu strežniku.
    - Strežnik po prejemu sporočila preveri, če ima skupno skrivnost z NAS in če je tako, potem preveri geslo ter ga (če je vse OK) potrdi. V nasprotnem primeru pošlje „Access Reject“.
  - Geslo pri PPP se pošilja prek omrežja.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in podprti protokoli overjanja.
  - Overjanje pri CHAP (Challenge Handshake Authentication Protocol):
    - Uporabnik pošlje zahtevek NAS, ta pa v odzivu posreduje 16B izziv CLG, ki ima določen ID.
    - V odzivu uporabnik uporabi isti ID, doda uporabniško ime in odziv MD5(ID, SS, CLG).
    - NAS v Access Request posreduje ID, uporabniško ime in odziv strežniku RADIUS, ki na podlagi up. imena poišče SS, izračuna MD5(ID, SS, CLG) rezultat primerja s prejeto vrednostjo in pošlje ustrezen odziv.
  - Pri CHAP se geslo ne pošilja prek omrežja.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in podprti protokoli overjanja.



Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in beleženje (obračunavanje).
  - Prenos primitivov je prek protokola UDP.
  - Uporablja dva primitiva, „Accounting Request“ (vedno od odjemalca k strežniku) in „Accounting Response“ (v obratni smeri).
  - NAS mora biti sposoben beleženja.
  - Atributi primitivov so Type (start / stop), Input / Output Packets/Octets (število dohodnih / odhodnih paketov / bytov), Session Time (poslan po koncu seje in podaja trajanje povezave), Authentic (podaja, kako je bil uporabnik overjen).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in obračunavanje.
  - Problematično izvajanje beleženja na podlagi nezanesljive storitve:
    - fragmenti UDP se lahko izgubijo ali podvojijo;
    - s tem je povzročeno pomanjkljivo zaračunavanje storitev, npr. ob izgubi Stop primitivov (prenizek znesek obračuna);
    - zaradi performančnih razlogov operaterji omejijo največje število možnih sej s čimer ob izgubi primitivov Stop uporabnik ne dobi dostopa za otvoritev nove seje.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

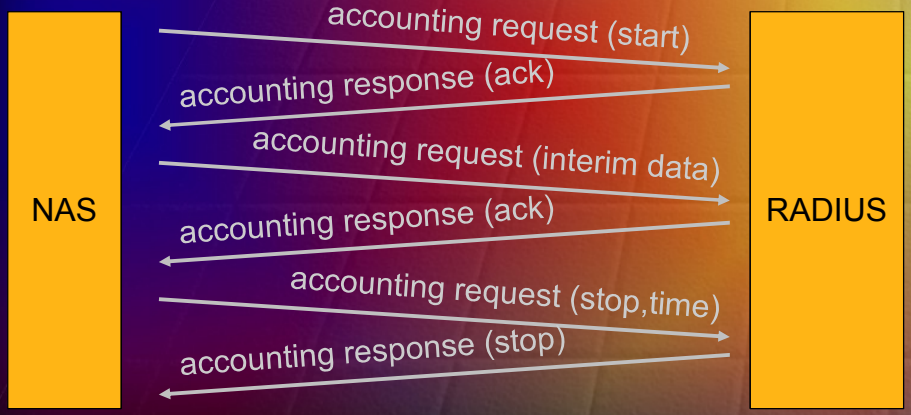
- RADIUS in obračunavanje.
  - Zanesljivost obračunov lahko izboljšamo z uporabo ponovitev in podaljšanjem dovoljenega časa njihovega pošiljanja.
  - Varnost pri beleženju je malenkost boljša kot pri ostalih operacijah - Accounting Request in Accounting Response sta overjena z uporabo skupne skrivnosti:

    authReq = MD5(Code, ID, Length, 16 zero bytes, request attributes, SS)

    authRes = MD5(Code, ID, request authenticator, SS).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in obračunavanje.



Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS in podpora mobilnim omrežjem.
  - Podpora gostovanja (angl. roaming) je omogočena prek veriženja proksijev.
  - Vsak par proksijev v verigi si deli svojo skupno skrivnost, vsak proksi pa v eno smer igra vlogo odjemalca, v drugo pa strežnika.
  - Usmerjanje primitivov poteka na osnovi vrednosti NAI (Network Access Identifier).
  - Ker je overjanje le od točke do točke, so možni napadi tipa „napadalec vmes“ (angl. man-in-the-middle).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS - zaključki.
  - Sistemi OAB postajajo ključni v omrežjih tako s stališča obračunavanja kot varnosti.
  - RADIUS ima mnogo pomanjkljivosti (že podanih).
  - Rešitve z razširitvami RADIUS-a so zelo otežene, saj ne ne omogoča novih, kompleksnejših protokolov za overjanje (zaradi omejenega število primitivov in omejene dolžina atributov).
  - Problem investicij v obstoječo infrastrukturo (podobno kot pri SMTP).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- RADIUS – ključni standardi.
  - Rigney C., Remote Authentication Dial-In User Service (RADIUS), Draft, IETF, 2000.
  - Rigney C., RADIUS Accounting, RFC 2866, IETF, 2000.
  - Rigney C., RADIUS Extensions, RFC 2869, IETF, 2000.
  - Aboba B., Vollbrech J., Proxy Chaining and Policy Implementation in Roaming, RFC 2607, IETF, 1999.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

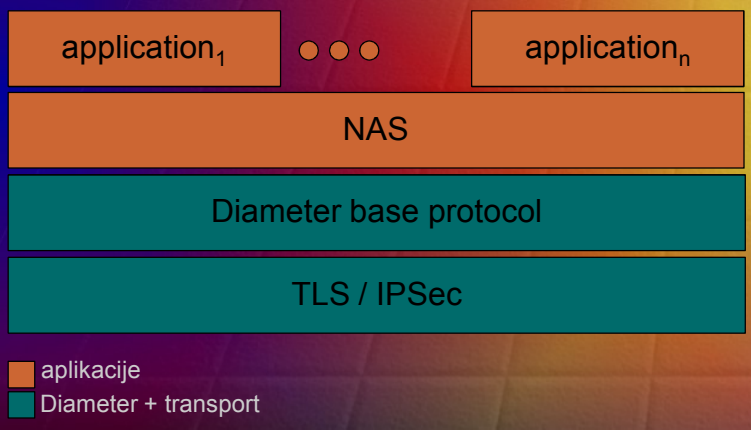
- Diameter.
  - Standardizacija RADIUS-a končana v letu 2000 – zaradi množice slabosti opuščene nadgradnje.
  - Začetek iskanja novega standarda, kjer so bili izhodiščni predlogi protokol SNMP, protokol COPS in protokol Diameter:
    - Slabost SNMP je slaba podpora overjanju.
    - Slabost protokola Common Open Policy Service je, da prvenstveno služi kakovosti storitev (angl. QoS) in bi na požarnih pregradah nastala težava pri filtriranju – je fragment AAA ali QoS?

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter.
  - V osrednjem standardu so opredeljeni strežniki, proksiji, sam protokol (osnovni nabor sporočil z atributi), ter operabilnost med različnimi administrativnimi domenami.
  - Aplikacije so obravnavane v dopolnilnih standardih in ne osrednjem standardu.
  - V primeru Diametra postane tudi NAS del aplikacijskega sloja.
  - Osrednji standard ne pokriva overjanja in avtorizacije - je osredotočen na (beleženje) obračunavanje.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter.



Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter in varnost.
  - Protokol omogoča varnost od konca do konca (end-to-end) ali od točke do točke (point-to-point).
  - Zaščito od konca do konca lahko zagotovi TLS ali IPSec.
  - Težava pri zaščiti od konca do konca nastopi, če so potrebni proksiji, ki potrebujejo vpogled v vsebino (npr. signalizacija pri prehajanju in sledenju, angl. roaming) – skrivanje atributov.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter in prenos (transport).
  - Prenos temelji na zanesljivem, povezavno usmerjenem protokolu, ki je lahko:
    - TCP (Transmission Control Protocol) ali pa
    - SCTP (Stream Transmission Transport Protocol) – ta je namenjen prenosu toka podatkov med dvema končnima točkama predvsem za podporo vzpostavljanja telefonske povezave prek Interneta in ustrezno signalizacijo.
  - Strežniki in agenti morajo podpirati TCP in SCTP, odjemalci pa vsaj enega od njih.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter in aplikacije.
  - Obračunavanje (accounting) – od aplikacij je edina obravnavana v osnovnem standardu.
  - Upravljanje dobropisa (credit control) – ta služi podpori popularnih predplačniških modelov v celičnih, mobilnih omrežjih.
  - Omrežna dostopna točka (NAS) – ta obravnava interakcijo odjemalcev za omogočanje dostopa (NAS) in strežnikov s poudarkom na overjanju (za protokole PAP, CHAP in druge).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

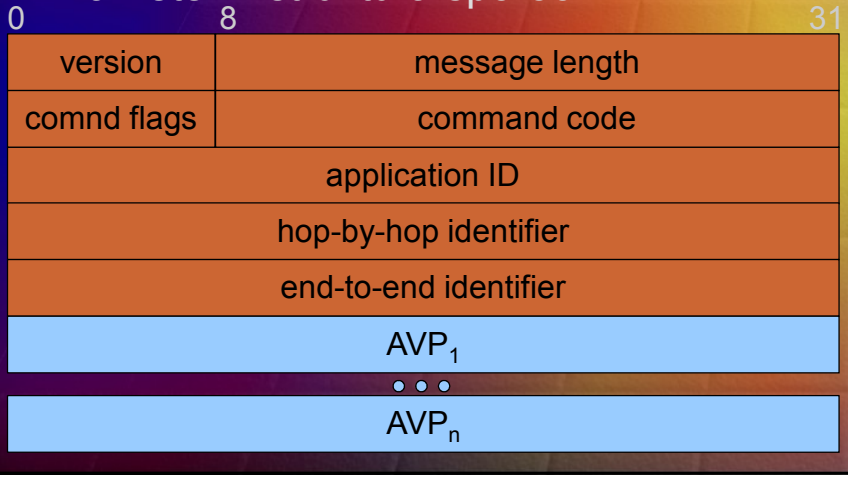
- Diameter in aplikacije.
  - Mobilni IP (mobile IP) – ta podpira overjanje in avtorizacijo za mobilni IP, ki ima specifične zahteve pri prenosu in usmerjanju paketov med računalniki (RADIUS tu nima definirane podpore).
  - Razširljiv protokol za overjanje (Extensible Authentication Protocol, EAP) – ta aplikacija podpira množico možnih postopkov overjanja, ki jih omogoča EAP in sicer tako za ožičena kot brezžična omrežja.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – podrobnosti protokola.
  - Protokol je tipa vsak-z-vsakim (peer-to-peer), saj tako odjemalec kot strežnik lahko kreirata bodisi zahtevo, bodisi odgovor.
  - Zaradi te narave protokola so tipi sporočil poimenovani kar ukazi (angl. commands).
  - Sporočila se sestoje iz glave in koristne vsebine, ki jo predstavljajo atributi.
  - Atributi so podani v formatu atribut-vrednost (attribute-value pair, AVP).
  - Atributi pravzaprav podajajo ukaze.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – struktura sporočil.



Infrastruktura za overjanje, avtorizacijo in obračunavanje

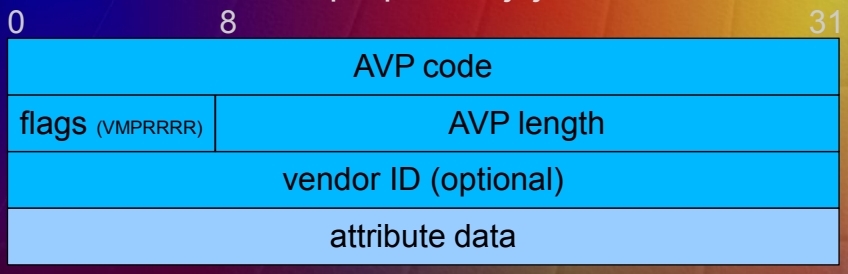
- Diameter – struktura sporočil.
  - Verzija (version) določa različico - trenutno je ta vrednost 1.
  - Zastavice ukazov (command flags) določajo tip sporočila:
    - R pomeni zahtevo ali odziv (request / response);
    - P pomeni, da se sporočilo lahko usmerja oz. posreduje proksiju (proxiable);
    - E označuje napake (error);
    - T označuje, če je sporočilo lahko ponovno poslano, da zmanjšamo podvojitve.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – struktura sporočil.
  - Koda ukaza (command code) določa ukaz, povezan s sporočilom, npr. „abort session request“.
  - Identifikator aplikacije (application ID) določa tisto aplikacijo, ki ji je sporočilo namenjeno.
  - Identifikator vmesnih točk (hop-by-hop ID) vsebuje identifikatorje, s pomočjo katerih so izzivom pridruženi ustrezni odzivi.
  - Identifikator končnih točk (end-to-end identifier) služi skupaj z atributi preprečevanju podvajanj sporočil.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – struktura atributov.
  - AVP se lahko poljubno dodajajo sporočilu.
  - Nekatera sporočila zahtevajo minimalno število AVP in prepovedujejo določene AVP.



glava atributa

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – struktura atributov.
  - Koda AVP (AVP code) določa tip atributa in te tipe standardizira IANA.
  - Kode od 0 do 255 so vzvratno združljive z RADIUS-om.
  - Zastavice (flags):
    - V je za proizvajalca specifična zastavica (vendor);
    - M pomeni obvezno zastavico (mandatory);
    - P pomeni zahtevo za enkripcijo od konca do konca (protect);
    - RRRRR so rezervirane zastavice (reserved).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – primeri AVP.
  - Origin-host AVP – ta atribut doda izvorna točka in ga vmesni agenti ne smejo spremeniti (prisoten mora biti v vseh sporočilih).
  - Origin-realm AVP – ta atribut določa varnostno področje (angl. realm) pošiljatelja in mora biti prisoten v vseh sporočilih ter ga vmesni agenti ne smejo spremeniti.
  - Destination-host AVP – služi usmerjanju proti domačemu strežniku oz. domači domeni uporabnika, ko je ta fiksna.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – primeri AVP.
  - Destination-realm AVP – ta podaja varnostno področje, kamor mora biti usmerjeno sporočilo.
  - Routing AVP – služi usmerjanju sporočil skozi sistem Diametra (odjemalci, agenti, proksiji, strežniki).
  - Result-code AVP – podaja rezultat za določeno zahtevo in sicer ali je bila uspešno izvršena ali ne in podrobnejšo opredelitev napake.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – koncepti prenosa.
  - Obstajata seja in povezava:
    - Seja je logični koncept na aplikacijskem nivoju, ki se vzpostavi med končno napravo, to je odjemalcem in strežnikom, vmes pa so lahko posredniki (imenovani tudi agenti).
    - Povezava je transportni koncept (koncept prenosa sporočil) in pomeni povezavo med katerimakoli soležnima osebkoma, ki sta sposobna izmenjave sporočil protokola.
    - Preslikava med povezavo in sejo ni nujno 1:1 – npr. overjanje je lahko del ene seje, podatki te seje pa so lahko multipleksirani z drugimi sejami znotraj določene povezave.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – koncepti usmerjanja.
  - Vozlišča uporabljajo tabele soležnih entitet in tabele varnostnih področij (angl. realms):
    - Tabela soležnih osebkov vsebuje vnose o soležnih entitetah (agentih), stanju le-teh, ali so statično ali dinamično konfigurirani, itd.
    - Druge uporabljajo agenti zato, da določijo primerno varnostno območje (kar je sorodno usmerjanju pri paketih IP, le da ni nujno, da se vedno ujemajo naslovi v celoti, ampak v večini mest), ali da določijo točno lokacijo (kar je sorodno host ID pri usmerjanju paketov IP), itd.
  - RADIUS ne določa delovanja proksijev, sledenja, niti podpore varnostnih področij.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – usmerjanje sporočil.
  - Če se sporočilo ne procesira lokalno, ga vozlišče na podlagi tabele soležnih osebkov (=entitet) posreduje ustreznemu na poti do soležnega osebka.
  - Pri posredovanju mora biti upoštevano končno varnostno območje, ki ga opredeljuje Destination-realm AVP.
  - Zahteve, ki ne smejo biti posredovane dalje, so ustrezno označene.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – usmerjanje sporočil.
  - Zahteve so lahko posredovane le določenemu varnostnemu območju in tam procesirane s strani poljubnega strežnika (te vsebujejo le Destination-realm AVP).
  - Zahteve so lahko poslane točno določenemu strežniku v določenem varnostnem območju (te morajo vsebovati tako Destination-host AVP kot tudi Deatination-realm AVP).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – varnost.
  - Podpora IPSec je obvezna za vse entitete, medtem ko je podpora TLS za odjemalce in končne naprave opcijska, kar olajša izvedbo (ni nujna podpora procesno zahtevne PKI in certifikatov X.509 na nivoju aplikacije).
  - Poleg IPSec in TLS zaščite je za varovanje od točke do točke predvidena tudi uporaba kriptografskih razširitev (cryptographic message syntax, CMS).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – varnost.
  - Prenos od točke do točke mora biti obvezno ščiten z IPSec ali TLS (to še vedno omogoča napade s strani zlonamernih agentov).
  - IPSec mora biti podprt v transportnem načinu, vsak paket mora biti overjen.
  - Če IPSec ali TLS ni na voljo, se lahko prenašajo le sporočila za podajanje zmožnosti (capabilities).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

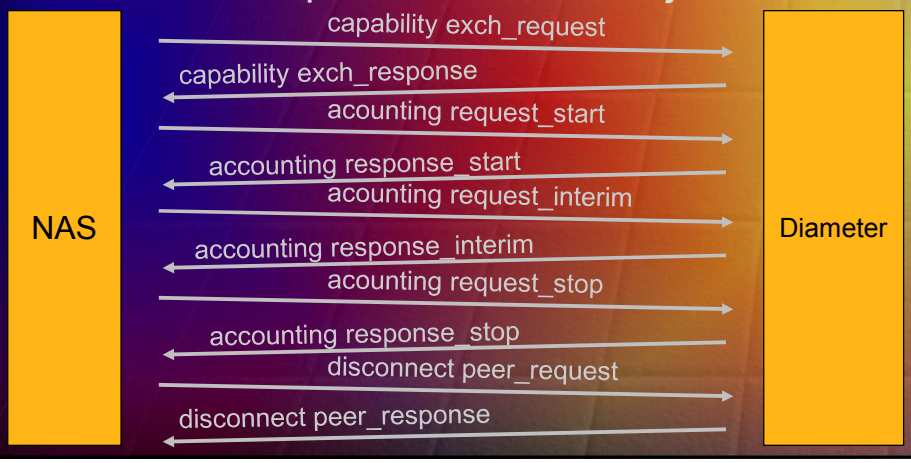
- Diameter – varnost.
  - Pri uporabi TLS mora računalnik, ki je iniciiral povezavo, delovati kot odjemalec, soležni osebek pa kot strežnik TLS, overjanje mora biti opravljeno obojestransko.
  - Po overjanju mora slediti še avtorizacija vseh povezav vzdolžnih poti, predno se začno prenašati dejanska sporočila – s tem preprečimo, da se ta ne bi prenašala prek neustreznih varnostnih področij.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – obračunavanje.
  - Za razliko od RADIUS-a so metode za obračunavanje zaobjete v temeljni specifikaciji Diametra.
  - Bolj podrobno so te metode razdelane v sledečih standardih:
    - Aboba B. et al., Introduction to Accounting Management, RFC 2975, IETF, Reston, oktober 2000.
    - Brownlee N., Blount A., Accounting Attributes and Record Formats, RFC 2924, IETF, Reston, september 2000.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – potek obračunavanja.



Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Primerjava Diameter – RADIUS.
  - Diamter je povezavno usmerjen in tudi sam uporablja zanesljiv prenos (TCP).
  - Diameter podpira proces samo-korekcije napak (angl. fail-over) – če se povezava z nekim agentom, ki obdeluje podatke, podre, se obdelava teh podatkov avtomatsko posreduje drugemu agentu.
  - Sporočila pri Diamatru lahko generira tudi “strežnik”, kar omogoča izboljšave, npr. ponovno overjanje (re-authentication).

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Primerjava Diameter – RADIUS.
  - Pri RADIUS-u strežnik in odjemalec nimata možnosti, da bi oznanila podporo različnih atributov, torej ni možno pogajanje.
  - Diameter zagotavlja varnost in sicer tako na nivoju povezave kot seje.
  - Diameter podpira agente in usmerjanje med domenami – podpora npr. gostovanju!
  - Diameter lahko s pomočjo DNS dinamično išče soležne entitete.

Infrastruktura za overjanje, avtorizacijo in obračunavanje

- Diameter – ključni standardi.
  - Aboba B. et al., Criteria for Evaluating AAA Protocols for Network Access, RFC 2989, IETF, Reston, november 2000.
  - Calhoun P., Diameter Base Protocol, RFC 3588, IETF, Reston, september 2003.
  - Abouba B., Wood J., Authentication, Authorization and Accounting Transport Profile, RFC 3539, IETF, junij 2003.
  - Loughney J., Diameter Command Codes for Third Generation Partnership Project (3GPP), RFC 3589, IETF, september 2003.

Varovanje brezžičnih lokalnih omrežij

- Brezžična lokalna omrežja.
  - Ključna je družina standardov 802.11 organizacije IEEE – ti v bistvu določajo le segment linijskega dostopa (angl. last hop).
  - Standardizacija v okviru odbora IEEE 802 se ni osredotočala na testiranje skladnosti.
  - Problemi z nezdružljivostjo naprav 802.11 pripeljejo do združenja Wi-Fi alliance:
    - Ustanovljena l. 1999, danes ima več kot 200 članov (Cisco, Nokia, Dell, Apple, Sony, MS...).
    - Sprejema nabor testnih specifikacij in certificira združljive proizvode.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Prvi standard na tem področju je bil Wired Equivalent Privacy (WEP).
  - Snovalci so izhajali iz tega, da želijo paralelo ožičenih omrežij Ethernet (IEEE 802.3)
    - kjer je se signal propagira znotraj kabla,
    - s čimer je relativno „zaščiten“ zaradi same fizične ujetosti v medij.
  - Poslanstvo protokola WEP je zato le realizacija omenjene želje - „varno ujeti signal v medij“ (pas na 2.4 in 5 GHz EMS).

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Vzpostavitev sejnih ključev:
    - Izmenjave sejnih ključev v smislu uporabe temu namenjenih kriptografskih protokolov ni.
    - Izmenjava ključev izven seje (angl. out-of-band) - ključi med dostopno točko in postajo se nastavijo ročno.
    - To vodi do nastavitve predvidljivih vrednosti.
    - Vsaka entiteta ima lahko štiri različne ključe, a se ta možnost zaradi praktičnih težav redko uporabljajo.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Overjanje:
    - Pred priklopom v omrežje mora postaja ugotoviti, do katerih omrežij ima pristop in obratno – omrežje mora ugotoviti, ali dana postaja lahko dostopa do omrežja.
    - Dostopne točke (angl. access points) periodično pošiljajo okvire za oznanjanje (angl. beacons), s katerimi oznanjajo obstoj omrežja.
    - Znotraj teh okvirov se nahaja omrežno ime (angl. Service Set Identificator, SSID, ki je do 32 alfa-numeričnih znakov dolg niz).

Varovanje brezžičnih lokalnih omrežij

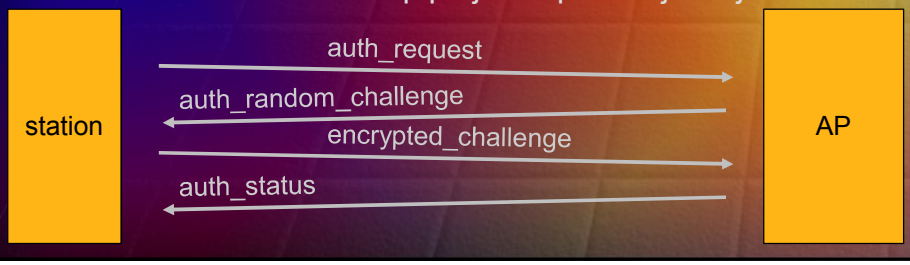
- IEEE 802.11 - varnost.
  - Overjanje:
    - Postaja ima za priklop na voljo dve možnosti – pasivno ali aktivno pregledovanje kanalov.
    - Pri pasivnem pregleduje EMS na možnih frekvenčnih pasovih, pri aktivnem pošlje sama poizvedbo, kjer lahko navede konreten SSID.
    - V primeru prejema več odzivov s strani dostopnih točk se postaja odloči za eno od njih začne postopek overjanja.
    - Postopek overjanja je lahko tipa Open Systems Authentication (OSA) ali Shared Key Authentication (SKA).

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Overjanje - OSA.
    - Je skrajno enostaven in primitiven protokol – v bistvu dovoli dostop poljubni postaji.
    - Postaja, ki se želi priklopiti v omrežje, pošlje zahtevo za “overjanje” dostopni točki, ki v odzivu, v kolikor dovoli postopek OSA, potrdi priključitev.
    - Dostopna točka lahko seveda zavrne zahtevo OSA, če je tako konfigurirana.
    - OSA je dobesedno OPEN system authentication.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Overjanje - SKA.
    - Protokol temelji na principu izziv – odziv.
    - Postaje so razdeljene v dve skupini – tiste, ki imajo dovoljen dostop in tiste, ki ga nimajo, osnova za dostop pa je skupen deljen ključ.



Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Overjanje - SKA.
    - Zahtevi za overjanje sledi izziv, ki je dolg 128 oktetov in je psevdo-naključno število (ta vrednost je dobljena iz naključnega inicializacijskega vektorja in deljenega ključa).
    - Po prejemu postaja kriptira vrednost z deljenim skupnim ključem in ga vrne dostopni točki.
    - Ta dekriptira prejet odziv in ga primerja s poslano vrednostjo.
    - V primeru ujemanja pošlje potrditev, sicer zavrne dostop.

Varovanje brezžičnih lokalnih omrežij

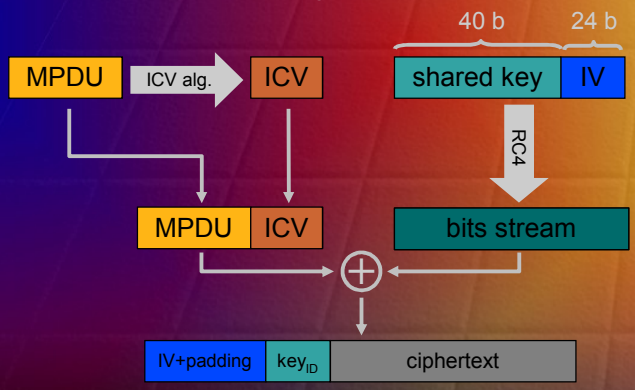
- IEEE 802.11 - varnost.
  - Overjanje – slabosti SKA.
    - Isti ključ si deli z dostopno točko množica postaj.
    - Isti kluč je možno deliti tudi med več dostopnimi točkami.
    - Četudi bi vsaka postaja imela svoj ključ, 802.11 ne omogoča overjanje dostopne točke (v resnici SKA overja le postajo) – poljubna točka se lahko vrine v komunikacijo in sledi celotnemu prometu.
    - SKA pravzaprav temelji na WEP in inherentno podeduje vse njegove slabosti.
    - Minimalna zaščita je, da zahtevamo da postaja pozna SSID oz. da filtriramo naslove MAC.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Protokol WEP - potek:
    - Izračun ICV (angl. Integrity Check Value) preko celotnega okvira (MAC Protocol Data Unit, MPDU).
    - Sledi izbor glavnega ključa izmed štirih možnih ključev.
    - Sledi izbor inicializacijskega vektorja (IV), ki se z operacijo stika doda izbranemu ključu, kar služi kot seme za izračun ključa z uporabo RC4.
    - Izstopni tok bitov iz RC4 se z operacijo XOR aplicira nad MPDU in ICV - enkripcija.
    - Dodajanje glave kriptirani vsebini – 3 okteti vsebujejo IV, en pa podaja ID izbranega ključa.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Zaupnost – enkripcija pri WEP.



Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – slabosti.
    - RC4 je tekoč kripto-algoritem (angl. Stream-cipher), ki deluje v sinhronem načinu.
    - Kriptografski mehanizem kot tak je neprimeren glede na naravo prenosnega medija.
    - Izguba (napaka) v enem samem bitu uniči čistopis od vključno točke z napako dalje.
    - Izguba bitov / okvirov na brezžičnem mediju je pogost pojav zaradi narave samega medija.
    - Blažitev problema z uporabo drugega tekočega ključa za vsak okvir.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – slabosti.
    - Tekoči ključ je izhod algoritma RC4, kjer se uporabli stik IV in glavnega skrivnega ključa.
    - Ker je IV (trije okteti dolžine) v čistopisu dodan v glavi okvira, je za ugotovitev glavnega ključa potrebno le preostalih *n*-3 oktetov.
    - Ker za vsak paket generiramo nov tekoči ključ, s tem izpostavimo glavni ključ, saj je izhod iz RC4 le stik IV in glavnega ključa – več ko je pri istem ključu na voljo pripadajočih tajnopisov, lažji je napad.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP - napad Fluhrer-Mantin-Shamir (FMS):
    - Napad izkorišča iskanje t.i. šibkih ključev.
    - Najbolj enostaven primer šibkega ključa je niz bitov, ki so vsi enaki 0.
    - Po določenem času poteka komunikacije je na voljo dovolj okvirjev, kjer so bili uporabljeni šibki ključi.
    - Dodatna olajšava za napad je dejstvo, da je prvih 8 oktetov tajnopisa glava SNAP (Sub-Network Access Protocol) – XOR paketa in SNAP razkrije del ključa!

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – napad pri uporabi istega ključa:

$$C_1 = P_1 \oplus key_{RC4}$$
$$C_2 = P_2 \oplus key_{RC4}$$
$$C_1 \oplus C_2 = P_1 \oplus P_2$$

    - Če je poznanih dovolj podatkov o P_1 je moč izračunati P_2 (in obratno).
    - Čim poznamo enega od čistopisov, lahko izračunamo ključ in dobimo čistopise ostalih tajnopisov.

Varovanje brezžičnih lokalnih omrežij

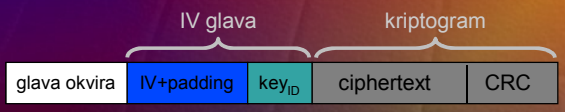
- IEEE 802.11 - varnost.
  - WEP – napad pri uporabi istega ključa:
    - Ključ je dolžine 64 bitov, kjer je 40 bitov fiksnih in pripadajo glavnemu ključu.
    - Spreminja se torej samo IV, kar pomeni, da moramo pri napadu z grobo silo preiskati le 2^{24} različnih vrednosti, da dobimo pravi ključ.
    - Možni ključi pri menjajočem se IV bodo hitro porabljeni – tipičen paket šteje 1500 B, hitrost je 11 Mb/s --> ponavljanje po 18300 sekundah.
    - Standard celo dovoljuje, da je IV ves čas ista vrednost!

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – zagotavljanje celovitosti:
    - Za izračun ICV uporabljamo ciklične redundančne kode (CRC-32), ki niso močan kriptografski mehanizem.
    - CRC nad XOR je linearna operacija:

      $$CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$$

    - Napad na celovitost – struktura okvira WEP:



Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – napad na celovitost:
    - Napadalec želi pravo vrednost X, ki se nahaja v okviru, nadomestiti z vrednostjo Z.
    - Nato izračuna $Y=X \oplus Z$, $X \oplus \mathbf{Y}$ in $CRC(X) \oplus CRC(Y)$.
    - Zatem spremeni okvir iz [X,CRC(X)] v [$X \oplus \mathbf{Y}$, $CRC(X) \oplus CRC(Y)$], kar je enako

      $$[X \oplus \mathbf{Y}, CRC(X \oplus Y)]$$

    - Ampak okvir je vendar kriptiran?!

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – napad na celovitost:
    - Četudi je ICV skupaj s koristno vsebino kriptiran, je napad možen:

$$RC4(K, X \oplus \mathbf{Y}) = RC4(K, X) \oplus \mathbf{Y}$$

in torej tudi

$$RC4(K, CRC(X \oplus \mathbf{Y})) = RC4(K, CRC(X)) \oplus CRC(Y)$$

    - Zgornja notacija (povzeta neposredno po referenčni literaturi) je neeksaktna - RC4(K, X⊕Y) v bistvu pomeni niz operacij XOR nad K (ki je izhod iz PRNG, to je RC4), nad X in nad Y.
    - Kaj je razlog za omenjeno slabost?

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – napad s preusmerjanjem:
    - Problem je tudi dejstvo, da ICV ne ščiti same glave okvira 802.11, kar omogoča nov, banalen napad – napad s presumeritvijo.
    - Predpostavimo, da sta na isti pristopni točki priključeni dve postaji, A in B. A do pristopne točke uporablja WEP, B pa dostopa prek parice – ko A pošlje paket namenjen B, ga pristopna točka dekriptira in pošlje čistopis točki B.
    - Napadalec prestreže okvir, spremeni namembno adreso v glavi okvira na C (ni zaščite celovitosti), ga ponovno odda in prisptopna točka dekriptirano vsebino vroči točki C.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WEP – napad s ponovitvijo:
    - Dodatna možnost je uporaba napada s ponovitvijo (angl. replay attack).
    - Okvire ne glede na vsebino enostavno prestrežemo (brezžični medij) in jih po določenem času nespremenjene ponovno oddamo na medij.
    - Napad je možen, ker PPE (protokolne podatkovne enote, angl. protocol data units, PDUs) protokola WEP ne uporabljajo enoličnih identifikatorjev (časovnih zaznamkov ali naključnih vrednosti).

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Povzetek slabosti WEP:
    - Ni mehanizma za varno (dinamično) izmenjavo ključev prek nevarovanega medija.
    - Uporaba tekočega tajnopisnega postopka, ki zahteva sinhronizacijo med komunicirajočima osebkoma.
    - Zgornjo slabost kompenzira WEP tako, da za vsak PPE uporablja nov ključ, ki ga dobi z enostavnim stikom skrivnega deljenega ključa in IV, kar je uporabljeno kot vhod v generator psevdonaključnih števil, ki je RC4 – možnost napada z metodo FMS.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Povzetek slabosti WEP:
    - Glavni ključ je običajno vnešen ročno, zato je to časovno statična vrednost in spreminja se le IV pri generiranju sprotnega ključa, kar pomeni le 2^{24} različnih ključev – a standard dovoljuje celo, da je sprememba IV opcijska!
    - Za zagotavljanje celovitost se uporablja CRC-32, ki kriptografsko močan.
    - ICV ne ščiti celovitosti celotnega podatkovnega okvira.
    - Overjanje je le enosmerno – pristopna točka overi postajo, obratno ni možno.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Nov standard namesto WEP - 802.11i/WPA.
    - Izhodiščni problem je uporaba obstoječe strojne opreme, ki je podpirala WEP.
    - Skupina v okviru IEEE se je odločila za nov standard 802.11i z AES, ki pa ni vzvratno združljiv z WEP, a potrebna je vzvratno združljiva rešitev.
    - V tej situaciji vstopi Wi-Fi Alliance, ki specificira Temporal Key Integrity Protocol (TKIP) tako da ohrani obstoječo 802.11 infrastrukturo – to je pozano tudi kot Wi-Fi Protected Access ali WPA.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Nov standard namesto WEP - 802.11i/WPA.
    - WPA pokriva upravljanje ključev in overjanje (kar podaja standard 802.11X) in je predhodnik 802.11i.
    - Standard 802.11i je poznan tudi kot WPA2, ki uporablja AES – za razliko od WPA, ki podpira le TKIP (in algoritem Michael za MIC).
    - 802.11i loči brezžična omrežja na tista za domačo uporabo in tista za poslovno uporabo – za slednjo zahteva infrastrukturo za overjanje.
    - 802.11i za domačo uporabo omogoča vzpostavitev ključev „izven pasu“.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Nov standard namesto WEP - 802.11i/WPA.
    - Za kompenzacijo šibkosti WEP doda WPA še en sloj v hierarhijo ključev, da zaščiti glavni ključ.
    - Hierarhija ključev WEP je dvonivojska, pri WPA pa večnivojska.
    - Izhodišče hierarhije je glavna skrivnost (angl. master secret, MS), iz katere izračunamo glavni ključ za vsak par komunicirajočih osebkov (angl. pair-wise master key, PMK). Iz tega ključa izvedemo prehodni ključ za vsak par (angl. pair-wise transient key, PTK) in iz njih končno ključ za enkripcijo posamezne PPE.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Standard 802.11i / WPA.
    - Standard je zasnovan okrog seje, kjer seja označuje posamezno povezavo med pristopno točko in postajo (vsak nov pristop šteje kot seja).
    - PMK je dolžine 256 bitov.
    - PTK se generira na začetku vsake seje in označuje nabor štirih sejnih ključev od katerih je vsak dolžine 128 bitov; prvi služi enkripciji podatkov, drugi zagotavljanju celovitosti, tretji enkripciji ključev EAPoL (Extensible Authentication Protocol over LAN) in četrti zagotavljanju celovitosti ključev EAPoL.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Standard 802.11i / WPA.
    - Po vzpostavitvi seje se tranzietne ključe izračuna kot (PRF pomeni pseudo-random function)

PTK=PRF-512(PMK, “pair-wise key expansion”, AP_MAC || STA_MAC || ANonce, SNonce)

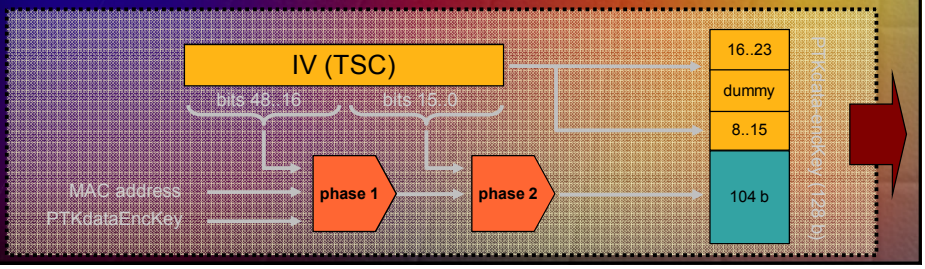
    - PTK je rezultat uporabe tudi naslovov MAC, s čimer so sejni ključi vezani na strojne naslove.
    - Različne sejne ključe za vsako povezavo dosežemo z vključevanjem vrednosti za enkratno uporabo (angl. nonce / NumberONCE):

ANonce=PRF-256(RandNum,“init-counter”,AP_MAC ||time)

SNonce=PRF-256(RandNum,“init-counter”,STA_MAC ||time)

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Standard 802.11i / WPA.
    - Vrednosti PTK lahko pristopna točka in postaja izračunata vzporedno in neodvisno po opravljeni izmenjavi enkratnih vrednosti in naslovov MAC.
    - Za ključe za kriptiranje paketov služi mešanje ključev (TSC pomeni TKIP Sequence Counter):



Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Standard 802.11i / WPA.
    - Algoritem mešanja ključev uporablja strojno opremo, razvito za WEP (združljivost!).
    - IV je dolg 48 b in faza 1 uporablja prvih 32 (MSB) bitov, ki pa se spreminjajo le na vsakih 65536 PPE; ker je ta faza procesno zahtevna (zgoščevalna funkcija treh parametrov) je tako zmanjšana obremenitev – faza 2 je računsko bistveno manj zahtevna.
    - Zaradi “mešanja“ napadalec težko najde povezavo med IV in ključem za kriptiranje posamezne PPE (per-packet key).

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Standard 802.11i / WPA - zaupnost:
    - WEP je imel IV dolžine le 24 bitov, za katerega niti ni bilo obvezno spreminjanje.
    - TKIP ima IV dolg 48 bitov tako da čas za kolizijo (pojav paketa z istim IV) namesto nekaj ur traja več sto let – v resnici je IV dolg 56 bitov, a uporablja se jih 48, osem pa jih služi za preprečevanje šibkih ključev.
    - Mešanje ključev oteži iskanje povezave med ključem za kriptiranje paketa in IV, hkrati pa je izvedljivo na strojni opremi za WEP.

Varovanje brezžičnih lokalnih omrežij

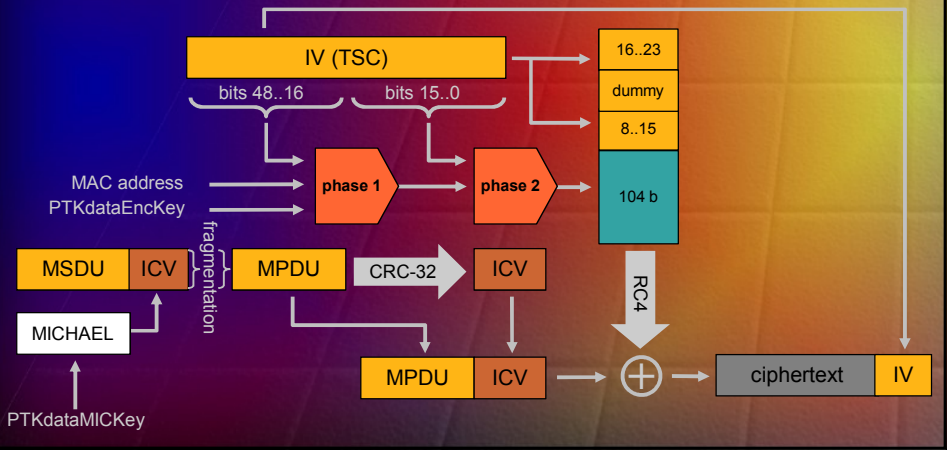
- IEEE 802.11 - varnost.
  - Standard 802.11i / WPA - celovitost:
    - Uporaba CRC-32 pri WEP nima kriptografske trdnosti – želja snovalcev je bila enostavnost (hitrost) računskih operacij.
    - Algoritmi za izračun MIC/ICV običajno zahtevajo veliko množenj, ki je računsko zahtevna operacija – novi algoritem pri TKIP je MICHAEL.
    - Algoritem MICHAEL uporablja le seštevalnike in pomične registre in jih je moč izvesti na obstoječih sistemih WEP.
    - PPE ima tako dve vrednosti MIC/ICV – prva je stari CRC-32, druga pa izhod alg. MICHAEL.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - Standard 802.11i / WPA - celovitost:
    - Algoritem MICHAEL je kompromis in ni tako kriptografsko močan kot SHA-1 ali MD5 (slednja sta računsko prezahtevna za realizacijo na strojni opremi za WEP).
    - S tem je namerno dopuščena lažja možnost poneverb celovitosti, zato TKIP v primeru, ko v eni sekundi zazna dve prejeti vrednosti MIC, ki se ne ujemata z izračunanimi vrednostmi, izbriše vse ključe, prekine sejo in počaka eno minuto, preden ponovno vzpostavi sejo.
    - Pri WPA se mora IV z vsako novo PPE ("paketom") inkrementalno povečati.

Varovanje brezžičnih lokalnih omrežij

- WPA – celovitost in zaupnost.

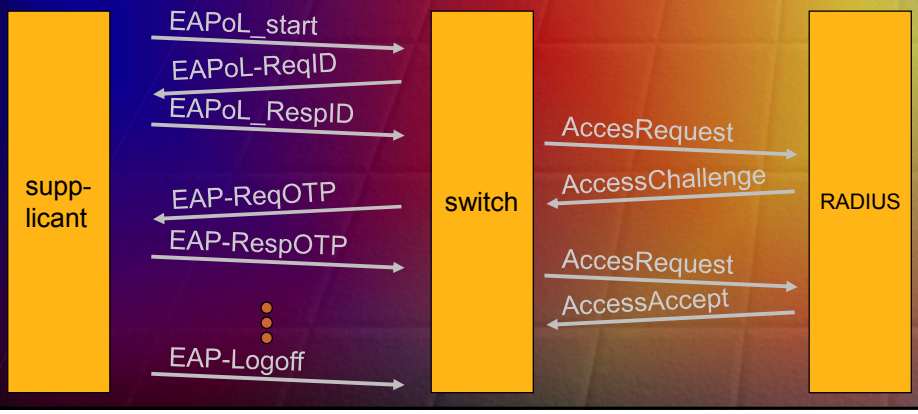


Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WPA – overjanje:
    - Za overjanje uporablja Extensible Authentication Protocol over LAN (EAPoL).
    - EAPoL uporablja tri entitete: prosilca, overilca in overilni strežnik.
    - Overilec na podlagi odziva overilnega strežnika omogoči ali prepreči dostop do omrežja.
    - Zasnova protokola EAPoL predvideva vključitev sklopov AAA – tipično je to RADIUS.

Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11 - varnost.
  - WPA – overjanje / potek EAPoL:



Varovanje brezžičnih lokalnih omrežij

- IEEE 802.11i (WPA 2).
  - WPA je bil podmnožica specifikacije 802.11i, od katere je skoraj v celoti prevzel upravljanje ključev in zato tudi WPA 2 nima bistvenih sprememb.
  - Overjanje pri WPA 2 je enako kot pri WPA.
  - Za zaupnost in celovitost WPA 2 uporablja bistveno boljši algoritem – Advance Encryption Standard (AES).

Formalne metode

- Formalne metode (FM) so metode za specifikacijo in razvoj rač. sistemov, ki največkrat temeljijo na logiki, diskretni matematiki in gramatikah.
- Področja namembnosti so:
  - podajanje specifikacij,
  - načrtovanje,
  - analiza,
  - validacija in verifikacija.
- FM zahtevajo eksplicitno podajanje predpostavk in sklepanja na podlagi relativno majhne množice pravil.

Formalne metode

- Prednost FM je zmanjševanje takih vrst sklepanja (in na njih temelječih zaključkov), ki so posledica (le) intuicije.
- FM lahko omogočajo mehansko preverjanje, kar je zelo primerno za analizo računalniških sistemov (strojnih in programskih sklopov).
- Velik pomen formalnih metod na področju varnosti, zlasti kriptografskih protokolov.

Formalne metode

- Metoda R. Rueppel-a:
  - služi razvoju kriptografskih protokolov;
  - primerna kot uvodna metoda za pedagoške namene (povezava z gramatikami);
  - temelji na jeziku, ki omogoča podajanje varnostne arhitekture kot niza “besed”;
  - dizajniranje varnostne arhitekture postane pravzaprav problem generiranja ustreznega niza “besed” v jeziku;
  - analiza varnostne arhitekture postane problem razčlenjevanja niza in ugotavljanja, ali pripada jeziku (parsing).

Formalne metode

- Metoda R. Rueppel-a:
  - Predpostavlja, da sta fundamentalni varnostni storitvi overjanje in zaupnost.
  - Osnova modeliranja sta zato zaupni kanal in overovitveni kanal.
  - Podpira tudi iskanje odgovorov na vprašanja:
    - Kakšne dizajnerske možnosti so na voljo na določenem nivoju načrtovanja varnostne arhitekture?
    - Kakšne so posledice določenega izbora v smislu kompleksnosti upravljanje ključev?
    - Kdaj je arhitektura dorečena?

Formalne metode

- Metoda R. Rueppel-a - temeljni principi:
  - Predpostavimo simetričen kanal:

    $Secu(N^2) \rightarrow sym(secu, N^2), Secu(N^2),$

    kjer
  - $Secu(N^2)$ na levi podaja cilj ščitenja N^2 podatkovnih kanalov, $sym(secu, N^2)$ podaja uporabo simetričnega tajnopisnega mehanizma, $Secu(N^2)$ na desni pa podaja zahtevo po ščitenju N^2 ključev.
  - Varnostni cilj na levi strani produkcije implicira izpolnitev zahtev na desni strani produkcije.

Formalne metode

- Podrobnosti metode R.Rueppla:
  - končni (terminalni) simboli predstavljajo varnostne mehanizme in jih podajamo z malo začetnico;
  - neterminalni simboli predstavljajo varnostne cilje (storitve) in jih podajamo z veliko začetnico;
  - pravila (produkcije) gramatike podajajo možne načine relizacije ciljev.

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Porazdeljeni varnostni cilji:
    - *Auth*(*N*) označuje (enosmerni) individualni overovitveni kanal, ki je pridružen vsakemu udeležencu in v katerega lahko le piše, vsakdo pa lahko iz njega le bere.
    - *Conf*(*N*) označuje (enosmerni) zaupni individualni kanal, ki je pridružen vsakemu udeležencu in iz katerega lahko ta le bere, vsakdo pa lahko vanj piše.
    - *Secu*(N^2) označuje individualni varni kanal, ki povezje vsak par udeležencev:

$$Secu(N^2) \rightarrow Auth(N), Conf(N)$$

(zagotavljanje individualnega varnega kanala je ekvivalentno zagotavljanju ind. kanala za overjanje in ind. kanala za zaupnost)

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Varnostni cilji, ki vključujejo zaupanja vreden center (angl. trusted authority, TA):
    - *Auth*(*ta*,1) označuje centraliziran overovitveni kanal, ki je pridružen TA, iz katerega lahko bere vsakdo, piše vanj pa le TA.
    - *Conf*(*ta*,1) označuje centraliziran zaupni kanal, ki je pridružen TA, iz katerega lahko bere le TA, piše vanj pa lahko vsakdo.
    - *Secu*(*ta*,*N*) označuje centraliziran varni kanal, ki si ga TA deli z vsakim posameznim udeležencem (za vsakega udeleženca tvori po en kompozitni kanal).

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Varnostni cilji, ki vključujejo zaupanja vreden center (angl. TA):
    - Na podlagi definicije *Secu*(*ta*,*N*) sledi
      $$Secu(ta,N) \rightarrow Auth(ta,N), Conf(ta,N)$$
    - *Auth*(*ta*,*N*) označuje individualen overovitveni kanal proti TA, ki je pridružen vsakemu udeležencu, ki lahko vanj piše, iz njega pa lahko bere le TA.
    - *Conf*(*ta*,*N*) označuje individualen zaupni kanal od TA, ki je pridružen vsakemu udeležencu, ki lahko iz njega bere, vanj pa lahko piše le TA.

Formalne metode

- Podrobnosti metode R.Rueppla - elementarni kanali in konstrukti:
  - Fizični kanal - sporočilo je zaščiteno s fizičnim načinom ščitenja (kurirji, optični kabli,...).
  - Simetrični kanal - sporočilo je zaščiteno s pomočjo simetričnega tajnopisnega postopka.
  - Asimetrični kanal - sporočilo je zaščiteno s pomočjo asimetričnega tajnopisnega postopka.

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Fizični kanal:
    - Za označevanje sistema z varnim fizičnim kanalom med vsakim parom udeležencev uporabimo notacijo $phys(secu, N^2)$ - ustrezna produkcija je

      $$Secu(N^2) \rightarrow phys(secu, N^2)$$

    - Fizični kanal je moč uporabljati tudi samo za overjanje, npr. CD-R, in to označimo s $phys(auth, N)$, kar pomeni sistem s fizičnim overovitvenim kanalom, ki je pridružen vsakemu udeležencu - ustrezna produkcija je

      $$Auth(N) \rightarrow phys(auth, N)$$

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Simetrični kanal - osnovna dejstva:
    - Za doseganje zaupnosti kriptiramo sporočilo *M* z uporabo simetričnega algoritma in kripto ključa *K*: $\{M\}_K$.
    - Za doseganje overjanja uporabimo simetričen ključ *K* in z njim tvorimo kodo za overjanje sporočila - KZOS (angl. message authentication code - MAC): *M, MAC(K,M).*
    - Za hkratno overjanje in zaupnost je potrebno uporabljati dva različna ključa, še bolje pa tudi različna algoritma.

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Mehanizem Simetrični kanal (*sym*()):
    - *sym*(*secu*, N^2) označuje simetričen sistem, ki nudi simetričen varni kanal med vsakim parom udeleženecev;
    - *sym*(*secu*, *N*) označuje centraliziran simetričen sistem, ki nudi simetričen varni kanal med centrom in vsakim udeležencem;
    - poznavanje ključa implicira sposobnost branja iz in pisanja v varen simetrični kanal.

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Mehanizem Simetrični kanal (*sym*()).
    - Pri uporabi simetričnega kanala za dosego varnosti imamo problem varnega porazdeljevanja ustreznih ključev:
      $Secu(N^2) \rightarrow sym(secu, N^2), Secu(N^2)$
      Za vzpostavitev varnih kanalov med vsakim parom izmed N udeležencev (cilj na levi) lahko uporabimo simetrični kanal (cilj na desni), a moramo zagotoviti varen kanal med vsakim parom za distribucijo ključev (cilj na desni).
    - Analogno dobimo (porast kompleksnosti!):
      $Conf(N) \rightarrow sym(secu, N^2), Secu(N^2)$
      $Auth(N) \rightarrow sym(secu, N^2), Secu(N^2)$

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Mehanizem Asimetričen kanal (*asym*()):
    - Za dosego zaupnosti pri asimetričnem kanalu pošiljatelj kriptira sporočilo M z javnim ključem prejemnika Kj: $\{M\}_{Kj}$.
    - Za dosego overjanja pri asimetričnem kanalu pošiljatelj kriptira sporočilo M s svojim privatnim ključem Kp (kar je dig. podpis): $\{M\}_{Kp}$.
    - *asym*(*mode*,*N*) podaja asimetričen sistem, ki vsakemu uporabniku priredi lasten asimetričen kanal (*mode* je lahko *auth* ali *conf* ali *secu*).

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Mehanizem Asimetričen kanal (*asym*()).
    - Temeljne produkcije:

      $Conf(N) \rightarrow asym(conf, N), Auth(N)$

      $Auth(N) \rightarrow asym(auth, N), Auth(N)$

      Novi cilj $Auth(N)$ na desni označuje problem overjenega porazdeljevanja javnih ključev.
    - Varni kanal dobimo s kompozicijo dveh asimteričnih kanalov - najprej pošiljatelj podpiše sporočilo, nato pa ga kriptira s prejemnikovim javnim ključem:

      $Secu(N^2) \rightarrow asym(secu, N), Auth(N)$
    - Novi cilj $Auth(N)$ na desni pomeni overjeno porazdelitev javnih ključev udeležencev.

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Mehanizem Zaupanja vreden center (*ta*()):
    - *ta*(*secu*, *N*) - center je vreden zaupanja za varno manipulacijo skrivnosti;
    - *ta* (*auth*, *N*) - center je vreden zaupanja za overjeno manipulacijo podatkov udeležencev;
    - *ta* (*conf*, *N*) - center je vreden zaupanja za zaupno manipulacijo podatkov udeležencev.
  - Varni kanali v cent. okolju (back & forth relay):

    $Secu(N^2) \rightarrow ta(secu, N), Secu(ta,N)$
    - Varni kanali med udeleženci potekajo preko varnih kanalov s centrom.

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Primer storitve overjanja (zaupnosti) med *N* udeleženci z uporabo mehanizma *ta*() (back & forth relay).
    - Prvi korak:

      $Auth(N) \rightarrow Auth(ta, N), ta(auth,N), Auth(ta,1)$

      $Conf(N) \rightarrow Conf(ta, 1), ta(conf,N), Conf(ta,N)$
    - Drugi korak:

      $Auth(ta, 1) \rightarrow asym(auth, 1)$

      $Conf(ta, 1) \rightarrow asym(conf, 1), Auth(ta,1)$
    - *Auth*(*ta*, 1) pomeni overjeno porazdeljevanje javnega ključa TA vsem udeležencem.

Formalne metode

- Podrobnosti metode R.Rueppla.
  - Kompozitni konstrukti - okolje s certifikati:
    - Uporabnik registrira javni ključ.
    - TA podpiše javni ključ uporabnika s svojim privatnim ključem.
    - Certifikat je dostopen vsem uporabnikom.
    - Modeliranje certifikacijskega kanala z gramatičnim pravilom:

      $Auth(N) \rightarrow phys(auth,N), ta(auth,N), asym(auth,1), Auth(ta,1)$

Sistem z *N* overjenimi javnimi ključi vzpostavimo z *N* fizičnimi kanali za overjanje napram TA, ki porazdeli te javne ključe prek asimetričnega kanala za overjanje, vendar pa je potrebno realizirati nov cilj, to je overjeno porazdelitev javnega ključa TA vsem udeležencem.

Formalne metode

- FM R.Rueppla - primer načrtovanja.
  - Dizajnirajmo arhitekturo z N udeleženci, ki zagotavlja njihovo overjanje.
  - Predpostavimo, da želimo zasnovati našo arhitekturo na simetrični kriptografiji, vendar ostane odprto vprašanje porazdeljevanja ključev.
  - Primer izvedbene možnosti s TA:

$$Auth(N) \rightarrow sym(secu, N^2), Secu(N^2)$$
$$Secu(N^2) \rightarrow asym(secu, N), Auth(N)$$
$$Auth(N) \rightarrow$$
$$phys(auth, N), ta(auth,N), asym(auth,1), Auth(ta,1)$$
$$Auth(ta, 1) \rightarrow phys(auth, 1)$$

Formalne metode

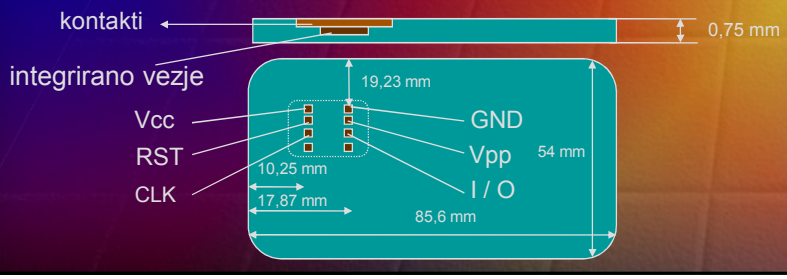
- Imamo sledeč protokol za vzpostavitev varnih kanalov (overjanje in zaupnost):
  - A in B želita vzpostaviti varno sejo in izbereta skrivna ključa k_1 in k_2.
  - Oba kriptirata skrivna ključa z javnim ključem TA in ga pošljeta TA.
  - TA dekriptira ključa, izbere sejni ključ k_s, ga kriptira z k_1 in k_2 ter pošlje A in B.
  - A in B s skrivnima ključema dekriptirata sejni ključ in vzpostavita *secu* kanal.
- Ali zgoraj navedeni protokol zagotavlja overjanje in zaupnost?

VARNOSTNI MEHANIZMI IN TEMELJNI VARNOSTNI TEHNIČNI GRADNIKI

VARNOSTNI MEHANIZMI
IN TEMELJNI VARNOSTNI
TEHNIČNI GRADNIKI

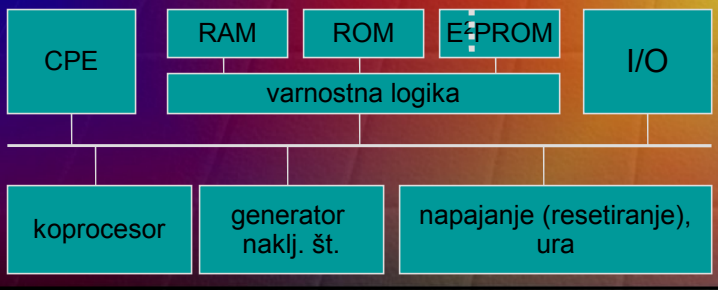
VARNOSTMI MEHANIZMI - pametne kartice

- Pametne kartice (angl. smart cards).
  - Pametne kartice so kartice, ki vsebujejo mikrokontroler in ustrezajo standardom ISO 7816, od 1 do 11 (kartice s kontakti).
  - Standradi ISO so osnova za specifikacije skupine EMV (Europay, MasterCard in VISA).



Pametne kartice

- Pametne kartice - strojna arhitektura.
  - Najpogostejša osnova Motorola 6805 / Intel 8051.
  - Varnostna logika - nadzor dostopa do pomnilniških lokacij (preprečevanje večanja vrednosti določenih spominskih lokacij, “address scrambling”, itd).

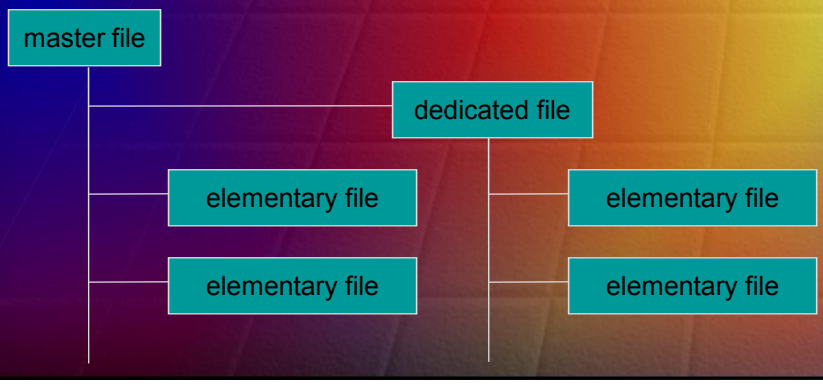


Pametne kartice

- Pametne kartice - strojna arhitektura.
  - Integrirano vezje najpogosteje CMOS z napajanjem med 2,2 V in 5,5 V, frekvenca 5 MHz.
  - ROM - vsebuje COS (Card Op. System).
  - PROM - serijska številka kartice (do 32 bytov).
  - E^2PROM - hranjenje podatkov, življenjska doba 10.000 pisanj / brisanj oz. 10 let, prostorsko in energetsko zelo “potraten”.
  - RAM - delovni pomnilnik.
  - Zaščita: spominske celice najgloblje v substratu, metalizacijska plast proti elektronski mikroskopiji, detekcija nižjih hitrosti ure, varnostna logika.

Pametne kartice

- Pametne kartice - struktura datotek.
  - Hierarhija datotek, dostop do EF prek DF in MF, kjer je nadzor dostopa in kontrolni podatki.

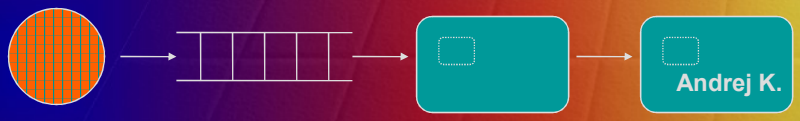


Pametne kartice

- Pametne kartice - vhod / izhod.
  - Komunikacijo definira ISO 7816 - 3:
    - znakovno usmerjena (character oriented),
    - bločno usmerjena (block oriented),
    - sinhrona ali asinhrona,
    - dvosmerna komunikacija prek I/O.
    - Najpogosteje je v uporabi znakovno usmerjena asinhrona komunikacija - hitrost določi terminal (clock) in delilniki frekvence na kartici. Terminal kartico aktivira z Vcc in RST in kartica odgovori ATR (Answer To Reset), ki vsebuje tip kartice in način komunikacije.

Pametne kartice

- Proces proizvodnje pametne kartice.



polprevodniški substrat | ID proizvajalca, tip vezja, ser. št. | ID vgrajevalca, ključ kartice | vnos podatkov in aplikacijskega ključa

izdelava mikrokontrolerjev | identifikacija in pakiranje | montaža | personalizacija

Pametne kartice

- Finančne transakcije – spolšen model EMV.

Pametne kartice

- Pametne kartice - overjanje.
  - Statično - kartica ima vgrajene certifikate in podpise, ne izvaja kriptoprocesiranja.
    - Kartica pošlje podatke in digitalni podpis.
    - Problem verne poneverbe pod.na drugi kartici.
  - Dinamično:
    - Terminal da izziv (naključen niz) in kartica s privatnim ključem izračuna ustrezen odziv.
    - Problem točne poneverbe kartice (strukturne).
  - Overjanje lastnika: PIN, biometrika.

Pametne kartice

- Pametne kartice - aplikacije.
  - Elektronske denarnice in mikroplačilni sistemi (IBM μiKP) - plačevanje parkirnin, telefonskih pogovorov, prevozov.
  - Medicinske aplikacije (KZZ).
- Rast tržišča (vir IDC Corp.):
  - 430 milijonov enot v l. 1999,
  - 610 milijonov enot v l. 2000 (ocena).
- Trendi:
  - kripto podpora (koprocesorji),
  - kartice JAVA (Open Card Framework - Gemplus, Schlumberger).

Teoretični temelji

Information theory

- Information theory addresses two related problems: the noisy channel and the secret channel problem. In both cases an original message M is sent over a communication channel and recieved as M'.
- In case of noisy channel the problem is how to restore a distorted message (which is achieved by addition of redundant bits, i.e. error control codes).
- In case of secret channel the noise corresponds to enciphering information and received message M' to ciphertext. The role of the cryptanalyst is similar to the role of the receiver in the noisy channel problem, while the role of the sender is to make message recovery infeasible.

Teoretični temelji

Information theory

- The amount of information in a message is measured by the average number of bits needed to encode all possible messages in an optimal encoding.
- The amount of information in a message is formally measured by the entropy of the message, which is a function of the probability distribution over the set of all possible message.

Definition Let $X_1, \ldots, X_n$ denote n possible messages occurring with probabilities $p(X_1), \ldots, p(X_n)$, where $\sum_i p(X_i) = 1$. Then entropy of a given message is defined by the weighted average

$$H(X) = -\sum_i p(X_i) \log_2 p(X_i)$$

or writing this as a sum taken over all messages X

$$H(X) = -\sum_X p(X) \log_2 p(X) \text{ or}$$
$$H(X) = \sum_X p(X) \log_2 (1/p(X)).$$

Teoretični temelji

Information theory

- The number of bits needed to encode message X in an optimal way (i.e. which minimizes the expected number of bits to be transmitted) is represented by term $\log_2(1/p(X))$.
- Because $(1/p(X))$ decreases with increasing $p(X)$, frequently occurring messages are assigned shorter codes, while longer ones are assigned to infrequent messages.
- The weighted average $H(X)$ gives the expected number of bits in optimally encoded messages.

Example Let $n = 3$, and let 3 messages be A, B and C, where $p(A) = 0,5$ and $p(B) = p(C) = 0,25$. Then $\log_2(1/p(A)) = 1$ and $\log_2(1/p(B)) = 2 = \log_2(1/p(C))$. Therefore

$$H(X) = (1/2)\log_2 2 + 2((1/4)\log_2 4) = 0,5 + 1 = 1,5.$$

Teoretični temelji

Information theory

Discussion of the example.

- An optimal encoding assigns a 1-bit code to A and 2-bit codes to B and C. A can be encoded with 0, and B with 10 and C with 11.
- This encoding is optimal - any other encoding would require at least 1,5 bits per letter.
- Encoding of a sequence ABAACABC would be 010001101011.
- B or C can not be encoded with one bit, as there would be overlapping with encoding of A. For example, if B is encoded with 1, then 11 would mean two Bs or one C. It is however possible to separate letters with spaces, but these spaces must be encoded again in computers, therefore excessive use of resources is needed.

Teoretični temelji

Information theory

Example Suppose all messages are equally likely, thus $p(X_i) = 1/n$ for $i = 1, \ldots, n$. Then $H(X) = n((1/n)\log_2 n) = \log_2 n$. Thus $\log_2 n$ bits are needed to encode each message. For $n = 2^k$ the number of needed bits is k.

Facts about entropy:

- Given n, entropy is maximal for $p(X_1) = \ldots = p(X_n) = 1/n$. This happens when all messages are equally likely.
- $H(X)$ decreases as the distribution of messages becomes more skewed, reaching a minimum $H(X) = 0$ at $p(X_i) = 1$ for some message X_i.
- Thus entropy of a message measures its uncertainty in that it gives the number of bits of information that must be learned when the message has been distorted by noise or enciphering.

Teoretični temelji

Information theory

Example Suppose an attacker knows that the ciphertext F&$KLM corresponds to plaintext MALE or FEMALE - the uncertainty is one bit (an attacker needs to determine only e.g. the first character).

Example Suppose an attacker knows that some ciphertext corresponds to a salary, then the uncertainty is more than one bit, but not more than $\log_2 n$ bits, where n is the upper bound for salaries.

Example (the vulnerability of public key cryptosystems when used for secrecy). Let $M' = (M)_{K_{pub}}$ present encrypted message with the public key K_{pub}. Even if private deciphering is computationally infeasible, it is possible to attack the system if an attacker knows that the ciphertext is a salary, an integer less than 1 M USD. This means he / she has to perform (in the worst case) operations $M' = M'_i$ for $i = 1, \ldots, 1000000$ to find the match. To prevent this kind of attacks, a random bit string can be appended before enciphering.

Teoretični temelji

Information theory

Let us assume a certain language:

- Consider the set of all messages X that are N characters long. The rate of language r is defined by $r = H(X)/N$, which gives the average number of bits of information in each character. For large N and English language, this is 1,0 to 1,5 bits/letter.
- The absolute rate of the language is defined to be the maximum number of bits of information that could be encoded in each character assuming all possible sequences of characters are equally likely. If there are L characters in the language, then the absolute rate is given by $R = \log_2 L$, the maximum entropy of the individual character. For English, this is $R = \log_2 26 = 4,7$bits/letter.
- The redundancy of a language with rate r and absolute rate R is defined by $D = R - r$. For $R = 4,7$ and $r = 1, D = 3,7$ (all units b/letter), whence the ratio D/R is approx. 79%.

Teoretični temelji

Information theory

One may reduce the uncertainty of messages with additional info.

Example Suppose X is a 32 bit integer with all values to be equally likely. Thus the entropy is $H(X) = 32$. Suppose we learn that X is even. Then the entropy is reduced by one bit, because LSB must be 0.

Given a message $Y \in \{Y_1, \ldots, Y_m\}$, where $\sum_{i=1}^{i=m} p(Y_i) = 1$, let $p_Y(X)$ denote conditional probability of message X given message Y (i.e. $P(X \mid Y)$, and let $p(X, Y)$ be joint probability of message X and message Y, thus $p(X, Y) = p_Y(X)p(Y)$.

Definition The equivocation is the conditional entr. of X given Y:

$$H_Y(X) = -\sum_{X,Y} p(X, Y) \log_2 p_Y(X),$$

which can be rewritten as

$$H_Y(X) = \sum_{X,Y} p(X, Y) \log_2(1/p_Y(X)) \text{ or}$$
$$H_Y(X) = \sum_Y p(Y) \sum_X p_Y(X) \log_2(1/p_Y(X)).$$

Teoretični temelji

Information theory

Example Let $n = 4$ and $p(X) = 1/4$ for each message X. Thus $H(X) = \log_2 4 = 2$. Now let $m = 4$ and $p(Y) = 1/4$ for each message Y. Suppose that each message Y narrows the choice of X from four to two messages, where both messages are equally likely:

$$Y_1 : X_1 \text{ or } X_2,\ Y_2 : X_2 \text{ or } X_3,\ Y_3 : X_3 \text{ or } X_4,\ Y_4 : X_4 \text{ or } X_1.$$

Thus for each Y, $p_Y(X) = 1/2$ for the two X's and $p_Y(X) = 0$ for the remaining two X's. The equivocation is thus

$$H_Y(X) = 4[(1/4)2((1/2)\log_2 2)] = \log_2 2 = 1.$$

Thus the knowledge of Y reduces the uncertainty of X to one bit, corresponding to the remaining two choices for X.

Teoretični temelji

Information theory

Perfect secrecy According to Shannon and his study of information theoretic properties regarding cryptographic systems, there are three classes of information:

1. Plaintext messages M occurring with prior probabilities $p(M)$, where $\sum_M p(M) = 1$.
2. Ciphertext messages C occurring with probabilities $p(C)$, where $\sum_C p(C) = 1$.
3. Keys K chosen with prior probab. $p(K)$, where $\sum_K p(K) = 1$.

Definition Let $p_C(M)$ be the probability that message M was sent given that C was received (C is the encryption of M). Perfect secrecy is defined by the condition $p_C(M) = p(M)$, which means that intercepting the ciphertext gives an attacker no additional information.

Teoretični temelji

Information theory

Perfect secrecy (PS) Let $p_M(C)$ be the probability of receiving ciphertext C given that M was sent. Then $p_M(C)$ is the sum of the probabilities $p(K)$ of the keys K that encipher M as C:

$$p_M(C) = \sum_{\substack{K \\ E_K(M)=C}} p(K)$$

A necessary and sufficient condition for **PS** is that for every C,

$$p_M(C) = p(C) \text{ for all } M.$$

Interpretation The probability of receiving a particular ciphertext C given that M was sent (encrypted under some key) is the same as the probability of receiving C given that some other message M' was sent (encrypted under a different key). Perfect secrecy is possible using random keys at least as long as the messages they encipher.

Teoretični temelji

Information theory

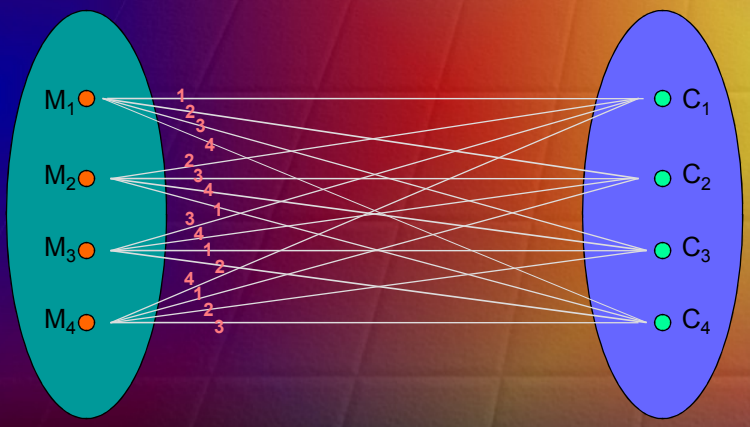
Example Assume 4 messages, all equally likely, and four keys, all equally likely. $P_C(M) = P(M) = p_M(C) = p(C) = 1/4$, for all M and C. Intercepting one of the ciphertexts $C_1, \ldots, C_4$ would give no hint to determine which of the four keys was used and, therefore, which the correct message is: M_1, M_2, M_3, or M_4.

Perfect secrecy requires that the number of keys must be at least as great as the number of possible messages. Otherwise there would be some message M, such that for a given C, no K deciphers C into M, implying $P_C(M) = 0$. An attacker would thereby eliminate certain possible plaintexts, which increases the chances of breaking the cipher.

One-time pad This cipher achieves perfect secrecy by deploying non-repeating random key stream that is as long as the message stream is.

Teoretični temelji

- Shema idealnega tajnopisnega postopka.



Teoretični temelji

Information theory

It follows that statistical analysis is in the heart of cryptanalysis. To make it as hard as possible, Shannon suggests the following:

- Remove some of the redundancy of the language before encryption (use e.g. file compression).
- Use confusion, which involves substitutions that make the relationship between the key and ciphertext as complex as possible. This makes the relationship between the statistics of the ciphertext and encryption key as complex as possible.
- Use diffusion, which involves transformations that dissipate the statistical properties of the plaintext across the ciphertext. This means that each plaintext digit affects value of many ciphertext digits and prevents attempts to deduce the key.

Teoretični temelji

Classical Crypto Systems - CCS

Substitutions - characters of plaintext are replaced by other characters. There are two families: monoalphabetic and polyalphabetic.

An example of monoalphabetic substitution:

plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z
ciphertext: d e f g h i j k l m n o p q r s t u v w x y z a b c

Polyalphabetic substitutions work as follows: A set of different monoalphabetic substitution rules is determined. Afterwards, a particular sequence of these rules is applied to the plaintext sequence.

Example: use for the first 10 bits rule no. 1, then for the second 10 bits rule no. 2, then for the third 10 bits again rule no. 1 and so on.

Attacks on monolaphabetic substitutions - counting the frequency of letters and knowing the language properties (this is much harder with polyalphabetic substitutions).

Teoretični temelji

Classical Crypto Systems - CCS

With transpositions one performs permutation on the group of plaintext letters, e.g. by writing plaintext in a rectangle and by permuting the order of columns.

An example of transposition:

plaintext:

t	h	i	s
i	s	s	i
m	p	l	e
t	e	x	t

ciphertext:

h	t	s	i
s	i	i	s
p	m	e	l
e	t	t	x

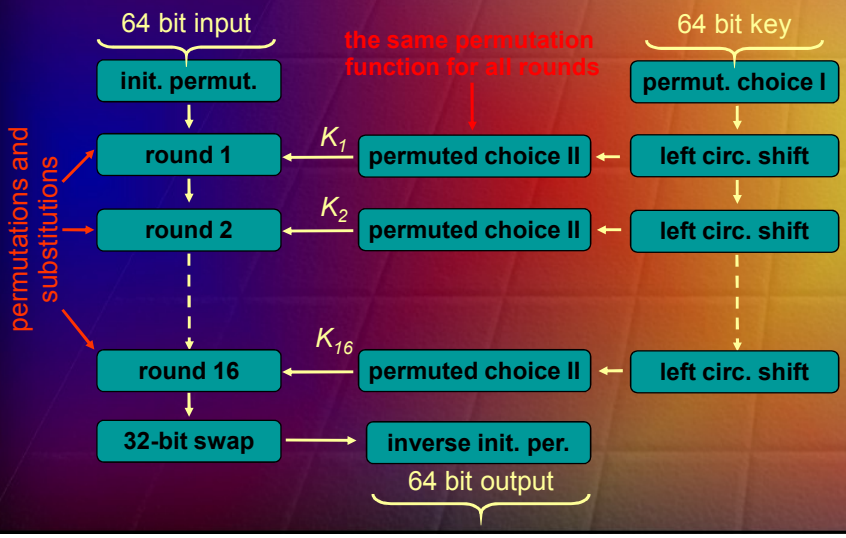
Classical cryptosystems depend heavily on combinations of substitutions and transpositions. Such combinations are often called product ciphers (if block ciphers include modular addition / multiplication, and / or linear transformation, these are advanced cryptosystems).

A typical example of CCS is DES (3DES).

Triple DES

- Je danes eden najbolj razširjenih simetričnih tajnopisnih algoritmov.
- Osnova je DES:
  - ta temelji na IBM-ovem tajnopisnem algoritmu Lucifer;
  - DES je bil uradno standardiziran s strani NIST leta 1977 in uradno podaljšan l. 1994 za uporabo za nadaljnjih pet let;
  - deluje nad 64-bitnimi bloki in potrebuje 64-bitne ključe (efektivnih je le 56 bitov ključa);
  - korakoma pretvori 64 bitne vhode v 64 bitne izhode.

Triple DES – Arhitektura navadnega DES



Triple DES– Permutacija pri DES

- Incialna permutacija:
  - Bit 1 se preslika v bit bit 58, bit 2 v bit 50,..
- Inverzna inicialna permutacija:
  - Bit 1 se preslika v bit 40, bit 2 v bit 8,…
- Enostavno lahko preverimo da velja $IP^{-1}(IP(b_n))=b_n$

(a) Initial Permutation (IP)

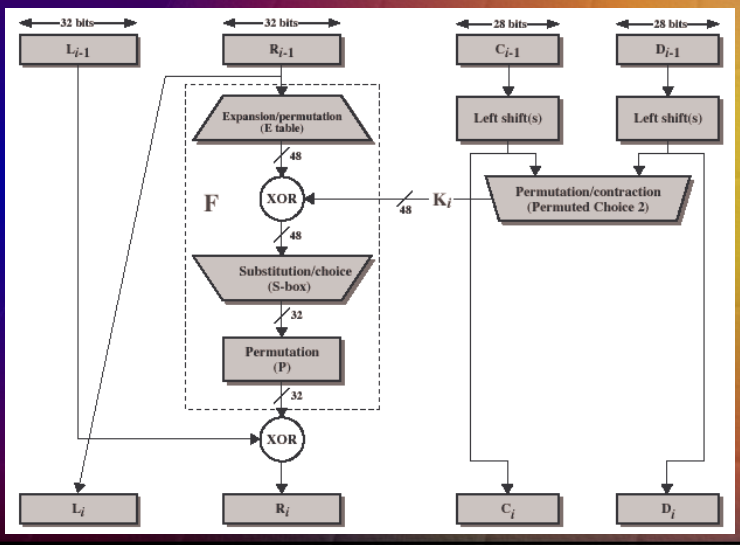
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Triple DES – prikaz posameznega cikla DES

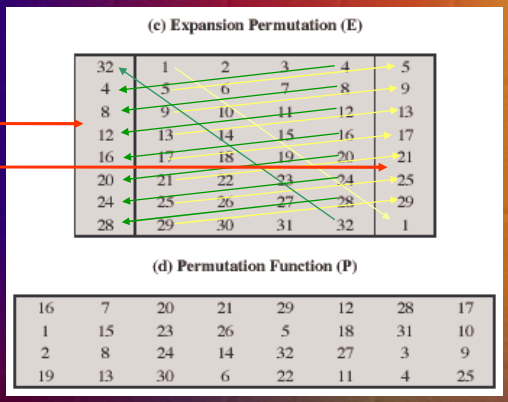
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$



Triple DES – struktura ciklov DES

- Ekspanzije (E) in permutacije (P).

duplication of 16 *R* bits (*R* denotes right-side bits, i.e. the second halve of 64 input into a round)



(c) Expansion Permutation (E)

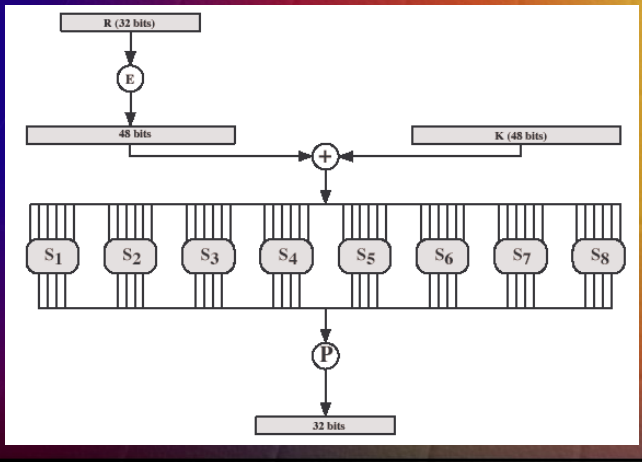
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(d) Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Triple DES – struktura ciklov DES

- Substitucije (S-boxes).



Triple DES – struktura ciklov DES

- Substitucije – S-boxes (indeksi se začno z 0).

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Input 011000 to S_1 denotes row 00 and column 1100, thus output is $a_{0,12} = 5$.

The output replaces the four middle input bits and the result is 0101.

S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Triple DES – struktura ciklov DES

- Generiranje (pod)ključev.
  - Vsak osmi bit od začetnih 64 bitov izpustimo, preostalih 56 bitov pa permutiramo skladno s spodnjo tabelo.

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Triple DES – struktura ciklov DES

- Generiranje (pod)ključev.
  - Rezultat razdelimo v dve polovici po 28 b in ju permutiramo v vsakem ciklu po tabeli II:

48 bit output →

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

  - Pred permutacijo vsako polovico rotiramo skladno s spodnjo tabelo rotacij:

(d) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Triple DES – struktura ciklov DES

- Dekripcija pri DES:
  - Uporabljamo isti algoritem, le “pod”ključe apliciramo v obratnem vrstnem redu.
- Ključni problem DES-a je kratek ključ.
  - Dvojni DES (2DES) s ključema K_1 in K_2 (C je tajnopis, P čistopis):
    - $C = E_{K2}(E_{K1}(P))$, $P = D_{K1}(D_{K2}(C))$.
    - Dokaz iz leta 1992: Pri danih K_1 in K_2 ni moč najti K_3, da bi veljalo $E_{K2}(E_{K1}(P)) = E_{K3}(P)$.
  - 2DES je načeloma torej močan, ker dvakratna uporaba dveh različnih ključev ne rezultira v preslikavi, ki bi bila rezultat ene preslikave z enim samim ključem.

Triple DES – utemeljitev strukture

- Vendar - zakaj 2DES ni dovolj dober?
- 2DES - napad “Meet in the middle”.
  - Napad sloni na dejstvu, da
    $C = E_{K2}(E_{K1}(P)) \Rightarrow X = E_{K1}(P) = D_{K2}(C)$.
  - Pri znanem paru (P,C) naredi sledeče:
    - Kriptiraj P za vseh 2^{56} možnih vrednosti ključa K_1, shrani rezultate in jih sortiraj.
    - Dekriptiraj C za vseh 2^{56} možnih vrednosti ključa K_2 in vsak rezultat primerjaj z zgornjo tabelo.
    - Ko pride do ujemanja, testiraj nov par (P,C) - če ponovno pride do ujemanja, vzemi ključ kot pravilen.

Triple DES – utemeljitev strukture

- 2 DES - napad “Meet in the middle”.
  - Moč algoritma 2DES:
    - Za vsak čistopis P obstaja 2^{64} vrednosti C.
    - V povprečju velja, da je za dani P približno število 112-bitnih ključev, ki povzročijo “lažni alarm” 2^{48} (št. ključev / št. tajnopisov, torej $2^{112}/ 2^{64}$).
    - Naslednji test nad dodatnim parom (P, C) zreducira število lažnih alarmov na $2^{48}/ 2^{64}=2^{-16}$.
    - Z določitvijo dveh parov blokov (P, C) je verjetnost, da z opisano proceduro najdemo pravi ključ, enaka $1 - 2^{-16}$.
  - Vidimo, da razbitje 2DES zahteva vložek, ki je zelo blizu reda 2^{56} operacij in ne 2^{112}.

Triple DES – utemeljitev strukture

- Triple DES:
  - V osnovi uporablja trikratno enkripcijo s tremi različnimi ključi (prepreči napad “Meet in the middle”).
  - Uporaba treh ključev pa ni praktična.
  - Na napade odporna različica je taka, da v prvi fazi izvedemo enkripcijo s prvim ključem, nato dekripcijo z drugim in nato spet enkripcijo s prvim ključem (dekripcija gre v obratnem vrstnem redu).

$C = E_{K1}(D_{K2}(E_{K1}(P)))$, $P = D_{K1}(E_{K2}(D_{K1}(C)))$.

No cryptographic significance for use of decryption in the second stage - there are practical reasons only to allow 3DES users decrypt DES encrypted data, because $C = E_{K1}(D_{K1}(E_{K1}(P))) = E_{K1}(P)$.

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Enosm. zgoščevalne funkcije - EZF (angl. one-way hash functions) so funkcije “H”, ki vhod “x” preslikajo v izhod “h”določene dolžine

$$h=H(x),$$

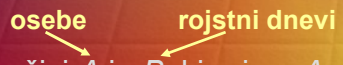
tako da velja, da
  - je vhod lahko poljubne dolžine,
  - izhod je fiksne dolžine,
  - in izračun $H(x)$ je enostaven za poljuben x, izračun v obratni smeri pa rač. zahteven.

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Dodatne zahteve za močne EZF:
  - Iz poznavanja h mora biti računsko neobvladljiv problem najti pripadajoči x, da velja $H(x)=h$.
  - Za poljubno izbrani x mora biti računsko neobvladljiv problem najti tak y, $x \neq y$, da velja $H(x)=H(y)$.
  - Za poljuben par (x,y) mora biti računsko neobvladljiv problem najti $H(x)=H(y)$.

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Izračun verjetnosti.



  - Predpostavimo dve množici A in B, kjer ima A neskončno, B pa končno število elementov.
  - Naj bodo elementi množice B naravna števila z intervala $[1,n]$.
  - Vsak element množice A se preslika v en točno določen element B.
  - Verjetnost, da se poljuben element iz A preslika v določen element v B je enaka za vse elemente iz A (uniformna distribucija).
  - Koliko elementov m iz množice A moramo naključno izbrati, da se zgodi vsaj ena kolizija v B z določeno verjetnostjo p?

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Izračun verjetnosti:
  - "*c*" pomeni kolizijo,
  - "*cf*" pomeni ne-kolizijo (ni trka),
  - "*n*" je število elementov v množici *B*.
- Paradoks fiksnega dne ("fixed-day paradox"):

  $p_c(n, m) = 1 - p_{cf}(n, m) = 1 - (n-1)^{m-1} / n^{m-1}$
- Paradoks rojstnega dne ("birthday paradox"):

  $p_c(n, m) = 1 - p_{cf}(n, m) =$
  $1 - (n / n)_1 * ((n-1) / n)_2 * \ldots * ((n-m+1) / n)_m =$
  $1 - n! / (n^m (n-m)!)$

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Primer napada (osnova paradoks rojstnega dne).
  - Dear [prof/dr] Johnson, this is to express my [honest/sincere] opinion about [teaching qualifications / academic qualifications] of dr. Kent. His [excellent / outstanding] achievements in his field with [numerous / many] references …
  - Dear [prof/dr] Johnson, this is to express my [honest/sincere] opinion about [teaching qualifications / academic qualifications] of dr. Kent. His [poor / weak] achievements in his field with [irrelevant/ minor] references …

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Principi EZF.
  - Vsak vhod gledamo kot niz *n*-bitnih blokov.
  - Vhod procesiramo blok za blokom, iterativno, tako da dobimo *n*-bitni izhod.
  - Najenostavnejša operacija v ta namen je uporaba operacije XOR.
  - Vključujemo enobitno rotacijo za izboljšanje kakovosti dobljenega izvlečka.

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Uporaba operacije XOR.

$$h_j = b_{1j} \oplus b_{2j} \oplus \ldots \oplus b_{mj},\ 1 \le j \le n$$

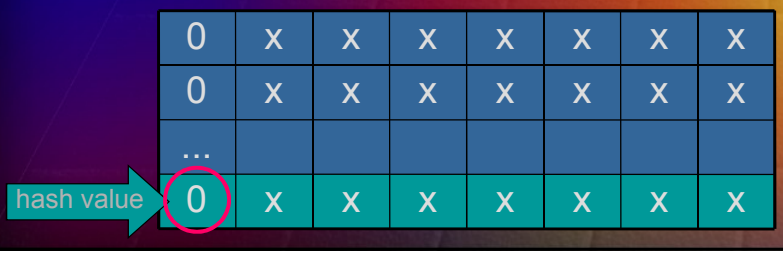
block 1	b_{11}	b_{12}	…	b_{1n}
block 2	b_{21}	b_{22}	…	b_{2n}
	…	…	…	…
block m	b_{m1}	b_{m2}	…	b_{mn}
	h_1	h_2	…	h_n

Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Principi EZF – enobitna rotacija.
  - Postavi *n*-bitni izvleček na vrednost 0.
  - Izvedi naslednje zaporedje operacij nad vsakim *n*-bitnim blokom vhoda:
    - Rotiraj trenutni izvleček za en bit v levo.
    - Izvedi XOR nad trenutnim blokom in rotiranim izvlečkom in to predstavlja nov trenutni izvleček.
    - Ponavlja prvi korak, dokler ne sprocesiraš vseh blokov na vhodu.
  - Rotacija je učinkovita za nenaključne podatke. Zakaj?

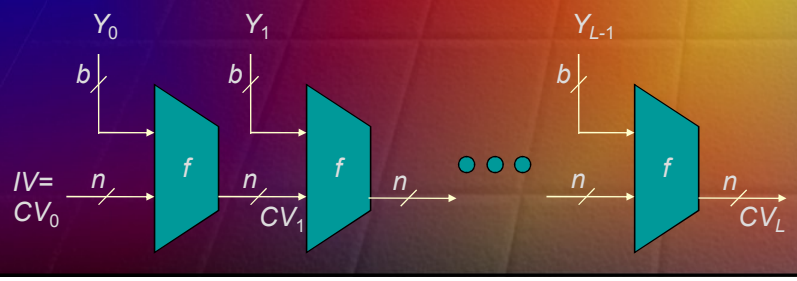
Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Pomen (ciklične) enobitne rotacije:
  - predpostavimo običajen tekst ASCII, kar pomeni, da je MSB vselej 0 in
  - predpostavimo neposredni 8-bitni izvleček.
  - Rezultat je ta, da smo 8 bitni izvleček v resnici reducirali na 7 bitnega.



Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Splošna zgradba EZF:
  - IV = inicialna vrednost, CV = sprem. veriženja;
  - Y_i = i-ti vhodni blok, f = kompresijska funkcija;
  - L = število vhodnih blokov, n = dolžina izvlečka;
  - b = dolžina vhodnih blokov ($b > n$).



Varnostni mehanizmi – Enosmerne zgoščevalne funkcije

- Splošna zgradba EZF.
  - Povzetek algoritmov:
    - $CV_0 = IV$ = inicialna n-bitna vrednost
    - $CV_i = f\,(CV_{i-1},\ Y_{i-1}),\ 1 \le i \le L$
    - $H(M) = CV_L$
  - Iteracije z uporabo kompresijske funkcije, ki ima dvodelni vhod:
    - n-bitni vhod iz predhodnjega koraka (verižena spremenljivka) in
    - b-bitni blok.
  - Ključna je kompresijska funkcija.

EZF – Secure Hash Algorithm SHA-1

- Značilnosti SHA-1:
  - Vhod je sporočilo m ($m < 2^{64}$ bitov), ki ga procesiramo v 512-bitnih blokih.
  - Izhod je 160 bitna vrednost.
- Procesiranje pri SHA-1:
  - Dodaj polnilne bite.
  - Dodaj dolžino originalnega sporočila.
  - Inicializiraj izravnalnik.
  - Procesiraj sporočilo v 512 bitnih blokih.
  - Podaj izhodno vrednost.

EZF – Secure Hash Algorithm SHA-1

- Dodajanje polnilnih bitov.
  - Vsako sporočilo polnimo s toliko biti, da je dožina kongruentna 448 po modulu 512 (dolžina $\equiv$ 448 (mod 512)).
  - Polnjenje opravimo tudi v primeru, če je sporočilo že ustrezne dolžine.
  - Prvi polnilni bit je 1, preostali so 0.
  - Št. polnilnih bitov je torej od 1 do 512.
- Dodajanje dolžine.
  - Dodamo 64 bitni blok, ki podaja dolžino originalnega sporočila pred polnjenjem.

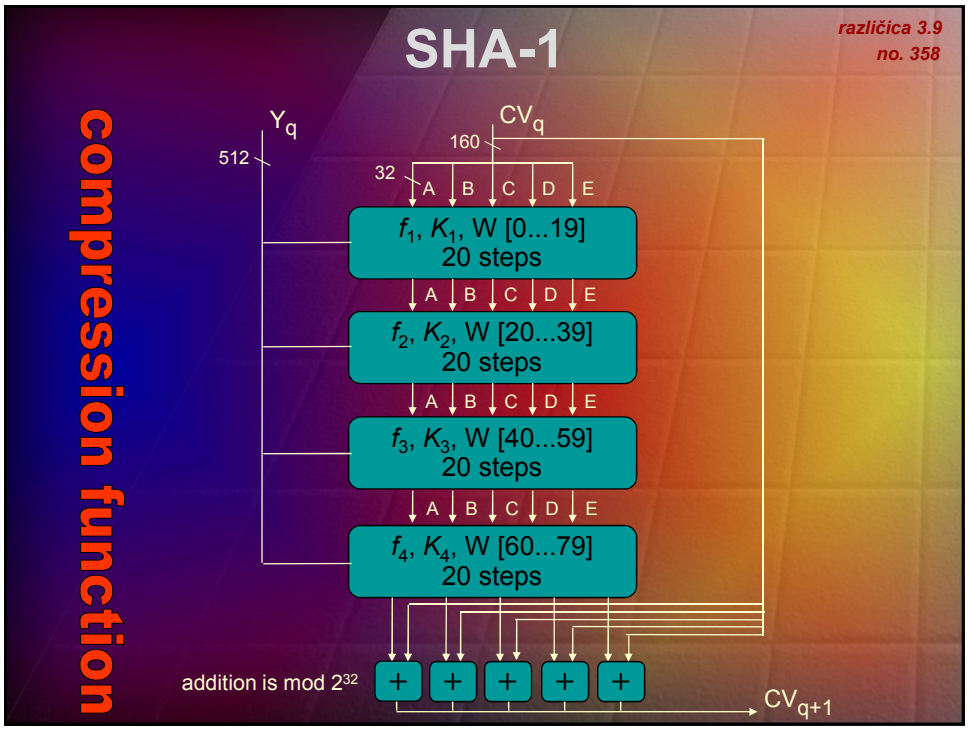
EZF – Secure Hash Algorithm SHA-1

- Inicializacija izravnalnika.
  - Vmesni in končni rezultat se nahajajo v 160 bitnem izravnalniku.
  - Izravnalnik se sestoji iz petih 32-bitnih registrov A,B,C,D in E, ki inicialno vsebujejo naslednje heksadecimalne vrednosti:
    - 67452301
    - EFCDAB89
    - 98BADCFE
    - 10325476
    - C3D2E1F0

EZF – Secure Hash Algorithm SHA-1

- Procesiranje 512-bitnih blokov - kompresija:
  - Ta funkcija se sestoji iz 4 ciklov (funkcije f_1, f_2, f_3, f_4), od katerih ima vsak 20 korakov.
  - Vsak cikel vzame trenutni 512-bitni blok, označen z Y_q, in 160 -bitno vrednost v izravnalniku (ki ga tvorijo registri ABCDE) ter izračuna novo vrednost v izravnalniku.
  - Vsak cikel uporablja aditivno konstanto K_t ($0 \leq t \leq 79$), kar pomeni 80 operacij v vseh ciklih skupaj.
  - Izhod četrtega cikla nad CV_q je dodan vhodu tega cikla samega in na ta način dobimo vhod CV_{q+1} za naslednji cikel (uporabljena je operacija seštevanje po modulu 2^{32}).

SHA-1



EZF – Secure Hash Algorithm SHA-1

- Vrednosti za K_t (t podaja zap. št. cikla):
  - $0 \le t \le 19$ → 5A827999
  - $20 \le t \le 39$ → 6ED9EBA1
  - $40 \le t \le 59$ → 8F1BBCDC
  - $60 \le t \le 79$ → CA62C1D6
- Povzetek SHA-1:
  - $CV_0 = IV$ (inic. vrednost izravnalnika ABCDE)
  - $CV_{q+1} = \mathrm{SUM}_{32}(CV_q, \mathrm{ABCDE}_q)$
    (seštevanje po modulu 2^{32})
  - $MD = CV_L$ → izvleček
    (L podaja število blokov v sporočilu, vključno s polnjenjem in oznako dolžine, MD pa pomeni "message digest")

EZF – Secure Hash Algorithm SHA-1

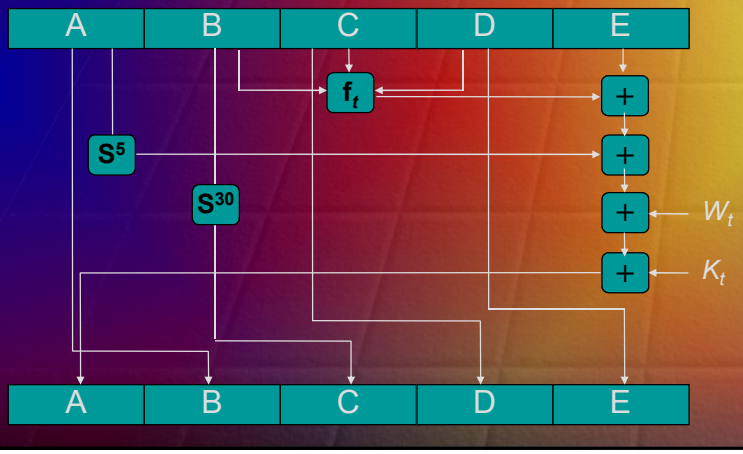
- Cikel kompresijske funkcije SHA-1:

$$A,B,C,D,E \leftarrow (E + f(t,B,C,D)+S^5(A)+W_t+K_t),A,S^{30}(B),C,D$$

  - A,B,C,D,E-predstavlja pet besed v izravnalniku;
  - $f(t, B, C, D)$ - predstavlja primitivno log. funkcijo;
  - S^k - pomeni krožni zamik 32 bitov za k bitov v levo;
  - W_t - 32-bitna beseda dobljena iz trenutnega 512-bitnega vhodnega bloka (glej naslednjo prosojnico);
  - K_t - aditivna konstanta (glej prejšnjo prosojnico);
  - + = seštevanje po modulu 2^{32}.

EZF – Secure Hash Algorithm SHA-1

- Cikel kompresijske funkcije SHA-1.



EZF – Secure Hash Algorithm SHA-1

- Kompresijska funkcija SHA-1 (cikel).
  - Določitev primitivne logične funkcije $f(t, B, C, D)$:
    - $0 \le t \le 19 \rightarrow f(t, B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$
    - $20 \le t \le 39 \rightarrow f(t, B, C, D) = B \oplus C \oplus D$
    - $40 \le t \le 59 \rightarrow f(t, B, C, D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$
    - $60 \le t \le 79 \rightarrow f(t, B, C, D) = B \oplus C \oplus D$
  - Izračun 32-bitnih besed W_t iz 512-bitnega vhoda:
    - Prvih 16 vrednosti dobimo neposredno iz danega bloka (prvih 16 korakov).
    - Preostale vrednosti (za preostalih 64 korakov) pa izračunamo po formuli

$$W_t = S^1(W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3})$$

EZF – SHA-1 standardi

- Družino SHA je razvil ameriški NIST (National Institute of Standards and Technology).
- Standardi:
  - SHA: FIPS PUB 180 iz leta 1993.
  - SHA-1: FIPS PUB 180-1 iz leta 1995.
  - SHA-X: FIPS PUB 180-2 iz leta 2002:
    - SHA-1, SHA-256, SHA-384, SHA-512,
    - osnova ostaja SHA-1.
  - SHA-1 je hitra, je enostavna in kompaktna za izvedbo.
  - SHA-1 je do l. 2006 bila odporna na napade.

EZF in pomembni standardi

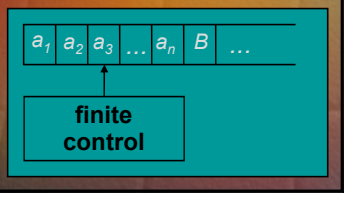
- RIPEMD-160:
  - ISO/IEC, "IT - Security techniques - Hash-functions - Part 3: Dedicated hash-functions," ISO 10118-3, Geneva, 1998.
- MD-4:
  - Rivest, R., "The MD4 Message-Digest Algorithm", RFC 1320, IETF, Reston, 1992.
- MD-5:
  - Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, IETF, Reston, 1992.

Teoretični temelji

- Turingov stroj (TS).
  - Ima kontrolno enoto s končnim številom stanj in trak z dano skrajno levo celico, ki se na desno širi v neskončnost - glava bere samo eno celico v danem trenutku.
  - Vsaka celica vsebuje točno en simbol iz končnega nabora simbolov - spočetka trak vsebuje na skrajni levi *n* vhodnih simbolov (program), preostale celice so prazne.
  - V enem pomiku kontrolne enote TS glede na stanje enote in skeniran simbol
    - spremeni stanje enote,
    - natisne nov simbol prek prejšnjega in
    - pomakne glavo bodisi desno ali levo.

Teoretični temelji

- TS formalno podaja *n*-terka
  $M=(Q, \Sigma, \Gamma, \delta, q_0, B, F)$, kjer je
  - Q končna množica stanj;
  - Γ končna množica tračnih simbolov, kjer B podaja t.i. prazen (angl. blank) simbol in kjer je Σ množica vhodnih simbolov ($\Sigma \subseteq \Gamma$) ter $B \in \Gamma \setminus \Sigma$;
  - δ je funkcija ("funkcija pomika")
    $Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$;
  - $q_0 \in Q$ je začetno stanje;
  - $F \subseteq Q$ je množica končnih stanj.



Teoretični temelji

Complexity theory

Computational complexity provides a basis for analysis of computational requirements of crypto-systems.

Definition An algorithm is a well-defined computational procedure that takes a variable input and halts with an output.

Complexity theory and cryptography:

- The strength of a cipher is determined by the computational complexity of the algorithms used to solve the cipher.
- The computational complexity of an algorithm is measured by its time requirements, expressed as a function of input, i.e. bits.
- This function is typically expressed as an order-of-magnitude / with asymptotic upper bound notation (the "big O" notation).

Teoretični temelji

Complexity theory

Definition $f(n) = O(g(n))$ if there exists a positive constant c and a positive integer n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$.

Example Let $f(n) = 17n + 10$. Then $f(n) = O(n)$ because $17n + 10 \leq 18n$ for $n \geq 10$, thus $g(n) = n$, $c = 18$, and $n_0 = 10$.

Example Let $f(n) = a_m n^m + a_{m-1} n^{m-1} + \ldots + a_0$. For a given m it follows that $f(n) = O(n^m)$. If $m = 1$, linear complexity $O(n)$ is obtained. If $m = 2$, quadratic complexity $O(n^2)$ is obtained.

Definition A polynomial-time algorithm is an algorithm whose worst-case running time is $O(n^m)$, where n is the input size and m is a constant. Any algorithm whose running time cannot be so bounded is called an exponential-time algorithm with $O(m^{h(n)})$, where m is some constant and $h(n)$ is a polynomial.

Example An example of exponential complexity is $O(2^n)$.

Teoretični temelji

Complexity theory

Explanation Turing machine (TM) is a finite state machine with an infinite read-write tape that serves as a model of computation.

Definition Problems that are solvable in polynomial time are tractable (computationally feasible). Problems that cannot be solved systematically in polynomial time are called intractable (computationally hard). Problems for which it is impossible to write an algorithm to solve them are undecidable.

Definition The class **P** consists of all problems solvable in polynomial time on deterministic TM. The class **NP** (non-deterministic polynomial) consists of all problems solvable in polynomial time on non-deterministic TM (perfect guess and verification in polynomial time).

Teoretični temelji

Complexity theory

Observation To systematically (deterministically) solve certain problems in **NP** seems to require exponential time.

Interpretation of a definition The class **NP** includes the class **P** because any problem polynomial solvable on a deterministic **TM** is polynomial solvable on a non-deterministic one.

Fact It is not proved whether **P=NP** or not. It is believed that **P** $\neq$ **NP**.

Definition A problem is **NP-hard** if it cannot be solved in polynomial time unless **P=NP**.

Definition A problem is in **NP-complete** if it is in **NP** and **NP-hard**.

Observation Known algorithms for systematically solving **NP-complete** problems have exponential worst case complexities.

Teoretični temelji

Complexity theory

In 1976 Diffie and Hellman suggested to apply computational complexity to design of crypto-systems:

- **NP-complete** problems are suitable because they cannot be solved in polynomial time by any known technique. Information is enciphered by encoding it in an **NP-complete** problem (knowing a secret key provides ability for a "perfect gues").
- More complex problems are not suitable because crypto transformations would require more than polynomial time.

Design of crypto-systems that are based on complexity should not rely only on worst-case complexity - the cryptanalyst often has a possibility of getting a large collection of statistically related problems. Some typical hard problems that are used for crypto-systems include factorization of large primes composites and discrete log.

Teoretični temelji

Groups

Definition A binary operation $*$ on a set S is a mapping from $S \times S$ to S. That is, $*$ is a rule which assigns to each ordered pair of elements from S an element of S.

Definition A group $(G, *)$ consists of a set G with a binary operation $*$ on G satisfying these axioms:

- The group operation is associative. That is, $a*(b*c) = (a*b)*c$ for all $a, b, c \in G$.
- There is an element $1 \in G$, called the identity element, such that $a*1 = 1*a = a$ for all $a \in G$.
- For each $a \in G$ there exists an element $a^{-1} \in G$, called the inverse of a, such that $a*a^{-1} = a^{-1}*a = 1$.
- A group is abelian (or commutative) if $a*b = b*a$ for all $a, b \in G$.

Teoretični temelji

Groups

Definition A group G is finite if $\mid G \mid$ is finite. The number of elements in a finite group is called its order.

Definition A non-empty subset H of a group G is a subgroup of G if H is itself a group with respect to the operation of G. If H is a subgroup of G and $G \neq H$, then H is called a proper subgroup of G.

Definition A group G is cyclic if there is an element $\alpha \in G$ such that for each $b \in G$ there is an integer i with $b = \alpha^i$. Such an element α is called a generator of G.

Definition Let G be a group and $a \in G$. The order of a is defined to be the least positive integer t such that $a^t = 1$, provided that such an integer exists. If such t does not exist, then the order of a is defined to be ∞.

Teoretični temelji

Groups

Explanation The multiplicative group notation has been used for the group operation. If the group operation is addition, then the group is said to be an additive group, the identity element is denoted by 0, and the inverse is denoted by $-a$.

Teoretični temelji

Rings

Definition A ring $(R, +, \times)$ consists of a set R with two binary operations arbitrarily denoted $+$ (addition) and $\times$ (multiplication) on R, satisfying the following axioms:

- $(R, +)$ is an abelian group with identity denoted 0.
- The operation $\times$ is associative. That is, $a \times (b \times c) = (a \times b) \times c$ for all $a, b, c \in R$.
- There is a multiplicative identity denoted 1, with $1 \neq 0$, such that $1 \times a = a \times 1 = a$ for all $a \in R$.
- The operation $\times$ is distributive over $+$. That is, $a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a)$ for all $a, b, c \in R$.

The ring is commutative if $a \times b = b \times a$ for all $a, b \in R$.

Definition An element a of R is called a unit or an invertible element if there is an element $b \in R$ such that $a \times b = 1$.

Teoretični temelji

Fields

Definition A field is a commutative ring in which all non-zero elements have multiplicative inverses.

Definition The *characteristic* of a field is 0 if $\overbrace{1+1+\ldots+1}^{m-times}$ is never equal to 0 for any $m \geq 1$. Otherwise, the characteristic of the field is the least positive integer m such that $\Sigma_{i=1}^{m} 1$ equals 0.

Example The set of integers under addition and multiplication is not a field, since the only non-zero elements with multiplicative inverses are 1 and -1. However, rational, real and complex numbers form fields of characteristic 0 under the usual operations.

Number theory

Definition For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval [1, n] which are relatively prime to n (Euler phi function).

Facts If p is a prime, then $\phi(p) = p - 1$. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Teoretični temelji

The integers modulo n with n being a positive integer

Definition If a and b are integers, then a is said to be *congruent to* b *modulo* n, written $a \equiv b \pmod{n}$ or $a \equiv_n b$, if n divides $(a - b)$. The integer n is called the modulus of the congruence.

Fact For all $a, a_1, b, b_1, c \in \mathbb{Z}$, the following are true:

- $a \equiv b \pmod{n}$ iff a and b leave the same reminder when divided by n.
- $a \equiv a \pmod{n}$ (reflexivity)
- If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$ (symmetry)
- If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ (transitivity)
- If $a \equiv a_1 \pmod{n}$ and $b \equiv b_1 \pmod{n}$, then $a + b \equiv a_1 + b_1 \pmod{n}$ and $ab \equiv a_1 b_1 \pmod{n}$.

Fact $(a * b) \equiv_n (a * c) \Rightarrow b \equiv_n c$ if a is relatively prime to n.

Teoretični temelji

The integers modulo n

Definition If x is any integer and n positive integer, then x mod n equals the integer remainder r in the range [0, n-1] after x is divided by n, i.e. $x \bmod n = r$.

Definition The *integers modulo* n, denoted $\mathbb{Z}_n$, is the set of (equivalence classes of) integers $\{0, 1, 2, \ldots, n\text{-}1\}$. Addition, subtraction, and multiplication in $\mathbb{Z}_n$ are performed modulo n.

Definition Let $a \in \mathbb{Z}_n$. The *multiplicative inverse* of a modulo n is an integer $x \in \mathbb{Z}_n$ such that $ax \equiv 1 \pmod{n}$. If such an x exists, then it is unique, and a is said to be *invertible*, or a unit; the inverse of a is denoted by by a^{-1}.

Definition The *multiplicative group* of $\mathbb{Z}_n$ is $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. In particular, if n is prime, then $\mathbb{Z}_n^* = \{a \mid 1 \leq a \leq n-1\}$.

Teoretični temelji

The integers modulo n

Fact Let $n \geq 2$ be an integer and p a prime.

- If $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. (Fermat's theorem)
- If $r \equiv s \pmod{p\text{-}1}$, then $a^r \equiv a^s \pmod{p}$ for all integers a. In other words, when working modulo a prime p, exponents can be reduced modulo p-1. In particular, $a^p \equiv a \pmod{p}$ for all a.
- If $a \in \mathbb{Z}_n^*$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. (Euler's theorem)
- If n is a product of distinct primes, and if $r \equiv s \pmod{\phi(n)}$, then $a^r \equiv a^s \pmod{n}$ for all integers a. In other words, when working modulo such an n, exponents can be reduced modulo $\phi(n)$.

Example Let $n = 21$.
Then $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.
Note $a \bmod n = r \Rightarrow a \equiv r \pmod{n}$,
BUT $a \equiv r \pmod{n} \not\Rightarrow a \bmod n = r$

Teoretični temelji

Izpeljava Frematovega teorema

Imejmo praštevilo p, ter celo število a, ki je tuje p. Vzemimo množici $A = \{1, 2, 3, ..., p-1\}$ in $B = \{1a, 2a, 3a, ..., (p-1)a\}$, kjer so zmnožki množice B dobljeni kot kongruence mod$p$. Trdimo, da je množica B le permutacija množice A. Dokaz s kontradikcijo:

- Vzemimo dva elementa m in n iz množice A (ki sta po predpostavki različna). Če množica B nima različnih elementov, velja po množenju $ma \equiv na (\mathrm{mod} p)$, ali $(m-n)a \equiv 0 (\mathrm{mod} p)$.
- Ker je a celo število (poljubno voljeno do pogoja, da je tuje p), mora veljati $m = n$, kar pa je v kontradikciji z izhodiščno predpostavko.

Tvorimo zmnožek elementov A in B, kjer za zmnožek $1*2*...*(p-1)$ velja, da je tuj p. Zato lahko z njim delimo oba člena te kongruence: $1*2*...*(p-1) \equiv_p 1a*2a*...*(p-1)a$ oz. $1*2*...*(p-1) \equiv_p 1*2*...*(p-1)*a^{p-1}$. Torej $a^{p-1} \equiv_p 1$, kar je Fermatov teorem.

Teoretični temelji

Frematov teorem - primeri

Imejmo $p = 5$ in $a = 7$ ter $A = \{1, 2, 3, 4\}$.
Torej je $B = \{2, 4, 1, 3\}$
(kar je rezultat $1 * 7 \bmod 5, 2 * 7 \bmod 5, 3 * 7 \bmod 5, 4 * 7 \bmod 5$).

Še primer residuuov po modulu in kongruenc.

- $a \bmod n = b \Rightarrow a \equiv_n b$. Primer: $7 \bmod 2 = 1 \Rightarrow 7 \equiv_2 1$.
- $a \equiv_n b \not\Rightarrow a \bmod n = b$. Primer: $14 \equiv_3 5 \not\Rightarrow 14 \bmod 3 = 5$.

Eulerjev teorem

Glede dokaza Eulerjevega teorema - ta je generalizacija Fermatovega teorema.

Teoretični temelji

Extended Euclidean algorithm

INPUT:
two non-negative integers a and b with $a \geq b$.
OUTPUT:
$d = \gcd(a, b)$ and integers x, y satisfying $ax + by = d$.

ALGORITHM - the running time (in bit operations) is $O((\lg n)^2)$:

1. If $b = 0$ then set $d \leftarrow a, x \leftarrow 1, y \leftarrow 0$, and return (d, x, y).
2. Set $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$.
3. While $b > 0$ do the following:
   (a) $q \leftarrow \lfloor a/b \rfloor, r \leftarrow a - qb, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$.
   (b) $a \leftarrow b, b \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4. Set $d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$, and return (d, x, y).

Teoretični temelji

Extended Euclidean algorithm - an example

q	r	x	y	a	b	x_2	x_1	y_2	y_1
-	-	-	-	4864	3458	1	0	0	1
1	1406	1	-1	3458	1406	0	1	1	-1
2	646	-2	3	1406	646	1	-2	-1	3
2	114	5	-7	646	114	-2	5	3	-7
5	76	-27	38	114	76	5	-27	-7	38
1	38	32	-45	76	38	-27	32	38	-45
2	0	-91	128	38	0	32	-91	-45	128

Computing multiplicative inverses in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$.
OUTPUT: $a^{-1} \bmod n$, provided that it exists.
ALGORITHM:

1. Use extended Euclidean algorithm to find integers x and y such that $ax + ny = d$, where $d = \gcd(a, n)$.
2. If $d > 1$, then $a^{-1} \bmod n$ does not exist. Otherwise, return x.

Teoretični temelji

Square-and-multiply exponentiation in $\mathbb{Z}_n$

INPUT: $a \in \mathbb{Z}_n$, and integer $k \in [0, n)$ whose binary representation is $k = \Sigma_{i=0}^{t} k_i 2^i$.
OUTPUT: $a^k \bmod n$.

ALGORITHM:

1. Set $b \leftarrow 1$. If $k = 0$ then return b.
2. Set $A \leftarrow a$.
3. If $k_0 = 1$ then set $b \leftarrow a$.
4. For i from 1 to t do the following:
   (a) Set $A \leftarrow A^2 \bmod n$.
   (b) If $k_i = 1$ then set $b \leftarrow A \cdot b \bmod n$.
5. Return b.

Teoretični temelji

Computational (bit) complexities in $\mathbb{Z}_n$

- Taking into account that $(a+b) \bmod n = a+b$ if $(a+b < n)$, the number of bit operations is $\lg a$ (or $\lg b$ if $b > a$). If $(a+b \geq n)$ then $(a+b) \bmod n = a+b-n$, so the number of bit operations is twice bigger than in previous case. Thus asymptotic complexity is $O(\lg n)$ (analogous arguments hold true for subtraction).
- Multiplication - multiply a and b as integers and than take the reminder, thus the worst case complexity is $O(lg^2 n)$.
- Multiplicative inversion can be computed with extended Euclidean algorithm - the complexity is $O(lg^2 n)$.
- Exponentiation can be computed with square-and-multiply algorithm, which has the asymptotic upper bound $O(lg^3 n)$.
- **But**, using appropriate modulus, the complexity of factorization and discrete log is (roughly) $O(e^{\sqrt{\ln n \ln(\ln n)}})$.

Teoretični temelji

RSA algorithm

Key generation

Entity A creates a public key and corresponding private key:

- Generate two large random and distinct primes p and q of roughly the same size.
- Compute $n = pq$ and $\phi = (p-1)(q-1)$.
- Select random integer e, $1 < e < \phi$, such that $\gcd(e, \phi)$=1.
- Use the extended Euclidean algorithm to compute the unique integer d, $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.

Public key presents pair (n, e), while d is private key (e is encryption and d decryption exponent).

Teoretični temelji

RSA algorithm

Encryption and decryption

Entity B encrypts for A a message m that is represented as an integer m in the interval [0, n-1]. B encrypts m by computing $c = m^e \bmod n$, while A decrypts it by computing $m = c^d \bmod n$.

Proof

Since $ed \equiv 1 (\bmod \phi)$, there exists an integer k such that $ed = 1 + k\phi$.

- If $\gcd(m, p)$=1, then by Fermat' s theorem $m^{p-1} \equiv 1 \pmod{p}$.
- Raising both sides of this congruence to the power $k(q-1)$ and multiplying them by m yields $m^{1+k(p-1)(q-1)} \equiv m (\bmod p)$.
- If $\gcd(m, p) = p$, then this last congruence is again valid since each side leaves 0, when divided by p.
- Hence, in all cases $m^{ed} \equiv m (\bmod p)$ and by the same argument $m^{ed} \equiv m (\bmod q)$.
- Since p and q are distinct primes, it follows that $m^{ed} \equiv m \pmod{n}$ and hence $c^d \equiv (m^e)^d \equiv m (\bmod n)$.

Teoretični temelji

RSA algorithm

An operation example with small parameters

Key generation.
Entity A chooses the primes $p = 2357$, $q = 2551$, and computes $n = pq = 6012707$ and $\phi = (p-1)(q-1) = 6007800$. Entity A chooses $e = 3674911$. With the extended Euclidean algorithm it finds $d = 422191$ such that $ed \equiv 1 (\mathrm{mod}\ \phi)$. A' s public key presents the pair $(n = 6012707, e = 3674911)$, while private key is $d = 422191$.
Encryption.
B encrypts a message $m = 5234673$ by computing $c = m^e \bmod n = 5234673^{3674911} \bmod 6012707 = 3650502$, and sends this result to A.
Decryption.
To decrypt c, A computes $c^d \bmod n = 3650502^{422191} \bmod 6012707 = 5234673$.

Teoretični temelji

- RSA - pomembna dejstva
  - Trdnost RSA temelji na predpostavki, da je faktorizacija velikih celih števil (kompozitov velikih praštevil) zahteven problem (angl. intractability of the integer factorization).
  - Indijski matematiki Agrawal, Kayal in Saxena so leta 2002 iznašli deterministični algoritem za preverjanje praštevil s polinomsko časovno kompleksnostjo (prej smo poznali le statistične teste).
- Standardi: RSA laboratories, RSA Cryptography Standard, PKCS #1 v 2.1, 2002.

Teoretični temelji

Diffie Hellman key agreement

Description The protocol rests on the assumption about computational intractability of discrete logarithms, i.e. given a prime p, a generator α of $\mathbb{Z}_p^*$, and an element $\beta \in \mathbb{Z}_p^*$, it should be infeasible to compute x, $0 < x \leq p-2$, such that $\alpha^x \equiv \beta (\mathrm{mod} p)$.

- Entities A and B agree on prime p and generator α of $\mathbb{Z}_p^*$, $2 \leq \alpha \leq p-2$,which are both made public.
- Entitiy A chooses secret x (at random) from the closed interval [1, p-2], while B does the same to obtain secret y.
- A sends $\alpha^x \bmod p$ to B and B sends $\alpha^y \bmod p$ to A.
- A computes $K = (\alpha^y)^x \bmod p$ and obtains the shared secret key, while B obtains it by computing $K = (\alpha^x)^y \bmod p$.

Variables x and y are referred to as private keys, while α^x and α^y are referred to as public keys.

20

Teoretični temelji

- Ranljivosti protokola DH.
  - Napad z “napadalcem vmes” (angl. man in the middle):
    - Napadalec prestreže vrednosti α^x *in* α^y ter ju nadomesti z $\alpha^{x'}$ in $\alpha^{y'}$.
    - Napadalec izračuna $\alpha^{x'y}$ za komunikacijo z B-jem in $\alpha^{xy'}$ za komunikacijo z A-jem.
    - Rešitev - uporaba certifikatov.
  - Slabe vrednosti eksponentov:
    - Izberemo eksponent tako, da je $\alpha^x = \alpha$, i.e. x=1.
    - Rešitev - primer je enostavno opaziti, a program mora imeti vgrajeno ustrezno preverjanje.

Obvladovanje varnosti IS

- Osnova je standard BS 7799 iz l. 1995.
- Leta 1999 nova različica BS 7799, ki se deli na dva dela:
  - prvi del vsebuje pristope in ukrepe pri ravnanju z informacijami (Kodeks varovanja informacij);
  - drugi del vsebuje proces vzpostavitve sistema varovanja (Sistem vodenja za varovanje informacij).
- Leta 2000 sprejet ISO 17799, ki je praktično enak BS 7799 iz leta 1999.
- Leta 2005 sprejeta zadnja različica standarda ISO 17799, enako BS 7799-2 kot ISO 27001, ki vključuje BS 7799-3 (risk management).

Obvladovanje varnosti IS

- Ocenjevanje tveganj (risk assessment) pomeni identifikacijo groženj, njihovih vplivov in ranljivosti informacij ter sistemov za njihovo procesiranje skupaj z oceno verjetnosti pojava posameznih tveganj.
- Upravljanje tveganj (risk management) pomeni proces identifikacije, nadzora in minimizacije tveganj ob sprejemljivih stroških.

Obvladovanje varnosti IS

- Kodeks dobrih običajev (angl. Code of practice) - ISO 17799.
  - Varovanje informacij pomeni:
    - zaupnost, ki zagotavlja le avtoriziran dostop,
    - celovitost, ki zagotavlja točnost in popolnost informacij ter njihovo procesiranje,
    - razpoložljivost, ki zagotavlja dostop do informacij, ko je to potrebno.
  - Varovanje informacij dosežemo z ustreznim naborom mehanizmov (praks, postopkov, organizacijskih struktur in strojno-programskih funkcij).
  - Osnovni dokument - varnostna politika.

Obvladovanje varnosti IS

- Kodeks ISO 17799.
  - Varnostne zahteve - izhodišča zahtev:
    - ocenitev tveganj,
    - zakonodajna/legalna in pogodbena razmerja,
    - iz poslovnih ciljev izhajajoči principi in zahteve določene organizacije.
  - Na osnovi varnostnih zahtev določimo varnostne kontrole:
    - bistvene zakonodajne kontrole (zaščita podatkov, zasebnosti, dostopnosti poslovnih listin, intelektualne lastnine,...);
    - najbolše obstoječe običaje (izobraževanje, dodelitev odgovornosti, poročanje,…).

Obvladovanje varnosti IS

- Kodeks ISO 17799.
  - Ključni dejavniki uspeha.
    - obstoj varnostne politike,
    - izvedba varnostne politike, ki je skladna z organizacijsko kulturo;
    - brezpogojna podpora s strani managementa;
    - dobro razumevanje problematike;
    - ustrezno izobraževanje in seznanjanje članov organizacije s problematiko;
    - trening in podpora;
    - merjenje učinkovitosti in ustrezno obravnavanje dogodkov s poročanjem v obeh smereh (od dna k vrhu in od vrha k dnu - npr. odzivi na pobude).

Obvladovanje varnosti IS

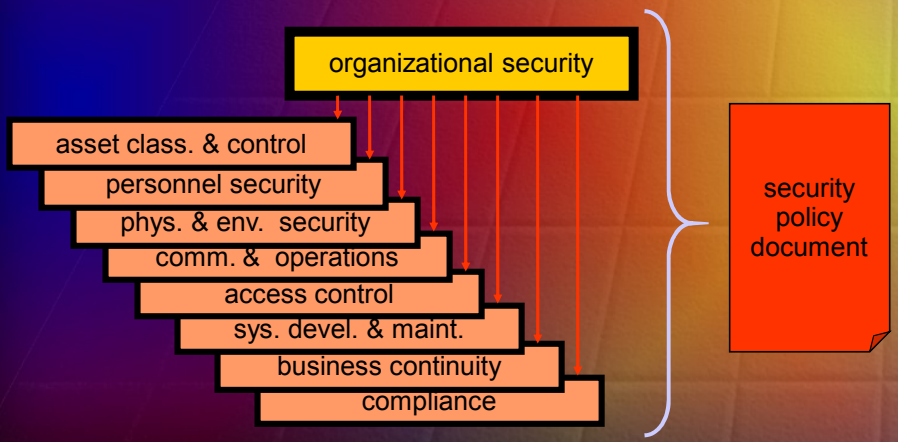
- Kodeks ISO 17799.
  - Varnostna politika (VP):
    - VP daje poslovodstvu smer in podporo za odločanje pri varovanju informacij.
    - VP mora biti dokumentirana in ta dokument, v katerem se vodstvo zaveze varnostni politiki, mora biti potrjen s strani vodstva.
    - Vse člani organizacije morajo biti seznanjeni z varnostno politiko - delno ali v celoti.
    - Minimalna VP: definicije, cilji, zaveza vodstva, kratko pojasnilo principov, standardi in legalne zahteve, kategorizacija virov in definicija odgovornosti ter referiranje druge podporne dokumentacije, določitev evalvacije in sprememb VP.

Obvladovanje varnosti IS

- Kodeks ISO 17799.
  - Vzpostavitev VP zahteva ustrezne organizacijske pristope, ki obsegajo:
    - klasifikacijo virov in kontrol,
    - osebno varnost,
    - fizično in okoljsko varovanje,
    - varovanje komunikacij in varovanje operacij,
    - nadzor dostopa,
    - razvoj in vzdrževanje IS,
    - načrtovanje nemotenega poslovanja,
    - skladnost.

Obvladovanje varnosti IS

- Kodeks ISO 17799.



Obvladovanje varnosti IS
(splošni principi)

- Org. infrastruktura za obv. varnosti.
  - Vodstveni forum za upravljanje varnosti: ta ocenjuje in potrjuje VP, spremlja ključne spremembe, spremlja in analizira varnostne incidente, podaja generalne iniciative za izboljšave.
  - Koordinacijski forum: določa specifične naloge, odgovornosti, metodologije za ocenjevanje tveganj, klasifikacijo varnosti, izvaja iniciative za povečanje pomena varnosti na nivoju organizacije, koordinira celotno dejavnost na tem področju.
  - Varnostni nadzornik (security officer).
  - Svetovalci: notranji, zunanji.

Obvladovanje varnosti IS
(splošni principi)

- Koordinacija - vključitev v ustrezne forume in telesa (npr. CERT).
- Revizija - je lahko interna, vendar je zaželena zunanja revizija s strani neodvisne specializirane organizacije.
- Dodelitev odgovornosti:
  - vsak nabor podatkov (informacijski vir) mora imeti lastnika, ki je zanj zadolžen,
  - odgovornost mora biti točno opredeljena in dokumentirana;
  - delitev obveznosti - povečamo nadzor (zmanjšana možnost prekoračitve pooblastil).

Obvladovanje varnosti IS
(splošni principi)

- Proces avtorizacije:
  - nivoji avtorizacije morajo biti opredeljeni in dokumentirani;
  - ta mora obstajati tudi za vključitev novih sklopov v sistem (način uporabe, kontrola HW in SW, itd.).
- Popis premoženja:
  - informacijski viri (zbirke podatkov, sistemska dokumentacija, priročniki);
  - programska oprema (aplikacije, razvojna orodja, sistemska oprema);
  - fizično premoženje (računalniki, usmerjevalniki, sistemi za arhiviranje);
  - podporne storitve (ogrevanje, hlajenje, osvetljevanje, električno napajanje, itd.).

Obvladovanje varnosti IS
(splošni principi)

- Klasifikacija informacij:
  - informacije imajo različne stopnje občutljivosti in skladno s tem jih ščitimo ne glede na to, ali so v elektronski ali kaki drugi obliki;
  - s klasifikacijo določimo, kako rokovati in ščititi določeno vrsto informacij;
  - klasifikacija zahteva periodično revizijo zaradi staranja informacij;
  - klasifikacijo opravljamo z etiketiranjem (pomen lastnika!);
  - preveč kompleksne klasifikacijske sheme dosežejo nasproten učinek.

Obvladovanje varnosti IS
(splošni principi)

- Klasifikacija informacij - označevanje in procesiranje:
  - Za označevanje so najbolj primerne fizične etikete, če to ne gre, pa elektronske.
  - Dejavnosti procesiranja, ki morajo biti nujno zajete, vključujejo kopiranje, hranjenje, prenos (pošta, faks, e-pošta), prenašanje z govorom, uničevanje.
  - Klasifikacija mora vključevati ne samo trakove diske, zgoščenke, ampak tudi računalniške izpise in ekranske maske.

Obvladovanje varnosti IS
(splošni principi)

- Delovne dolžnosti.
  - Namen je zmanjšati možnost človeških napak, napačne uporabe ali kraje.
  - Zadolžitve glede varovanja informacij morajo biti navedene v pogodbi in izvajane od samega začetka zaposlitve.
  - Novo zaposleni sodelavci morajo biti primerno nadzorovani (upoštevanje zasebnosti!) in morajo podpisati ustrezno izjavo, da bodo upravljali z zaupanimi informacijami skladno z varnostno politiko.

Obvladovanje varnosti IS
(splošni principi)

- Izobraževanje - nujno za izgradnjo zavesti o pomeu VP in skladnost delovanja z VP.
- Formaliz. postopki odziva na vdore in odkrite slabosti v informacijskem sistemu:
  - takojšnje poročanje po ustreznih kanalih;
  - izvedba ustreznih akcij;
  - nujna povratna informacija.
- Učenje na izkušnjah - potreba po dodatnih ukrepih, modifikacijah, revizijah VP.
- Disciplinski postopki - ti postopki morajo biti pozitivno naravnani in korektni.

Obvladovanje varnosti IS
Splošen nadzor

- Vzdrževanje reda v delovnem okolju:
  - papirni dokumenti in računalniški mediji morajo biti vselej shranjeni v zaklenjenih predalih, če niso v uporabi;
  - za izjemno občutljive podatke uporabljamo vodo in ognjevarne sefe;
  - če računalnik ni v uporabi, se mora uporabnik odjaviti s sistema;
  - natisnjene materiale moramo takoj odstraniti s tiskalnika;
  - ščitenje izhodne in vhodne pošte in faksa;
  - zaklepanje fotokopirnih strojev izven delovnih ur.

Obvladovanje varnosti IS

Splošen nadzor

- Iznos lastnine (opreme):
  - za vsak iznos je potrebna avtorizacija;
  - registracija časa iznosa in časa vrnitve;
  - periodične kontrole, da odkrijemo neavtoriziran iznos opreme in o tem obvestiti zaposlene.
- Dokumentiranost procedur:
  - procesiranja in rokovanja z informacijami,
  - zaporedja operacij, medsebojnih odvisnosti,
  - navodil za obravnavanje napak in neregularnih operacij (ravnanje z rezultati teh operacij),
  - navedbe kontaktnih točk v primeru težav,
  - ponovnega zagona/vzpostavitve prvotnega stanja.

Obvladovanje varnosti IS

Nadzor dostopa

- Upravljanje dostopa:
  - registracija uporabnikov z dodeljevanjem identifikatorjev in vročitvijo pisnega dokumenta o pravicah dostopa, ki ga podpišejo;
  - upravljanje privilegijev (predvsem sistemskih);
  - vodenje evidence o pravicah dostopa in ločevanje pravic (ista oseba mora kot navadni imeti različno identifikacijo kot sistemski uporabnik).
  - upravljanje gesel (struktura gesel, začasna gesla, enkratna gesla, veljavnost gesel);
  - revizija pravic dostopa uporabnikov (pogostejša revizija višjih privilegijev).

Obvladovanje varnosti IS

Nadzor dostopa

- Dostop do podatkov in procesov:
  - zahteve za posamezne aplikacije in identifikacija vseh z njimi povezanih informacij;
  - politika avtorizacije in širjenja (principi in varnostna klasifikacija);
  - skladnost nadzora dostopa in klasifikacije;
  - uporaba standardnih profilov in kategorij;
  - skladnost z zakonodajo in pogodbami;
  - razlikovanje obveznih in pogojnih omejitev (npr. dovoljenje administratorjem za spremembe).

Obvladovanje varnosti IS

Nadzor dostopa

- Odgovornosti uporabnikov:
  - uporaba gesel (tajnost, regularno spreminjanje, kakovostna gesla);
  - nadzor opreme v odsotnosti uporabnikov (zaključevanje procesov, odjavljanje s sistema).
- Nadzor dostopa do omrežja:
  - politika (katera omrežja in katere storitve so dosegljive, postopki avtorizacije in nadzora);
  - dovoljene poti dostopa (določene telefonske številke, določene omrežne povezave);
  - overjanje uporabnikov in sistemov (zunanji uporabniki).

Obvladovanje varnosti IS

Nadzor dostopa

- Nadzor dostopa do omrežja:
  - uporaba tajnopisja in enkratnih gesel;
  - ranljivost posameznih vrat (ports);
  - fizično in logično segmentiranje omrežij za povečanje nadzora (obrambni zidovi);
  - definiranje dovoljenih aplikacij in storitev (e-pošta, splet, eno ali dvosmerni prenosi datotek, interaktivni dostop, dovoljeni čas dostopa),
  - nadzor usmerjanja in smeri izvajanja aplikacij.

Obvladovanje varnosti IS

Nadzor dostopa

- Nadzor dostopa pri operacijskih sistemih:
  - avtomatska identifikacija terminalov;
  - ustrezen postopek prijavljanja (dovoljeno število neuspelih poskusov, prikaz ključnih podatkov ob prijavi na sistem…);
  - uporaba tajnopisja in gesel za enkratno uporabo;
  - uporaba sistemskih virov (overjanje, dostop le za časa prijave na sistemu, beleženje);
  - avtomatski odklop neaktivnih terminalov;
  - omejitve glede časa dostopa;
  - podrobno beleženje dogodkov in sledenje dogodkom: ID, čas, kraj, (ne)uspele operacije;
  - časovna sinhronizacija.

Obvladovanje varnosti IS

Nadzor dostopa

- Nadzor dostopa do aplikacij - velja podobno kot za operacijske sisteme.
- Mobilni računalniki in delo na daljavo:
  - problem večje izpostavljenosti na javnih mestih;
  - problem nadzora komunikacijskih povezav;
  - uvedba ustreznega nadzora (oprema za fizično zaščito, določitev dovoljenega časa uporabe, opazovanje dejavnosti, določitev potrebne strojne in programske opreme in postopkov).

Obvladovanje varnosti IS

Nadzor dostopa

- Ščitenje sredstev zaradi groženj, ki so posledica dostopa zunanjih entitet - identifikacija tveganj:
  - Vrsti dostopa: fizični dostop (kabineti, rač. sobe…) in logični dostop (prek omrežij).
  - Razlogi za dostop: potrebna je ocena tveganj, ki upošteva vrsto dostopa, vrednost podatkov in posledice za celoten sistem.
  - Pogodbeni izvajalci znotraj organizacije (instalaterji, snažilke, študentje …).

Obvladovanje varnosti IS

Nadzor dostopa

- Ščitenje sredstev zaradi groženj, ki so posledica dostopa zunanjih entitet - potrebna določila pri pogodbenih izvajalcih:
  - opis generalne VP,
  - ščitenje virov, ki vključuje:
    - informacije in programsko opremo,
    - procedure za ugotavljanje zlorab,
    - postopke za izročitev oz. uničenje ustreznih informacij po preteku pogodbenega razmerja,
    - celovitost in razpoložljivost,
    - omejitve kopiranja in širjenja informacij.

Obvladovanje varnosti IS

Nadzor dostopa

- Ščitenje virov zaradi groženj, ki so posledica dostopa zunanjih entitet - potrebna so določila pri pogodbenih izvajalcih:
  - opis vsake storitve, ki bo dostopna,
  - predviden in minimalen nivo storitve,
  - morebiten transfer zaposlenih,
  - odgovornosti posameznih strank,
  - odgovornosti zaradi zakonodajnih zahtev (ščitenje poslovnih podatkov, varovanje intelektualne lastnine,…).

Obvladovanje varnosti IS

Nadzor dostopa

- Ščitenje virov zaradi groženj, ki so posledica dostopa zunanjih entitet - potrebna so določila pri pogodbenih izvajalcih:
  - dogovori o nadzoru dostopov (dovoljeni načini dostopa in identifikacije, procesi avtorizacije),
  - definicija kriterijev učinkovitosti, njihovo zajemanje in poročanje,
  - pravica nadzorovanja / izključitve uporabnikov,
  - pravica spremljanja pogodbenih obveznosti,
  - način reševanja konfliktnih situacij,
  - odgovornosti glede instalacije in vzdrževanje strojne in programske opreme.

Obvladovanje varnosti IS

Nadzor dostopa

- Ščitenje virov zaradi groženj, ki so posledica dostopa zunanjih entitet - potrebna določila pri pogodbenih izvajalcih:
  - jasni postopki poročanja in pripadajočih dokumentov,
  - specifikacija procedur za morebitne spremembe,
  - načini fizičnega varovanja in varovanja pred škodljivo programsko opremo,
  - usposabljanje uporabnikov in administratorjev,
  - postopki poročanja pri zlorabah,
  - pogodbeno vključevanje pod-izvajalcev.

Obvladovanje varnosti IS

Nadzor dostopa

- Ščitenje virov zaradi groženj, ki nastanejo pri dostopih zunanjih entitet - “outsourcing” (oddaja del):
  - zakonodajne zahteve,
  - načini zagotavljanja odgovornosti do varovanja podatkov s strani zunanjih izvajalcev,
  - kakšen bo nadzor in omejevanje dostopa do občutljivih poslovnih informacij naročnika,
  - zagotavljanje storitev v primeru katastrofe,
  - fizično varovanje naročnikove opreme,
  - pravica naročnika, da nadzoruje izvajalca.

Obvladovanje varnosti IS

Varovanje opreme

- Preprečevanje uničenja premoženja ali motenja poslovnih procesov.
  - Oprema mora biti nameščena tako, da je minimizirana možnost dostopa, vendar tako, da ne spregledamo občutljivih sporočil.
  - Kontrolirati moramo možnosti kraje, ognja, eksplozij, dima, vdora vode, prahu, vibracij, kemičnih reakcij, elektromagnetnega sevanja (interferenc).

Obvladovanje varnosti IS

Varovanje opreme

- Preprečevanje izpada napajanja:
  - več virov napajanja,
  - uporaba naprav UPS,
  - uporaba pomožnega generatorja.
- Varovanje kablov:
  - napajalni in podatkovni vodi za informacijske sisteme morajo biti nedosegljivi (npr. podzemni), a ločeni za preprečevanje interferenc;
  - omrežni vodi morajo biti zavarovani pred prestrezanjem (izogibanje javnih območij).

Obvladovanje varnosti IS

Varovanje opreme

- Vzdrževanje opreme:
  - skladno z navodili proizvajalca;
  - opravljano s strani avtoriziranega osebja;
  - beleženje izpadov;
  - nadzor opreme pri iznosu (popravila).
- Varnost dislocirane opreme - veljajo enaka pravila, kot znotraj organizacije, vendar zahtevajo dodaten nadzor (npr. dostop od doma).
- Odslužena oprema: uničenje podatkov.

Obvladovanje varnosti IS

Fizično varovanje poslovnega okolja

- Varovana območja - preprečevanje neavtoriziranega dostopa (škodovanje ali motenje poslovnih informacij).
  - Obseg varovanja (definicija območij).
  - Nadzor fizičnega dostopa (npr. pametne kartice).
  - Varovanje uradov: nedostopni pripomočki, nevtralen izgled prostorov, ščitenje vrat in oken ter neobljudenih prostorov z alarmi, odstranitev nevarnih materialov, dislokacija varnostnih kopij podatkov.

Obvladovanje varnosti IS

Fizično varovanje poslovnega okolja

- Varovana območja.
  - Delo v varovanih območjih:
    - osebje se mora zavedati ustreznega režima;
    - nenadzorovano delo v varovanih območjih ni dovoljeno zaradi nevarnosti ali zlorab;
    - neobljudena varovana območja morajo biti zaklenjena in periodično pregledovana;
    - prepovedana uporaba naprav za snemanje (slik, videa, zvoka).
  - Območja za predajo in prejem - izolirana od varovanih območij, materiali morajo biti pred vnosom pregledani in registrirani.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Nadzor sprememb:
  - identifikacija bistvenih sprememb,
  - ocena potencialnih vplivov teh sprememb,
  - formalna potrditev planiranih sprememb,
  - seznanjanje relevantnega osebja,
  - dodelitev odgovornosti.
- Neregularni dogodki:
  - obstoj procedur za obvladovanje ner. dogodkov,
  - obstoj procedur za analizo,
  - obstoj procedur za vzpostavitev prvotnega stanja.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Ločevanje uporabe:
  - ločitev okolij (različni procesorji, imeniki, domene),
  - ločitev testnih in produkcijskih aktivnosti (različne procedure za dostop, nedostopnost razvojnih orodij navadnim uporabnikom, nedostopnost produkcijskega okolja razvojnemu osebju).
- Upravljanje zunanje (dislocirane) opreme:
  - identifikacija občutljivih aplikacij, ki morajo biti nameščene znotraj organizacije;
  - pridobitev soglasja lastnika aplikacije;
  - implikacije za poslovne procese;
  - specifikacija standardov in ukrepov za sledenje;
  - definicija procedur in odgovornosti za nadzor, poročanje in obvladovanje neregularnih dogodkov.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Načrtovanje izvedbe in kriteriji za sprejemljivost rešitev.
  - Ustrezne kapacitete za preprečevanje preobremenitev.
  - Kriteriji sprejemljivosti:
    - performančne značilnosti,
    - postopki testiranja opreme in vzpostavitve prvotnega stanja ter ponovnega zagona,
    - vpliv na obstoječe stanje varnosti in nabor varnostnih kontrol,
    - zagotovilo, da nov sistem ne bo poslabšal karakteristik obstoječega sistema,
    - izobraževanje.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Škodljiva programska oprema - detektiranje (preprečevanje) vnosa:
  - zahteva za uporabo legalnega softvera,
  - ustrezni obravnavanje softvera, pridobljenega prek omrežja,
  - namestitev in vzdrževanje protivirusnih programov,
  - pregledovanje softvera in datotek,
  - postopki za odpravo virusnih napadov in poročanje ter vzpostavitev prvotnega stanja,
  - sledenje literaturi (CERTs).

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Redno vzdrževanje.
  - Delo z rezervnimi kopijami:
    - vsaj trinivojski “back-up”,
    - fizična dislokacija kopij in njihova zaščita,
    - regularno preverjanje medijev,
    - regularno preverjanje postopkov arhiviranja.
  - Beleženje dela operaterjev:
    - zagon in izključitev sistema,
    - sistemske napake in korekcije,
    - potrditev pravilnega delovanja,
    - ime operaterja in čas.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

  - Beleženje pomanjkljivosti:
    - opis in ime uporabnika, ki jo je zaznal,
    - pregled in opis odpravljanja napak.
- Upravljanje omrežij:
  - velja enako, kot za sisteme same, a
  - kontrole in odgovornosti morajo biti ločene.
- Manipulacija medijev z informacijami:
  - hranjenje v zavarovanem okolju skladno z zahtevami proizvajalca,
  - avtoriziran iznos.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Manipulacija medijev z informacijami - postopki uničevanja za vsak tip medija:
  - papir,
  - zvočni zapisi,
  - kopirni papir,
  - poročila,
  - trakovi tiskalnikov,
  - magnetni trakovi,
  - mehki in trdi diski, diski CD,
  - izpisi programske kode in testni podatki,
  - sistemska dokumentacija.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Izmenjava informacij in softvera - preprečevanje modifikacij in zlorab:
  - formalizirani dogovori (procedure, lastništvo, zadolžitve, nadzor, odgovornosti, označevanje, upoštevani standardi in zakonodaja);
  - varovanje pri transportu (avtorizirani transporterji - kurirji, ustrezno pakiranje, zaznamki za zaznavanje neavtoriziranega dostopa, ločeni kanali).

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Izmenjava informacij in softvera - varnost elektronskega poslovanja:
  - overjanje (določitev potrebne stopnja identifikacije prodajalca in kupca),
  - avtorizacija (kdo je avtoriziran za postavljanje cen, izdajo ključnih dokumentov, kako se o tem lahko prepriča partner),
  - pogodbeni postopki (zahteve za zaupnost, nezatajljivost, zagotovilo vročitve in prejema),
  - zaupnost in celovitost transakcij (nedostopnost do podatkov o posebnih popustih, nadzor izvedbene neoporečnosti transakcij).
  - opredelitev odgovornosti.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Izmenjava informacij in softvera - varovanje e-pošte s pomočjo kontrol za:
  - preprečevanje neavtoriziranega dostopa (zavračanje storitev, napačna vročitev),
  - vplivi na poslovne procese zaradi hitrejšega širjenja informacij, ki dobivajo značaj oseba-osebi in ne podjetje-podjetju,
  - legalne omejitve (dokazilo o izvoru, vročitvi, uporaba tajnopisja),
  - dostopnost imenikov z elektronskimi naslovi,
  - preverjanje priponk in virusov;
  - določitev, za katere namen je primerna e-pošta;
  - nadzor dostopa z oddaljenih lokacij.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Izmenjava informacij in softvera - varnost elektronskih pisarniških naprav (faksi, kopirni stroji, telefoni, mobilni telefoni…):
  - določitev ranljivosti - snemanje pogovorov, zaupnosti pogovorov, odpiranja pošte, distribucija pošte;
  - nadzor deljenja informacij in določitev, kateri medij je primeren za upravljanje določene vrste informacij;
  - kategorizacija uporabnikov in določitev časa in kraja, kjer lahko dostopajo do naprav;
  - izdelava varnostnih kopij in definicija postopkov v primeru zlorab.

Obvladovanje varnosti IS

Upravljanje komunikacij in obratovanja

- Izmenjava informacij in softvera - javno dostopni sistemi:
  - nujna avtorizacija pred objavo informacije,
  - nujna zaščita integritete javno objavljenih inf.,
  - informacije morajo biti pridobljene skladno z zakonom (nedostopnost občutljivih informacij),
  - kanali do javnih informacij ne smejo ogrožati preostalega sistema.
  - Preostali načini izmenjave informacij:
    - problem prisluškovanja mobilnim telefonom,
    - puščanje sporočil na odzivnikih,
    - problem zaupne komunikacije na javnih mestih.

Obvladovanje varnosti IS
Razvoj in vzdrževanje sistemov

- Varnostne zahteve.
  - specifikacija splošnih varnostnih zahtev;
  - uvajanje novih rešitev (postopki testiranja);
  - varnost aplikacij:
    - kontrola veljavnosti vhodnih podatkov,
    - nadzor internega procesiranja,
    - overjanje in celovitost izmenjanih sporočil,
    - kontrola veljavnosti izhodnih podatkov.

Obvladovanje varnosti IS
Razvoj in vzdrževanje sistemov

- Tajnopisne kontrole:
  - politika uporabe (splošni principi, upravljanje ključev vključno s problematiko izgubljenih ključev, obnovljenih ključev, vloge in odgovornosti, določitev nivojev tajnopisne zaščite);
  - tajnopisni postopki: osnova analiza tveganj in oceno škode, uporaba skladno z zakonodajo;
  - digitalni podpis: predvsem poudarek na ščitenju privatnega ključa, njegovi dolžini in vrsti postopka, sicer velja enako kot za tajnopisne sisteme.

Obvladovanje varnosti IS

Razvoj in vzdrževanje sistemov

- Varnostne zahteve - upravljanje ključev:
  - zaščita pred razkritjem, modifikacijo in uničenjem (tudi fizična);
  - upoštevanje standardov glede generiranja, certificiranja, porazdeljevanja, hranjenja, izmenjave, osveževanja, preklicevanja, rekonstrukcije, arhiviranja, uničevanja in sledenja.

Obvladovanje varnosti IS

Razvoj in vzdrževanje sistemov

- Varnost sistemskih datotek - nadzor operativne programske opreme:
  - operativna programska oprema mora vsebovati le izvršljivo kodo;
  - koda ne sme biti v operativni uporabi dokler ni uspešno prestala testiranja;
  - voditi moramo sistemsko beleženje vseh nadgradenj;
  - predhodne različice moramo hraniti kot rezervo.

Obvladovanje varnosti IS

Razvoj in vzdrževanje sistemov

- Varnost sistemskih datotek - zaščita sistemskih testnih podatkov:
  - uporabiti moramo namišljene podatke in enake postopke nadzora dostopa, kot pri operativnih podatkih;
  - izvesti moramo posebno avtorizacijo za vsako kopiranje operativnih podatkov v testno okolje hkrati s sistemsko zabeležko.
  - Nadzor dostopa do izvorne kode: testne podatke moramo ločiti od operativnega sistema, določiti lastnika, jih hraniti v varnih prostorih, beležiti modifikacije in arhivirati stare različice.

Obvladovanje varnosti IS

Razvoj in vzdrževanje sistemov

- Zaščita pri razvoju in nadgradnji - procedure za nadzor sprememb:
  - vpeljava več stopenj avtorizacije, ki jo morajo ustrezni uporabniki izrecno sprejeti,
  - preprečevanje degradacije celovitosti obstoječega sistema,
  - identificirati moramo softverske komponente in zbirke podatkov, ki se jih tiče nadgradnja,
  - zagotoviti moramo ažuriranje sistemske dokumentacije in hranjenje stare dokumentacije,
  - beležiti sistemske spremembe in opravljati spremembe v primernem času.

Obvladovanje varnosti IS
Razvoj in vzdrževanje sistemov

- Zaščita pri razvoju in nadgradnji.
  - Spremembe sistemske opreme:
    - morajo biti plansko predvidene (tudi finančno);
    - morajo biti pravočasno najavljene,
    - predvideti moramo kontrole za preverjanje funkcionalnosti aplikacijske opreme.
  - Omejitve modifikacij:
    - te so načelno sprejemljive le, če jih opravi proizvajalec;
    - če sami izvajamo modifikacije, je potrebno soglasje proizvajalca, vpeljava kontrol, vodenje dokumentacije.

Obvladovanje varnosti IS
Razvoj in vzdrževanje sistemov

- Zaščita pri razvoju in nadgradnji.
  - Skriti kanali in Trojanski konji:
    - uporaba programov priznanega proizvajalca;
    - uporaba evaluiranih programov v izvorni kodi;
    - pregled izvorne kode in nadzor dostopa in modifikacij opreme.
  - Razvoj s strani zunanjih izvajalcev:
    - licenčne pogodbe;
    - upravljanje kakovosti (certificiranje) in možnost nadzora (dostop do posameznih faz);
    - testiranje in garancije.

Obvladovanje varnosti IS
Neokrnjenost poslovnih aktivnosti

- Definicija ustreznih postopkov:
  - Razumevanje nevarnosti, njihove identifikacije, verjetnosti neželenih dogodkov in razvrščanja.
  - Dokumentiranje relevantne strategije.
  - Redno preverjanje in nadgradnja.
  - Vključitev zavarovalnic in zavarovanj.
  - Postopki za neokrnjenost poslovnih procesov morajo vsebovati:
    - pogoje aktiviranja;
    - zaporedje reševalnih postopkov (vključevanje kriminalistov, javnosti in aktivnosti na novi lokaciji za vzpostavitev polne funkcionalnosti);
    - načrt za vzpostavitev prvotnega stanja;
    - načrt osveževanja, testiranja in izobraževanja.

Obvladovanje varnosti IS
Preverjanje skladnosti

- Skladnost z zakonodajnimi zahtevami.
  - Identifikacija relevantne zakonodaje.
  - Ščitenje intelektualne lastnine: postopki za nakup in instalacijo, hranjenje licenc, politika prenosa softvera tretjim osebam.
  - Varovanje dokumentacije: kategorizacija, določitev medijev in načina hranjenja (staranje medijev), hranjenje ključev pri digitalnih podatkih.
  - Preprečevanje nedovoljene uporabe (nadzor avtorizirane uporabe, obvestila pri prijavljanju na sistem o dovoljeni uporabi in zahteva po potrditvi).
  - Uporaba tajnopisja - izvozno uvozne omejitve, dovoljeni načini uporabe.
  - Zbiranje evidenc - pravila, dopustnost, kakovost in popolnost (ščitenje podatkov in zasebnosti).

Obvladovanje varnosti IS

Preverjanje skladnosti

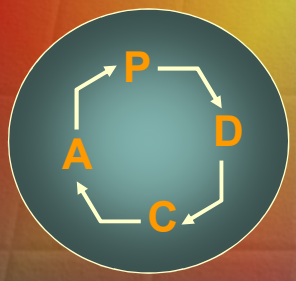
- Skladnost s tehničnimi specifikacijami:
  - v varnost usmerjeni standardi - Common Criteria (CC),
  - ostali tehnični standardi.
- Skladnost z organizacijskimi, to je revizijskimi in akreditacijskimi standardi (ISO 17799).
- Skladnost nadzora za čim večjo učinkovitost in čim manjše motenje poslovnih procesov.

Obvladovanje varnosti IS

- Najpomembnejša domača zakonodaja.
  - Kazenski zakonik.
  - ZEPEP - Zakon o elektronskem poslovanju in elektronskem podpisu.
  - ZEPEP-A - Zakon o spremembah in dopolnitvah zakona o elektronskem poslovanju in elektronskem podpisu
  - Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje.
  - ZEKom - Zakon o el. komunikacijah.
  - Zakon o varstvu osebnih podatkov.

BS 7799(2)-
Information Security Management System

- Sistem vodenja za varovanje informacij v organizaciji.
- Temelji na Demingovem krogu (PDCA):
  - načrtuj (plan),
  - vpelji in izvajaj (do),
  - preverjaj (check)
  - nadgrajuj in izboljšuj (act).



Evolucija BS 7799

- ISO 27001
  - Standard za sisteme obvladovanja informacijske varnosti - SOIV (information security management system – ISMS), nadomešča BS7799-2.
- ISO 27002
  - Ta je naslednik ISO 17799, ki je standard dobrih poslovnih običajev na področju infomrmacijske varnosti in nadomešča BS7799-1.

Evolucija BS 7799

- ISO 27003
  - To bo nov standard, ki bo podajal navodila za vzpostavitev SOIV.
- ISO 27004
  - Ta standard bo pokrival obvladovanje ISMS s tem, da bo podajal načine kvantitativnega vrednotenja (merjenja) učinkovitosti SOIV.

Evolucija BS 7799

- ISO 27005
  - Ta standard bo v zvezi z SOIV posebej osredotočen na obvladovanje tveganj (risk management).
- ISO 27006
  - Ta standard bo podajal konkretna navodila, kako in s katerimi koraki lahko organizacije pridobijo akreditacijo za podajanje certifikatov SOIV.

Standarda ISO/IEC 18043 in 18044

- Standarda se nanašata na sisteme za detekcijo vdorov – SDV (angl. intrusion detection systems).
- Predstavljata primer, kako je hitro spreminjajoča se tehnologija pripeljala do nuje po usklajenih organizacijskih postopkih, na čemer je tudi poudarek teh dveh standardov.

Standard ISO/IEC 18043

- IT, Security techniques, Selection, deployment and operations of IDS:
  - Daje osnovna vodila organizacijam, ki želijo uporabljati SDV.
  - Pojasnjuje kaj so SDV, našteva njihove prednosti in slabosti.
  - Daje izhodišča za strategijo v zvezi z njihovo namestitvijo in konfiguracijo ter integracijo z širšo varnostno politiko.

Standard ISO/IEC 18043

- IT, Security techniques, Selection, deployment and operations of IDS:
  - Izpostavlja in obravnava zakonske vidike s poudarkom na varovanju zasebnosti.
  - Vzpostavlja okvir za sodelovanje med organizacijami (povezovanje SDV) v smislu možnosti izmenjevanja ustreznih podatkov.
  - Daje priporočila, ki so usmerjena na organizacijski nivo.

Standard ISO/IEC 18044

- IT, Security techniques, Information Security Incident Management:
  - Podaja usmeritve in nasvete za ustrezne odzive na vdore, namenjene upravljavcem in skrbnikom informacijske varnosti.
  - Podaja podrobno strukturirane procese (sheme) varovanja – od načrtovanje, prek poročanja do povratnih informacij za obvladovanje vdorov.
  - Vključuje primere vdorov.

Zaključek

- Zagotavljanje informacijske varnosti postaja ena od osrednjih dejavnosti za zagotavljanje nemotenega poslovanja in ohranjanje poslovnega ugleda.
- Celovito obvladovanje informacijske varnosti izhaja iz poznavanja tehnoloških osnov, vendar mora biti ustrezno nadgrajeno z organizacijskimi, zakonodajnimi in revizijskimi postopki.
- Varnost je proces in ne stanje; je nujna za sodobno (elektronsko) poslovanje.