Kriptografija

Matej Kovačič

There are 10 kind of people, those who understand binary and those who don't.

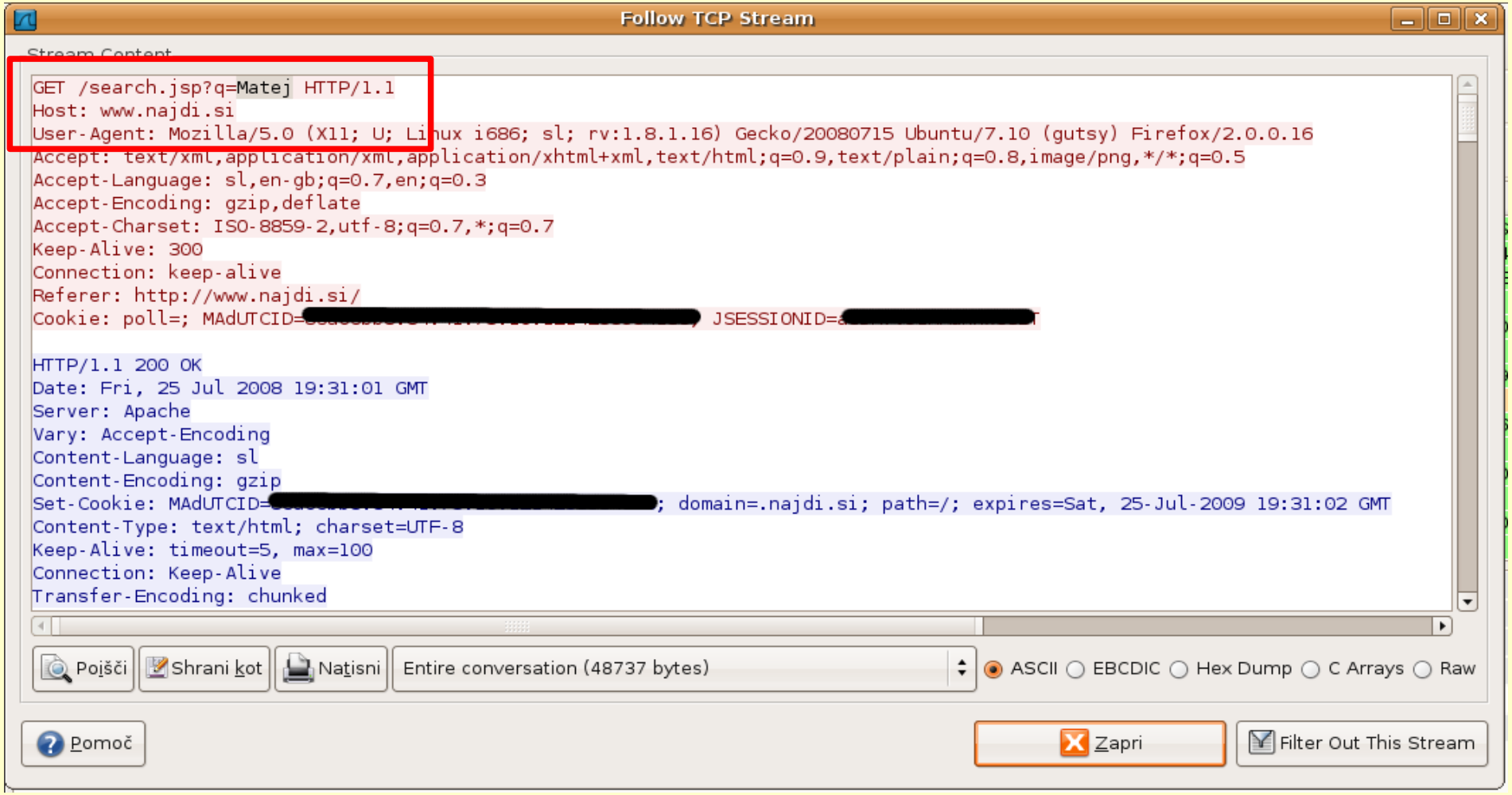
I: Uvod

- Zakaj kriptografija?
- Primer prestrezanje in prisluškovanje HTTP in HTTPS prometu, prisluškovanje nešifriranem SIP prometu.
- Kriptografija in zasebnost.
- Pravni vidiki uporabe kriptografije.
- Začetki in kratka zgodovina kriptografije.

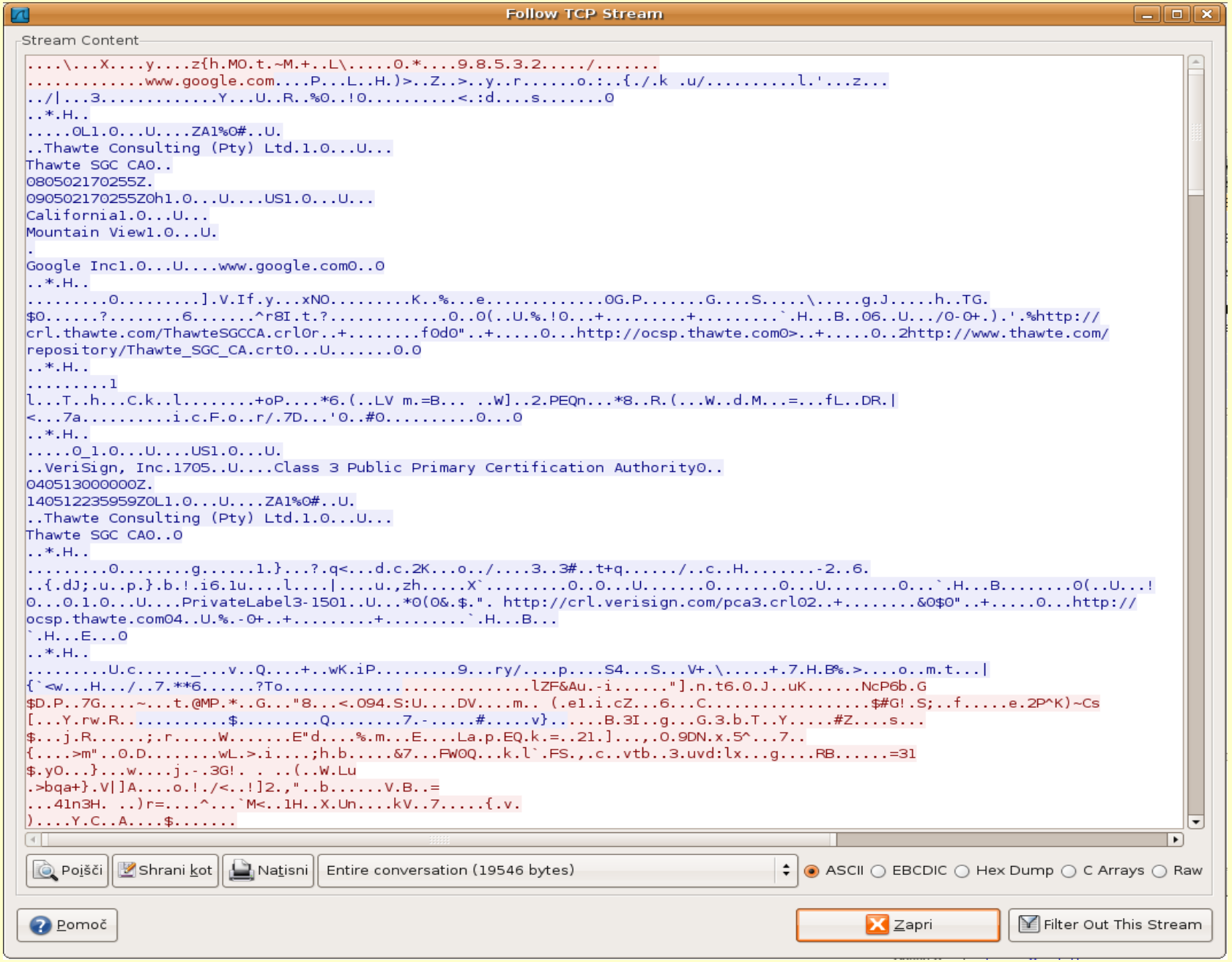
Osnovni pojmi

- Beseda kriptografija izvira iz grškega izraza *kryptos logos*, ki pomeni skrita beseda, prvi pa jo je v angleščini uporabil sir Thomas Browne leta 1658.
- Kriptologija je veda o tajnosti, šifriranju, zakrivanju vsebine sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza).
- S pomočjo kriptografije lahko onemogočimo prisluškovanje komunikacijam.
- Kriptoanaliza se ukvarja z razbijanjem šifriranih sporočil.

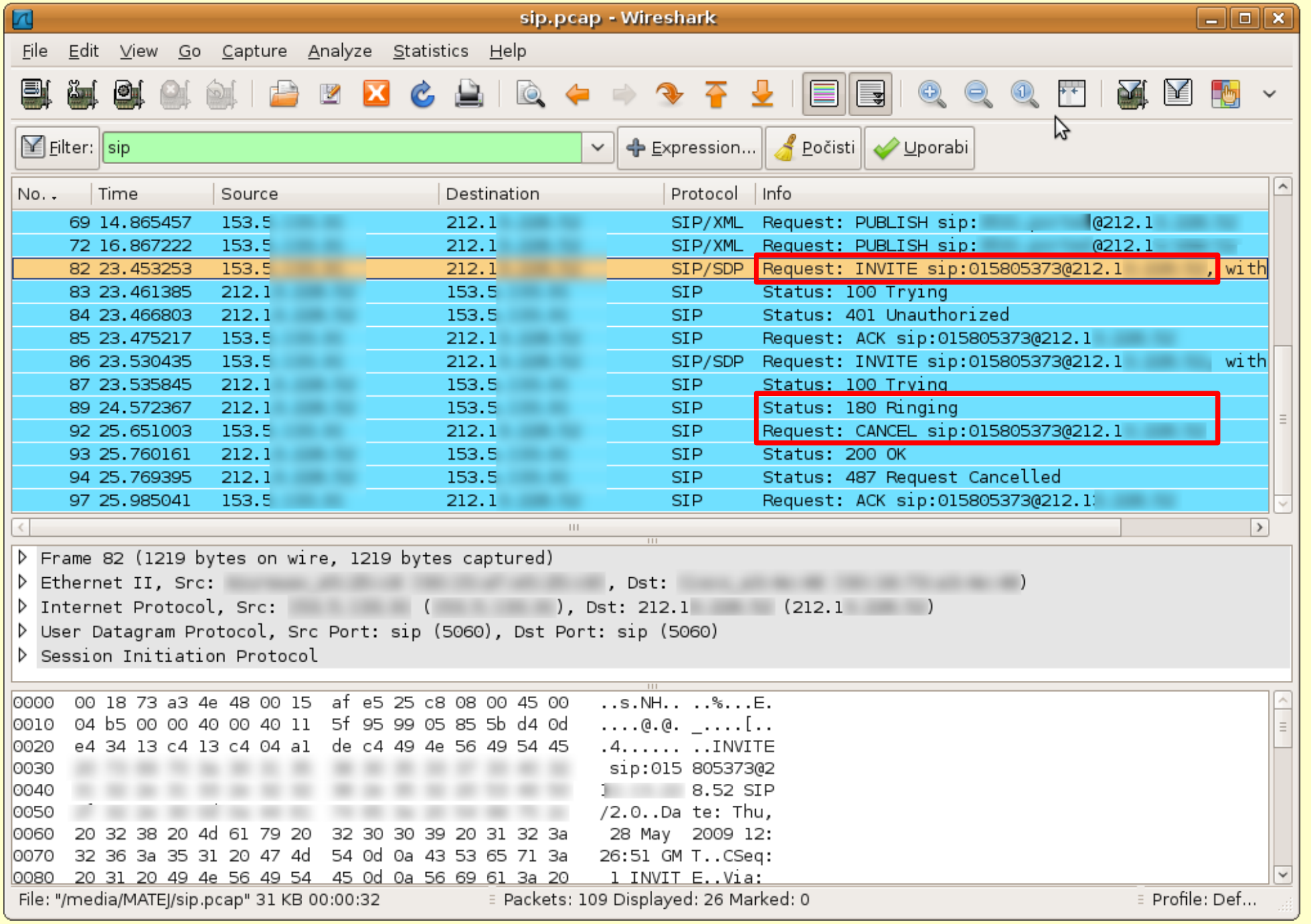
Zakaj kriptografija?



Nešifrirana spletna komunikacija.



Šifrirana spletna komunikacija.


sip.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: sip
Expression... Počisti Uporabi
No. Time Source Destination Protocol Info
69 14.865457 153.5 212.1 SIP/XML Request: PUBLISH sip: @212.1
72 16.867222 153.5 212.1 SIP/XML Request: PUBLISH sip: @212.1
82 23.453253 153.5 212.1 SIP/SDP Request: INVITE sip:015805373@212.1 , with
83 23.461385 212.1 153.5 SIP Status: 100 Trying
84 23.466803 212.1 153.5 SIP Status: 401 Unauthorized
85 23.475217 153.5 212.1 SIP Request: ACK sip:015805373@212.1
86 23.530435 153.5 212.1 SIP/SDP Request: INVITE sip:015805373@212.1 with
87 23.535845 212.1 153.5 SIP Status: 100 Trying
89 24.572367 212.1 153.5 SIP Status: 180 Ringing
92 25.651003 153.5 212.1 SIP Request: CANCEL sip:015805373@212.1
93 25.760161 212.1 153.5 SIP Status: 200 OK
94 25.769395 212.1 153.5 SIP Status: 487 Request Cancelled
97 25.985041 153.5 212.1 SIP Request: ACK sip:015805373@212.1
Frame 82 (1219 bytes on wire, 1219 bytes captured)
Ethernet II, Src: , Dst:)
Internet Protocol, Src: ( ), Dst: 212.1 (212.1)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
0000 00 18 73 a3 4e 48 00 15 af e5 25 c8 08 00 45 00 ..s.NH.. ..%...E.
0010 04 b5 00 00 40 00 40 11 5f 95 99 05 85 5b d4 0d ....@.@. _....[..
0020 e4 34 13 c4 13 c4 04 a1 de c4 49 4e 56 49 54 45 .4...... ..INVITE
0030 sip:015 805373@2
0040 8.52 SIP
0050 /2.0..Da te: Thu,
0060 20 32 38 20 4d 61 79 20 32 30 30 39 20 31 32 3a 28 May 2009 12:
0070 32 36 3a 35 31 20 47 4d 54 0d 0a 43 53 65 71 3a 26:51 GM T..CSeq:
0080 20 31 20 49 4e 56 49 54 45 0d 0a 56 69 61 3a 20 1 INVIT E..Via:
File: "/media/MATEJ/sip.pcap" 31 KB 00:00:32
Packets: 109 Displayed: 26 Marked: 0
Profile: Def...

Varnost ni izdelek

- Varnost ni izdelek oziroma nekaj, kar lahko kupimo, namestimo in pozabimo, pač pa gre za proces.
- Varnostno kulturo je treba razvijati in gojiti neprestano.

- Informacijska varnost in varnost v prometu: ni dovolj samo dober avto in opravljen izpit, znanje o varnosti je potrebno obnavljati in uporabljati neprestano.

Kaj je varnost?

- Overjanje, avtentikacija (ang. *authentication*): kdo je pošiljatelj, ko je prejemnik?
- Zaupnost (ang. *confidentiality*): sporočilo ostane znano samo pošiljatelju in prejemniku.
- Nadzor nad dostopom (ang. *access control*): kdo lahko dostopi do sporočila, beleženje dostopov.
- Avtorizacija (ang. *authorization*): kaj nekdo s sporočilom lahko stori?
- Dostopost (ang. *availability*): je sporočilo dostopno?

Kaj je varnost?

- Celovitost (ang. *integrity*): sporočilo ostane nespremenjeno.
- Preprečevanje tajenja (ang. *nonrepudiation*): pošiljatelj kasneje ne more zatajiti sporočila, prejemnik ne more zatajiti prejema.
- Dopustnost (ang. *admissibility*): varnost terminalne opreme, zagotovilo, da na terminalni opremi na kateri se bo avtenticiral uporabnik in kjer bo uporabnik bral sporočilo ni zlonamernih mehanizmov.

Kriptografija in zasebnost

- Zasebnost je človekova pravica.
- Kriptografija:
  - omogoča komunikacijsko zasebnost (e-pošta vs. razglednica),
  - povečuje varnost finančnih transakcij,
  - omogoča izpolnjevanje naših pravnih obveznosti pri varovanju poslovnih skrivnosti, osebnih podatkov, tajnih podatkov...
  - varuje naše podatke na nosilcih podatkov in v oblaku,
  - omogoča digitalno podpisovanje, preverjanje integritete podatkov in programske opreme.

Pravni vidiki kriptografije

- Uporaba kriptografije v večini demokratičnih držav ni ne prepovedana, ne omejena.
- Omejen je izvoz močne kriptografije v nekatere države.
- ZKP, 5./III: "*Obdolženec se ni dolžan zagovarjati in odgovarjati na vprašanja, če pa se zagovarja, ni dolžan izpovedati zoper sebe ali svoje bližnje ali priznati krivde.*"

Pravni vidiki kriptografije

- Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku, 219. a/VI: "*Imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave. Če noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. člena tega zakona, razen če gre za osumljenca ali obdolženca ali osebo, ki ne sme biti zaslišana kot priča (235. člen) ali se je v skladu s tem zakonom odrekla pričevanju (236. člen).*"

Pravni vidiki kriptografije

- Regulation of Investigatory Powers Act 2000 (Velika Britanija), Part III, Investigation of electronic data protected by encryption etc.:
  - RIPA predvideva prisilna dejanja za imetnika šifrirnega ključa: omogočiti mora dostop do nešifriranih podatkov ali izročiti šifrirni ključ.
  - V primeru nesodelovanja je zagroženo do 2 leti zaporne kazni.
  - Prvi primer uporabe tega člena je bil proti skupini, ki se zavzema za pravice živali.
  - Problem: kaj če bi obdolženi z razkritjem podatkov dobil kazen višjo od 2 let zapora?
  - Problem: verodostojno zanikanje.

Pravni vidiki kriptografije

- Prenosniki na mejah:
  - In re Boucher: zaseg na meji leta 2006, na Z: disku najdejo otroško pornografijo, a računalnik ugasnejo. 2007 je sodišče presodilo, da bi bilo razkritje gesla oblika pričanja. 2009 pa je višje sodišče presodilo, da mora osumljeni omogočiti dostop do vsebine šifriranega diska, katerega vsebino so pred tem že videli mejni policisti. Temelj za tako odločitev je bilo dejstvo, da je obdolženi pred tem policistom že pokazal dešifrirano vsebino diska.

Pravni vidiki kriptografije

- Prenosniki na mejah:
  - Kalifornijsko prizivno sodišče je leta 2008 razsodilo, da mejni kontrolni organi lahko preiščejo osebne računalnike brez sodne odredbe in tudi v primeru, da ne zaznajo kakršnekoli kriminalne aktivnosti.
  - Podobno je leta 2005 presodilo tudi Prizivno sodišče četrtega okrožja.
  - Leta 2006 so so sudanske varnostne sile na letališčih pričele zasegati in pregledovati prenosne računalnike, uradno zaradi prepovedi vnosa pornografije.

Pravni vidiki kriptografije

- Prenosniki na mejah:
  - Leta 2008 (pred olimpijskimi igrami v Pekingu) so ameriške protiobveščevalne službe izdale posebno opozorilo, v katerem svoje državljane svarijo pred kibernetskim vohunjenjem.

Več nadzora - več uporabe kriptografije?

- Obveščevalne službe v Veliki Britaniji se bojijo posledic preveč drakonske zakonodaje na področju nadzora. Razlog, ki ga citirajo je ta, da bodo, zaradi samozaščite uporabnikov in izogibanja sledenju, postale rešitve za šifriranje in skrivanje prometa vedno bolj tehnološko dovršene in hkrati tudi vedno lažje za uporabo istočasno pa bodo prešle tudi v možično uporabo.

Več nadzora - več uporabe kriptografije?

- Ker se je omejevanje P2P prometa že usmerilo v odkrivanje t.i. tipičnih profilov delovanja aplikacij - *traffic pattern fingerprinting*, bo to pomenilo, da se bo začelo uporabljati rešitve, ki se bodo trudili zakriti tudi vir ter ponor komunikacije in tip komunikacije, ne več samo vsebino komunikacije. Verjetno ni težko razumeti zakaj takšen splošen položaj državnim prisluškovalcem več ne bi ustrezal. Brez vsebine so podatki še vedno uporabni. Brez prometnega konteksta pa je to samo beli šum, ki ga znotraj ene države ni možno "prebiti".

Vir: Digitalna EU ta teden, 24. oktober 2009, Slo-Tech, <https://slo-tech.com/forum/t381677>

Začetki kriptografije

- Egiptovski nestandardni hieroglifi okrog leta 1900 pr. n. š.
- Kriptografijo so v zgodovini uporabljali večinoma za vojaške in politične namene npr. Rimljani (Cezarjev algoritem).
- Nekje okrog leta 1400 so na Zahodu začeli v večji meri šifrirati vsebino občutljivih pisem.
- Leta 1466 ali 1467 je Leon Batista Alberti napisal enega najstarejših znanih zahodnih esejev o kriptoanalizi.
- Sodobna zahodna kriptografija se je razvila kot posledica moderne diplomacije.

Začetki kriptografije

- V Benetkah je Giovanni Soro leta 1506 in 1510 opravil prve večje uspešne kriptoanalize šifriranih sporočil.
- Leta 1861 se v ZDA pojavi prvi kriptografski patent.
- Leta 1923 je Arthur Scherbius začel proizvajati šifrirne stroje Enigma (izboljšane različice so kasneje med drugo svetovno vojno uporabljali Nemci).
- V 30-tih letih 20. stol. je kriptografija začela postajati mehanizirana. Moderno kriptografijo je ustvaril telegraf.
- S pojavom radia, ki je omogočal enostavno nepooblaščeno prisluškovanje, pa se je razvila moderna kriptoanaliza.

Začetki kriptografije

- Sprva so za šifriranje (Enigma, Lorenz,...) in razbijanje šifer uporabljali mehanske naprave (Bombe, Colossus), kasneje pa računalnike s procesorji.
- Leta 1976 sta matematika Whitfield Diffie in Martin E. Hellman objavila kjer sta opisala protokol za varno izmenjavo šifrirnih ključev prek nezaščitenega medija, znano tudi kot sistem šifriranja z javnimi ključi.
- Leta 1977 so Ronald L. Rivest, Adi Shamir in Leonard M. Adleman opisali algoritem RSA.
- Leta 1991, je Philip R. Zimmerman napisal računalniški program PGP (Pretty Good Privacy).

Začetki kriptografije

- Sledila je “vojna proti javno dostopni kriptografiji”.
- Danes se kriptografija uporablja predvsem pri elektronskem poslovanju in zaščiti avtorskih pravic, pa tudi pri izmenjavi podatkov ter medosebnem komuniciranju.

II: Osnovni pojmi

- Koda vs. šifra.
- Osnovni šifrirni algoritmi in tehnike (Atbash, Cezarjev in Vigenerejev algoritem,... One Time Pad)
- Simetrična in asimetrična kriptografija.
- Zgostitveni algoritmi (lastnosti, uporaba in napadi).
- Digitalni podpis.
- Šifrirni ključ in šifrirno geslo (*passphrase*).
- Šifrirni kontejner.
- Steganografija in verodostojno zanikanje.

II: Osnovni pojmi

- Shrambe ključev in strojni žetoni.
- Overovitev.
  - PKI kriptografija (“*web of trust*” javnih ključev).
  - Certifikati in CA.
- Problem MITM napada.
- Varnost terminalnih naprav (tim. “*Pentagon of trust*”).

- Šifriranje komunikacij (e-pošte, IM, VoIP, ZRTP protokol) in šifriranje nosilcev podatkov.

Koda vs. šifra

- Koda, kodiranje: gre za zamenjavo besed (ali fraz) z drugimi besedami (frazami), ki so vnaprej pripravljene v tim. kodirni knjigi.
- Šifra, šifriranje: kode “delujejo” na nivoju pomenov (besed ali fraz), šifre pa na nivoju posameznih črk, bitov ali skupin črk.
- Pri šifriranju ne potrebujemo kodirne knjige, s pomočjo računalnikov ga je mogoče lažje izvajati.
- "Climb Mount Niitaka" (koda za napad na Pearl Harbour), “Dobiva se na kavi!!” (prinesi 2 g (število klicajev) droge),...

Osnovni pojmi

- Čistopis (ang. *cleartext*, *plaintext*) je temeljno, originalno sporočilo.
- Šifropis ali tajnopis (*kriptogram*, *ciphertext*) je zašifrirano sporočilo.
- Čistopis po nekem postopku (algoritmu, metodi) spremenimo v tajnopis, pri tem pa uporabimo neke vrednosti za parametre v šifrirnem algoritmu. Tem vrednostim pravimo ključ ali geslo.

Atbash

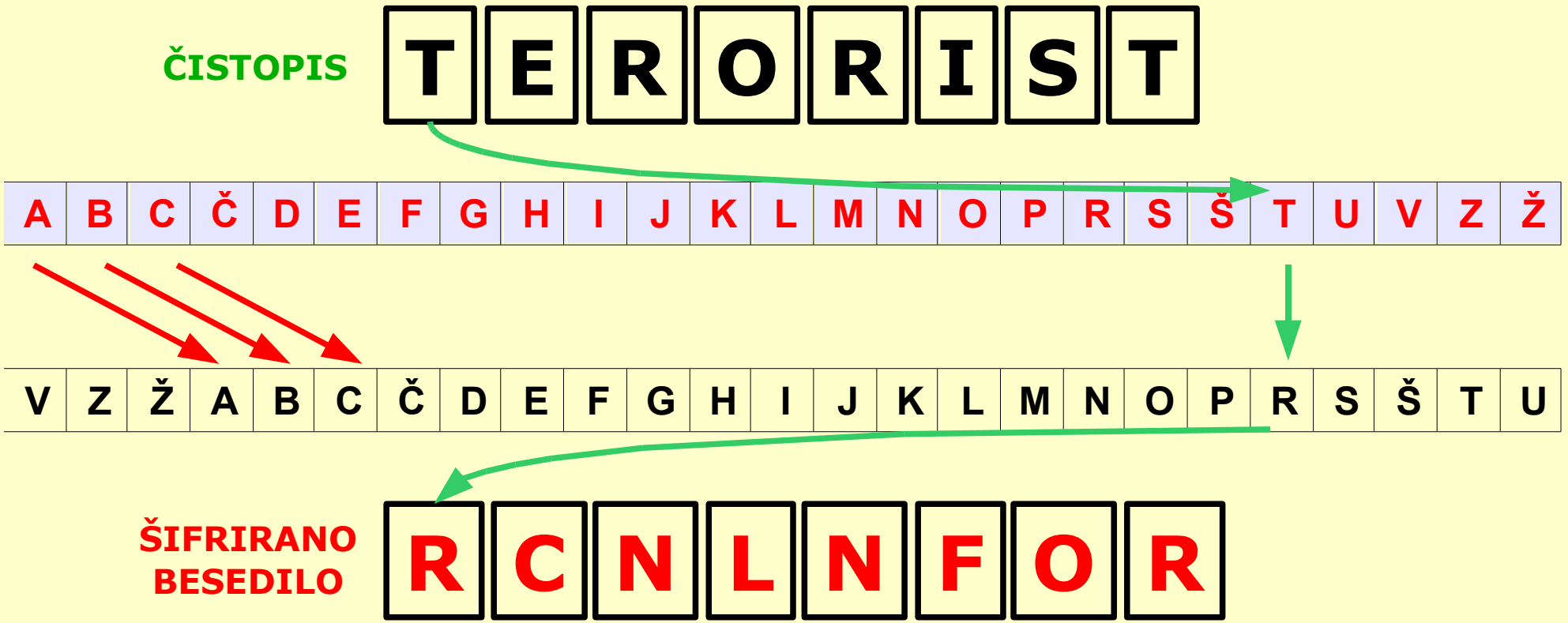
A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
↓																								
Ž	Z	V	U	T	Š	S	R	P	O	N	M	L	K	J	I	H	G	F	E	D	Č	C	B	A

ŠIFRIRANO BESEDILO

J	Ž	H	Ž	T

- Atbash so okrog 600-500 pr. n. št. pričeli uporabljati Hebrejci. Gre za obrnjeno abecedo.
- Gre za substitucijski monoalfabetni algoritem. Šifrirni ključ je en sam.

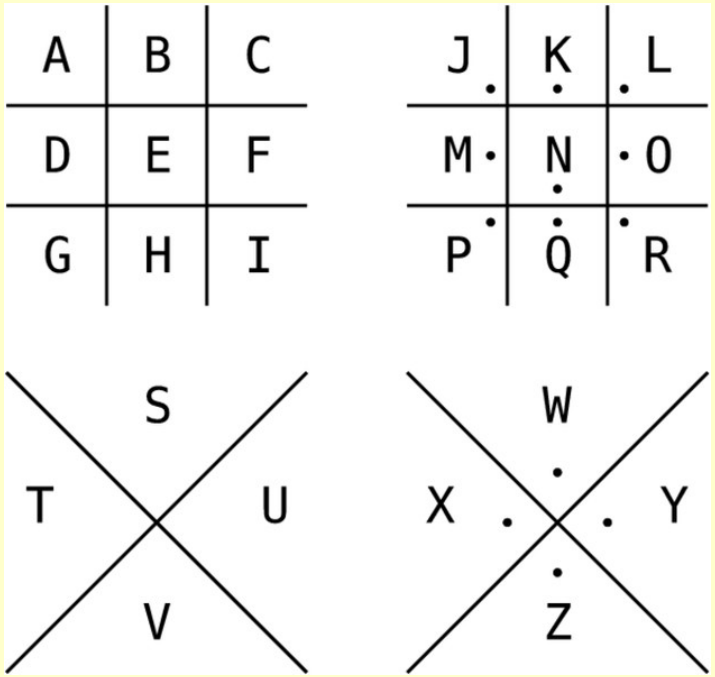
Cezarjev algoritem



- Gre za substitucijski monoalfabetni algoritem. Šifrirni ključ določa, za koliko mest se premakne tajna abeceda glede na običajno abecedo.
- Algoritem je veliko uporabljal Julij Cezar, praviloma z zamikom 3 znake.

Pigpen ali framazonski algoritem

- Pigpen ali framazonski algoritem so v 18. stoletju uporabljali framazoni. Gre za preprost substitucijski algoritem, ki namesto navadnih črk uporablja simbole.



Substitucijska tabela.

Skital

- Uporabljali so ga antični Grki za vojaške namene.
- Gre za palico, okrog katere navijemo trak...

N	A	P	A	D
D	A	N	E	S
O	B	E	N	I

Šifrirano sporočilo:
NDOAABPNEAENDSI

Vir in avtorstvo: Wikipedia, geslo: Scytale.

ROT13

- Substitucijski algoritem, ki tabelo znakov zarotira za 13 mest. Je inverzen.
- Funkcija v OpenOffice: =ROT13(“BESEDILO”).
- Uporabljali so ga za “skrivanje” potencialno žaljivih šal na Usenetu. Danes se še vedno uporablja v nekaterih produktih, recimo v Windows Xp za “kodiranje” nekaterih ključev v registru.
  - Kakšna je razlika med odvetniki in teroristi?
  - F grebevfgv arxngrev ywhqwr ghqv fvzcngvmvenwb!

Varnost preprostih substitucijskih algoritmov

KCJANFGKL

LDKBOGHLM

MELCPHIMN

NFMDQIJNO

OGNERJKOP

PHOFSKLPQ

QIPGTLMQR

RJQHUMNRS

SKRIVNOST

TLSJWOPTU

UMTKXPQUV

VNULYQRVW

WOVMZRSWX

Vigenerèjev algoritem

- Gre za polialfabetni algoritem, ki za šifrirni ključ uporablja geslo.
- Prvi opis polialfabetnega šifrirnega algoritma je okrog leta 1467 zapisal Leon Battista Alberti.
- Leta 1508 je Johannes Trithemius izumil šifrirno tabelo *tabulo recto*, algoritem pa je leta 1553 v svoji knjigi *La cifra del. Sig. Giovan Battista Bellaso* opisal Giovan Battista Bellaso.
- V 19. stoletju so izumiteljstvo algoritma zmotno pripisali Blaiseju de Vigenèreju.

Vigenerèjev algoritem

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	O
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	P	R	S	Š	T	U
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

GESLO

N	A	P	A	D	N	A	P

ČISTOPIS

T	E	R	O	R	I	S	T

ŠIFRIRANO BESEDILO

I	E	H	O	U	Z	S	K

- Geslo iščemo po stolpcih.
- Navadno besedilo iščemo po vrsticah.
- Presek nam da šifrirano besedilo.

Šifrirna tabela *tabula recta*.

Mehanske šifrirne naprave

- Albertijev *šifrirni disk* (opisal ga je Leon Battista Alberti v delu De Cifris leta 1467)

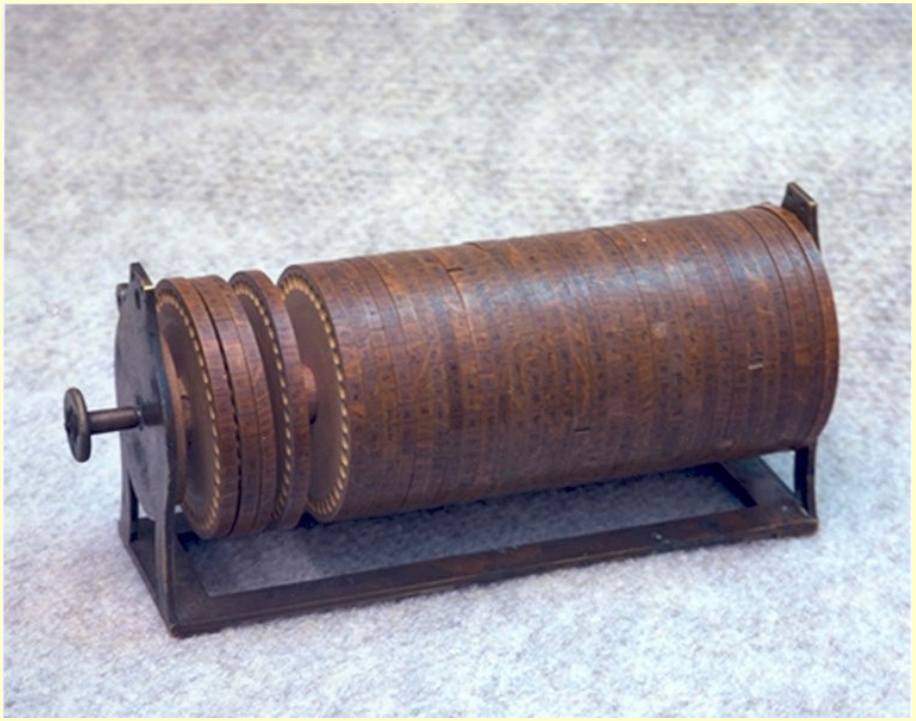
Vir in avtorstvo: Wikipedia, geslo: Alberti cipher disk

Mehanske šifrirne naprave

- *Šifrirni valj* (izumil ga je Thomas Jefferson 1790), kasneje pa ga je neodvisno izumil tudi Etienne Bazeries).
- Inačico M-94 je leta 1917 izumil major Joseph Mauborgne, uporabljala pa ga je ameriška vojska.
- Ključ v Bazeriesovem cilindru predstavlja vrstni red kolesc.

Mehanske šifrirne naprave

```
7:   R AFDCE O NJQGWTHSPYBXIZULVKM
9:   E NYVUB M CQWAOIKZGJXPLTDSRFH
5:   T SGJVD K CPMNZQWXYIHFRLABEUO
10:  R SCZQK E LMXYIHPUDNAJFBOWTGV
1:   E ZWAXJ G DLUBVIQHKYPNTCRMOSF
6:   A MKGHI W PNYCJBFZDRUSLOQXVET
3:   T EQGYX P LOCKBDMAIZVRNSJUWFH
8:   N OZUTW D CVRJLXKISEFAPMYGHBQ
2:   O YHGVS F UWIKPBELNACZDTRXMJQ
4:   W AORPL N DVHGFCUKTEBSXQYIZMJ
```



Vir in avtorstvo: Wikipedia, geslo: Jefferson disk

Mehanske šifrirne naprave

Vir in avtorstvo: Wikipedia, geslo:
Enigma machine

One time pad

- One-time pad, tudi one-time tape ali one-time letter pad.
- Leta 1917 sta ga odkrila Gilbert S. Vernam iz AT&T ter vodja kriptografskih raziskav ameriške vojske med prvo svetovno vojno major Joseph Mauborgne.
- Edini, ki je tudi teoretično nezlomljiv, če je pravilno uporabljen:
  - ključ mora biti popolnoma naključen;
  - ne sme biti večkrat uporabljen;
  - biti mora tajen.

One time pad

- V praksi je OTP neuporaben oz. težko uporaben.
- Med hladno vojno ga je uporabljala KGB (projekt Venona!).

- Primer: VUTQBANKX: ista verjetnost, da dobimo RINGARAJA ali SKRIVNOST.

- OTP zagotavlja popolno varnost (*perfect security*), celo proti napadu z grobo silo, saj vsa možna dešifrirana sporočila enako verjetno izhajajo iz šifriranega sporočila.

Sodobni šifrirni algoritmi

- DES, Twofish, Blowfish, AES,...
- Asimetrično kriptografijo so verjetno v 1960-tih letih odkrili v ameriški *NSA*, zagotovo pa nekoliko kasneje tudi v britanski tajni službi *Government Communications Headquarters*.
- Ronald L. Rivest, Adi Shamir in Leonard M. Adleman so leta 1977 objavili RSA algoritem.

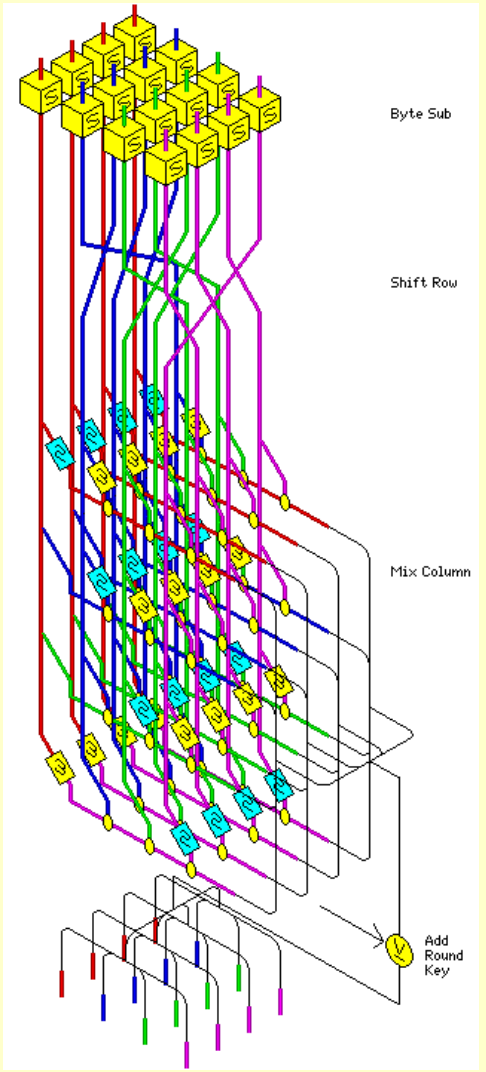
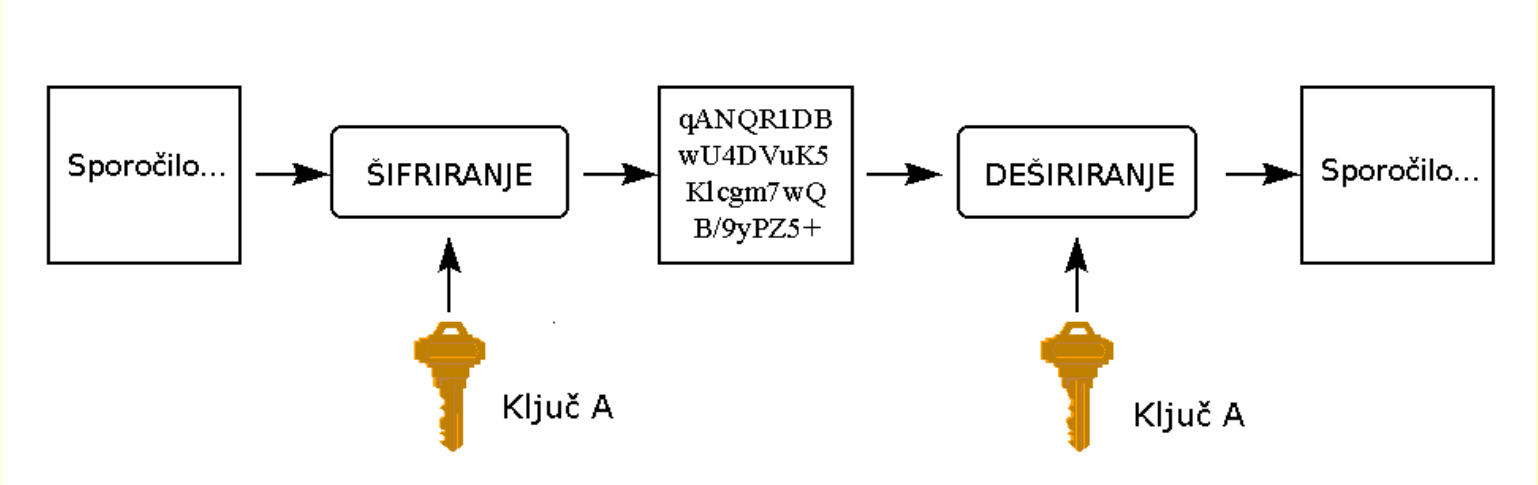


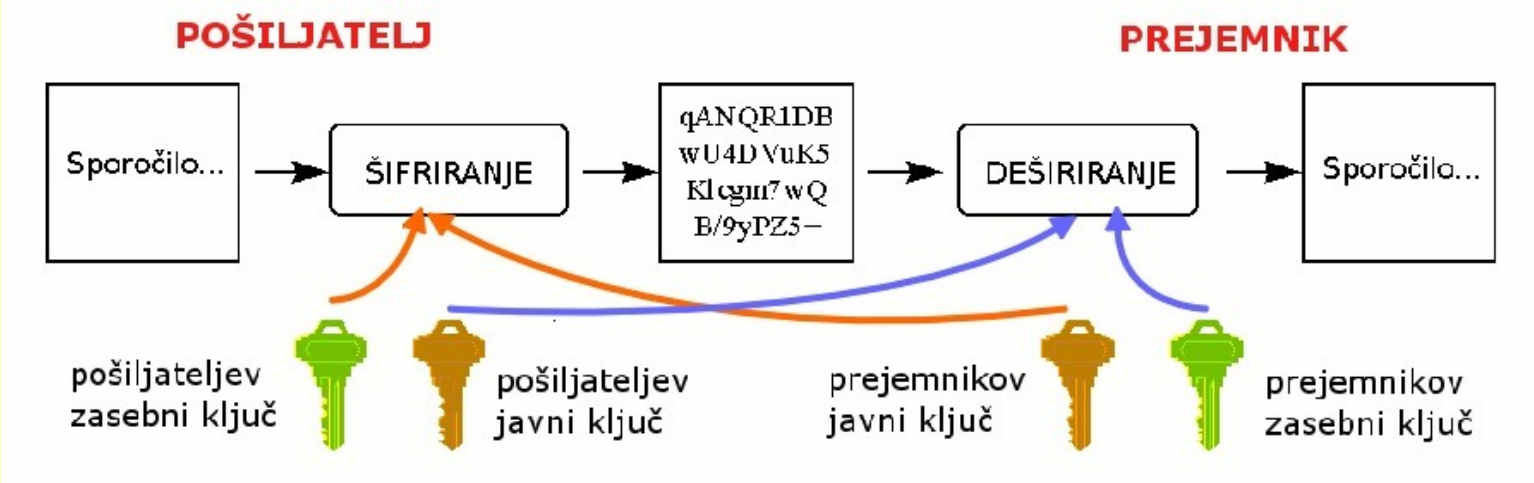
Diagram algoritma AES. Vir in avtorstvo: John J. G. Savard, A Cryptographic Compendium, <http://www.quadibloc.com/crypto/jscrypt.htm>.

Simetrična in asimetrična kriptografija

- Z vidika šifrirnega in dešifrirnega ključa poznamo dve vrsti kriptografije:
  - *simetrično*, ki za šifriranje in dešifriranje sporočila uporablja isti ključ (isto geslo)
  - *asimetrično*, pri kateri je ključ za šifriranje različen od ključa za dešifriranje.
- Prednost asimetrične kriptografije: odpade potreba po tim. varnih kanalih za prenos šifrirnih ključev.

Simetrična in asimetrična kriptografija

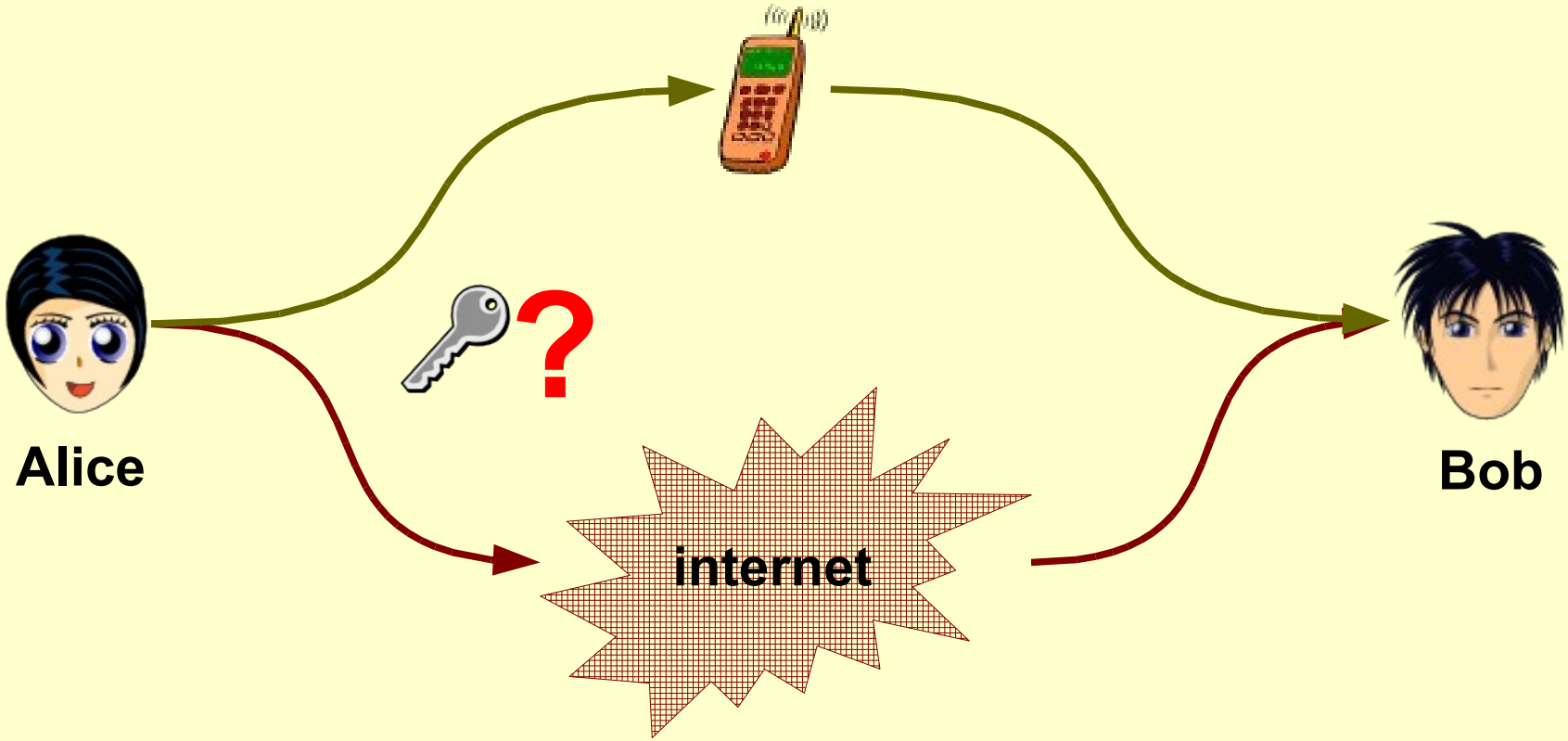




Shematski prikaz simetrične kriptografije in kriptografije z javnimi ključi.

Simetrična in asimetrična kriptografija

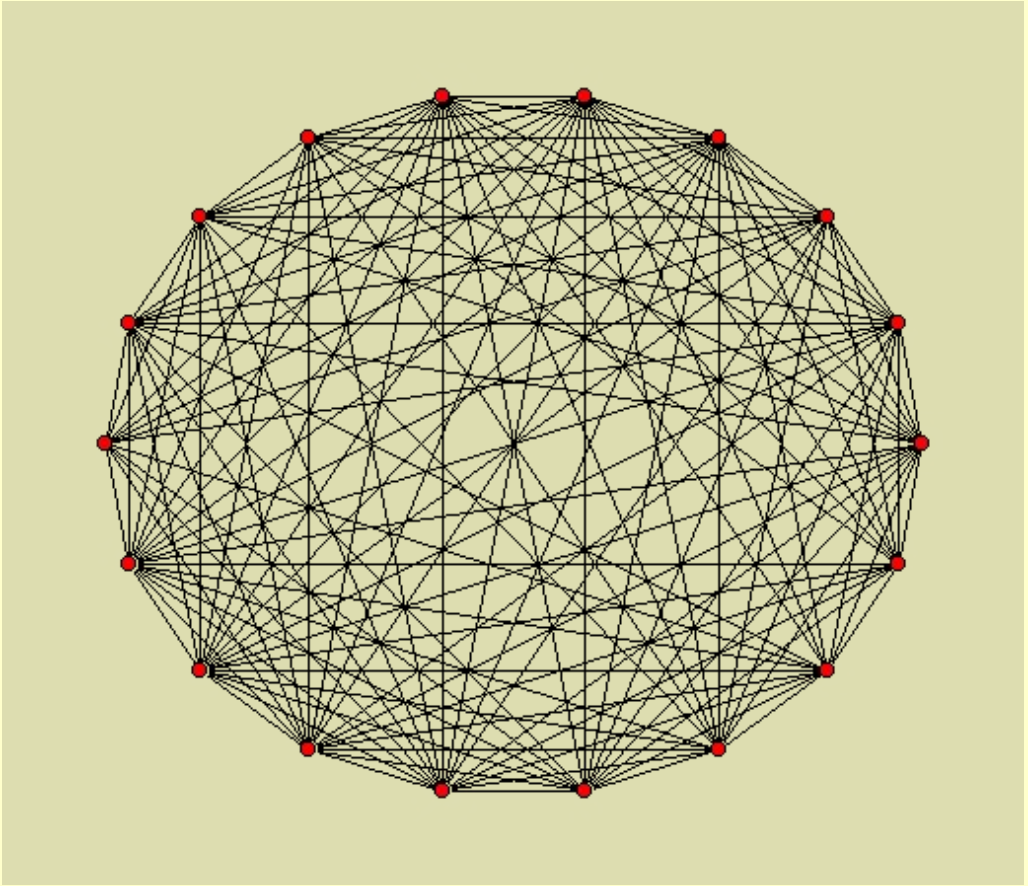
Problem tim. *varnega kanala*.



Simetrična in asimetrična kriptografija

Število gesel!

- št. gesel = n(n − 1)/2
- n=2; št. gesel = 1
- n=10; št. gesel = 45
- n=20; št. gesel = 190
- ...



Zgostitveni algoritmi

- Zgostitveni algoritmi (ang. *hash algorithms*, včasih tudi *message digests* ali *fingerprints*): poljubno dolg niz znakov preslikajo v število fiksne dolžine.
- Izračunajo tim. prstni odtis (ang. *fingerprint*) oz. kontrolno vsoto (*hash*) tega niza znakov, kar je osnova za digitalni podpis oziroma za zagotovilo, da sporočilo med prenosom ni bilo spremenjeno.
- Zgostitveni algoritmi so (morajo biti):
  - enosmerni (iz kontrolne vsote ni mogoče nazaj izračunati sporočila),
  - ne sme priti do kolizije (ne smeta obstajati dve različni sporočili, ki bi vrnili isto kontrolno vsoto).

Zgostitveni algoritmi

- Primeri zgostitvenih algoritmov:
- MD5, SHA-1, SHA256,...
- MD5: 75222cee3990e39e9fb48fa7ca6a733b
- SHA-1: 1f149834675ab2ae6d076ee3cbaa9158b6864ee1
- SHA-256: 3226338fb2c35ca40d39de77a0735779b1c0886f39a3762de2b502901567d39e

- Linux ukazna vrstica: md5sum, sha1sum, sha224sum, sha256sum, sha384sum, sha512sum

Digitalni podpis

- Digitalni podpis zagotavlja integriteto sporočila (da se vsebina sporočila ni spremenila med prenosom). Pošiljatelj kontrolno vsoto sporočila zašifrira s svojim šifrirnim ključem.
- Prejemnik kontrolno vsoto dešifrira ter jo primerja s kontrolno vsoto dejansko prejetega sporočila.
- Predpogoj: zaupamo v integriteto pošiljateljevega javnega ključa.
- (Vprašanje: kaj pa varnost zgostitvenega algoritma?)

Časovno žigosanje

- TSA - *Time Stamping Authority*, poseben zaupanja vreden strežnik, ki kontrolni vsoti dokumenta doda podatek o času nastanka in nato oba podatka digitalno podpiše.
- Časovno žigosanje omogoča preverjanje časa nastanka (oz. žigosanja) danega dokumenta, časovnega žiga pa ne more spremeniti niti lastnik dokumenta.
- OpenTSA.

Časovno žigosanje v verigi

- Primer: kako časovno žigosati npr. dnevniške zapise?

- Časovni žig (kontrolna vsota podatka + čas).
- Vsak naslednji časovni žig vsebuje še kontrolno vsoto prejšnjega časovnega žiga.

- S tem se tvori veriga, s pomočjo katere je mogoče ugotoviti ali je bil kakšen element v verigi odstranjen (izbrisan).

Geslo

- Geslo je osnovni in najpogosteje uporabljan zaščitni mehanizem.
- Gesla morajo biti dovolj kompleksna.
  - Se prenašajo v “plaintext” načinu ali ne?
  - So shranjena v “plaintext” načinu ali kot “hash”?
- Kompleksna gesla si je težko zapomniti: varnost vs. uporabnost.
  - gesla zapisana na listku ob računalniku
  - gesla v posebnem programu ali napravi (npr. programska varnostna naprava v Firefoxu).

Geslo

- *Metoda 1*: geslo sestavljeno iz stavka (“to je moje geslo” -> pozor pri čšž in SL/US tipkovnicah!).
- *Metoda 2*: geslo sestavljeno iz stavka + zamenjava črk s številkami (“t0j3m0j3g3s10”).
- *Metoda 3*: geslo sestavljeno iz prve (ali zadnje,...) črke daljšega besedila (An ban pet podgan -> abpp).
- Več o varnosti v poglavju o napadih na šifrirna gesla in ključe...

Šifrirni ključ in šifrirni kontejner

- Šifrirni kontejner (ang. *crypto container*): abstrakten objekt (navadno datoteka), ki služi kot nosilec šifriranih podatkov. V primeru verodostojnega zanikanja imamo več šifrirnih kontejnerjev, ki so skriti drug v drugem po principu “babuške”.
- Šifrirni kontejner ima v vzglavju shranjen ključ, s katerim so šifrirani podatki. Ključ se ne spreminja, je pa šifriran z geslom. Spreminjanje gesla omogoča “spreminjanje” ključa.

Šifrirni kontejner v LUKS formatu

Omogoča tudi menjavo gesel:

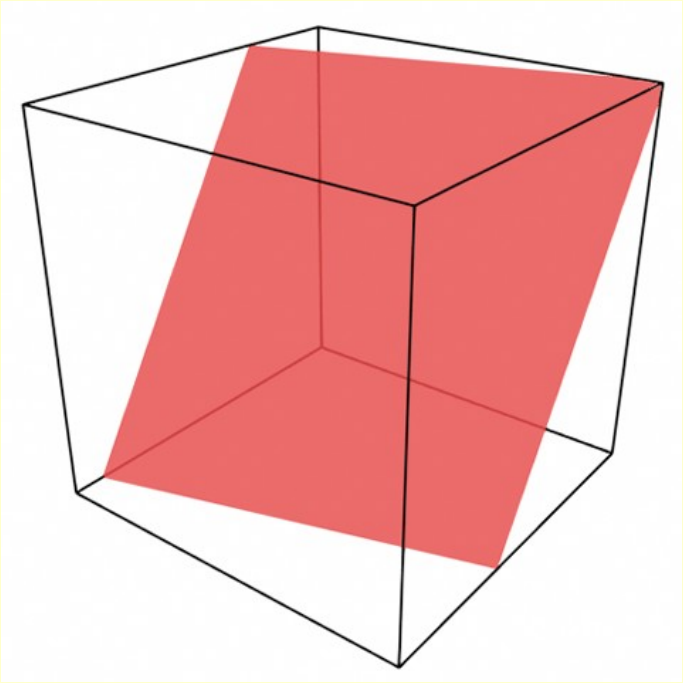
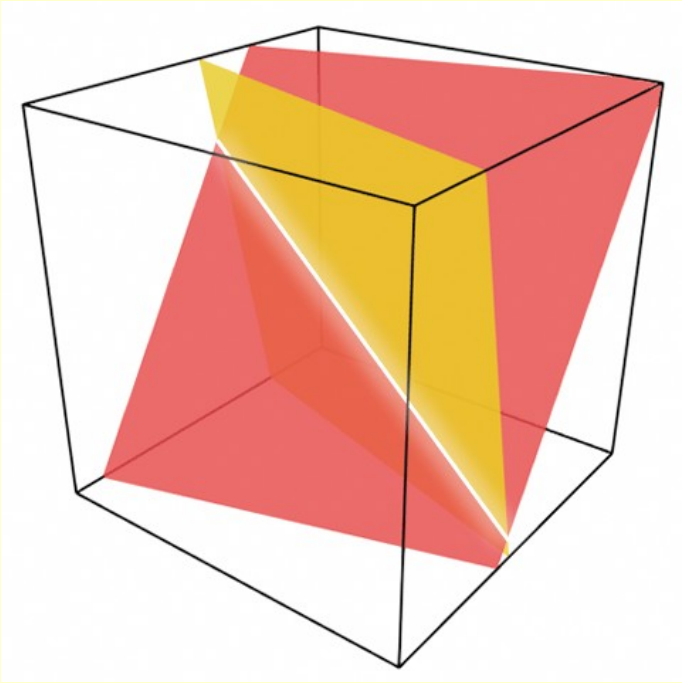
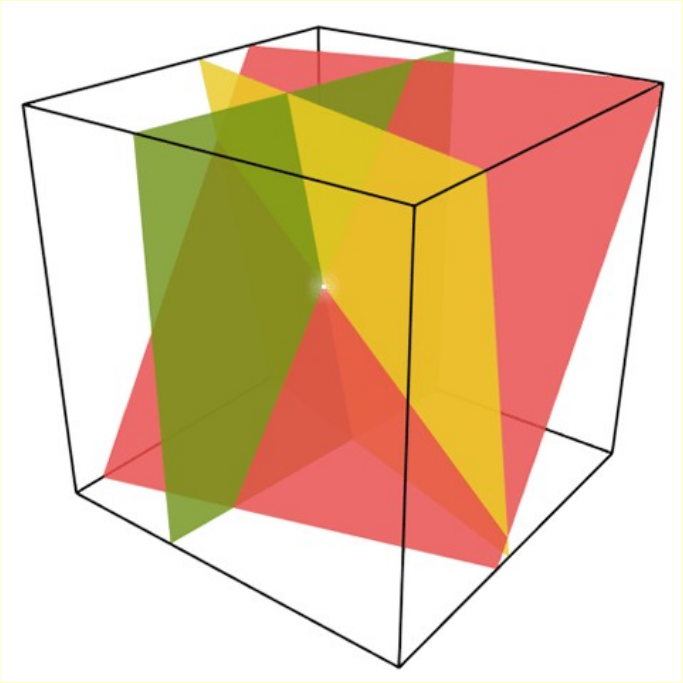
- dodamo novo geslo
- odstranimo starega.

“Posebna” gesla in ključi

- Enkratna gesla (predizračunana, generirana).
- Sejni ključi.
- Dvofaktorska avtentikacija, ključi prihajajo po različnih kanalih (primer: mTAN);
- Distribuirani ključi, kriptosistem s pragom (ang. *threshold cryptosystem*) in deljena skrivnost (ang. *shared secret*): za dešifriranje sta potrebna npr. vsaj dva od treh ključev...). Primer: odprtokodni oblačni datotečni sistem Tahoe (za obnovitev podatkov od 10 točk zadostujejo 3).

Deljene skrivnosti

- 1 general = 15 vojakov,...
- Za dešifriranje zadostuje ključ predsednika uprave ali dveh od treh namestnikov,...

- Vsaka ploskev predstavlja del ključa.
- Presečna točka predstavlja šifrirni ključ.
- Primer: ustvarimo 5 ploskev, katerekoli tri (ali več) nam dajo presečno točko.

“Posebna” gesla in ključi

- Sheme obnavljanja gesel (*key escrow*), in rezervna gesla (ang. *master key*):
  - elektronske ključavnice znamke Sentex: ***00000099#* (prve tri zvezdice aktivirajo administrativni način naprave, šest ničel je tovarniško privzeto geslo, z ukazom 99# se odprejo vrata, s končno zvezdico pa se ponovno izključi administrativni način)
  - prometni znaki,
  - napadi na bankomate,...

Vir in avtorstvo: i.hacked.com,
<http://www.i-hacked.com/content/view/274/48/>

“Posebna” gesla in ključi

- “Biometrična gesla”?
- Biometričnih parametrov ni mogoče zamenjati/preklicati.
- Ponarejanje prstnih odtisov, rezanje prstov,...
- Indentiteta in avtentikacija morata ostati ločeni!
  - Identiteta: kdo si?
  - Avtentikacija: kako lahko to dokažeš?
  - Sistem brez gesel - sistem, ki omogoča prijavo le z uporabniškim imenom: težava je, če imata dva uporabnika enako ime.
- Pametna kartica + PIN!

Sejni ključi

Primer GSM telefonije:

Ki, 128-bit: shranjen v SIM **in** HLR.

Omrežje -> (**RAND**, 128-bit) -> telefon

SIM: Ki + **RAND** @ A3 -> **SRES**, 32-bit

Telefon -> **SRES** -> omrežje

(Omrežje **SRES** preveri!)

Sejni šifrirni ključ **Kc**: **Ki** + **RAND** @ A8.

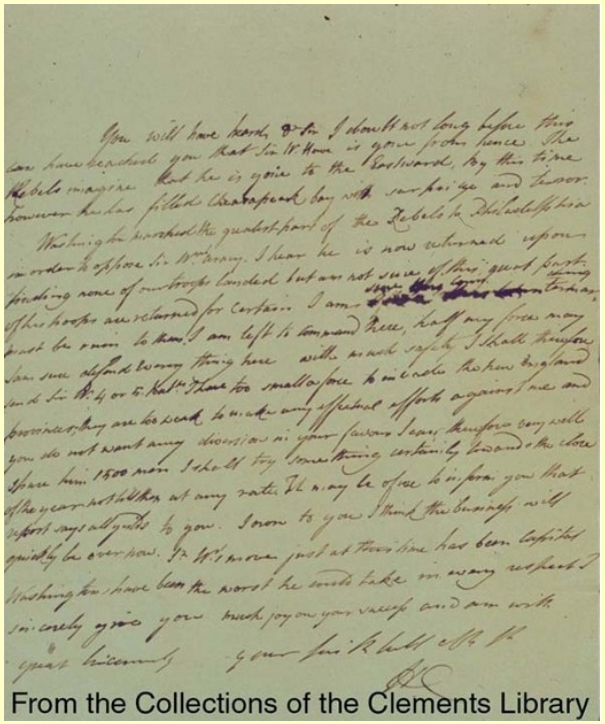
SIM -> **Kc** -> telefon, omrežje prav tako izračuna **Kc**; Kc se nikoli ne prenese preko omrežja!

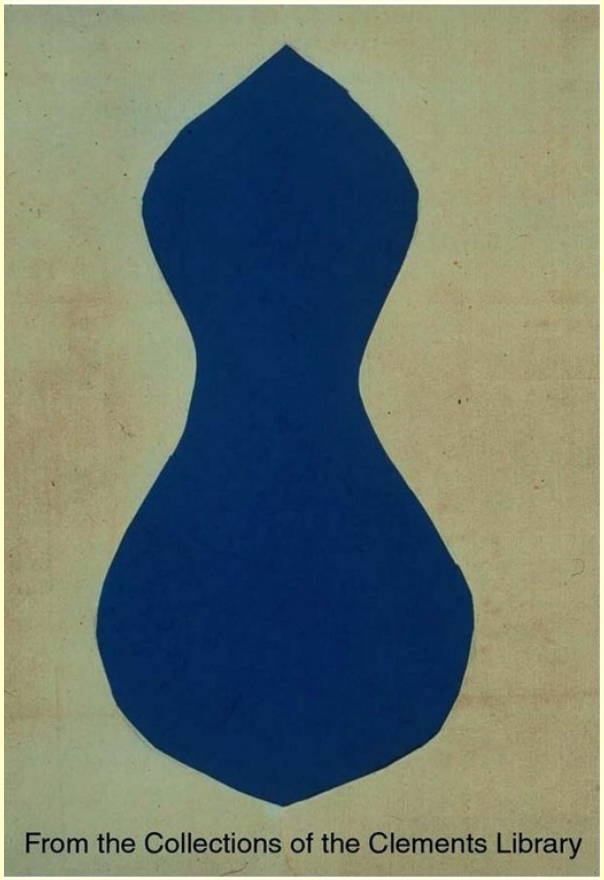
Šifriranje pogovorov: **Kc** + A5/x

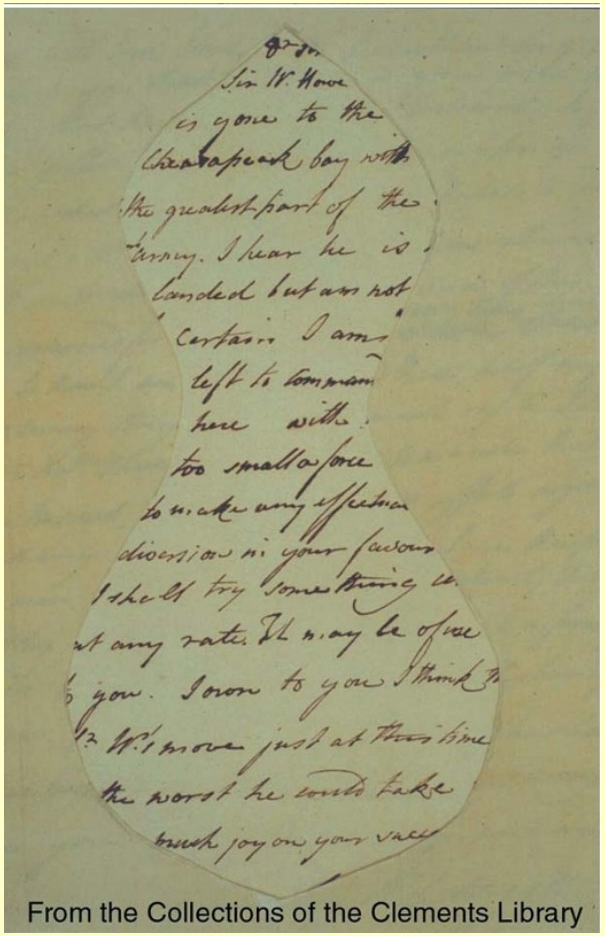
Skrivanje podatkov

- Steganografija: metode za skrivanje sporočil, ki med drugim omogočajo izmenjavo nevidnih sporočil, nevidno kodiranje, označevanje datotek z tim. elektronskim vodnim tiskom ter označevanje datotek z elektronskimi serijskimi številkami.
- Verodostojno zanikanje (ang. *plausible deniability*): skrivanje šifriranih podatkov v druge šifrirane podatke.

Skrivanje podatkov


From the Collections of the Clements Library


From the Collections of the Clements Library

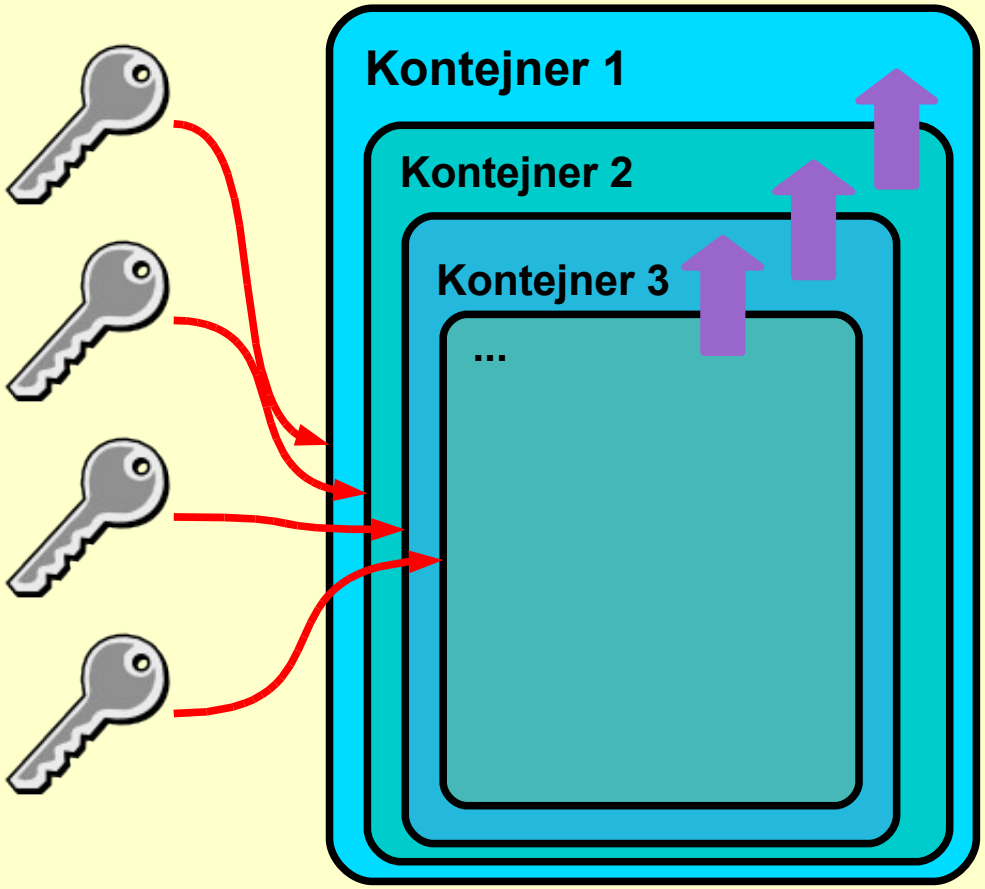

From the Collections of the Clements Library

Maskirano pismo: 10. avgust 1777, Henry Clinton -> John Burgoyne.
http://www.si.umich.edu/spies/letter-1777august10-1.html

S-Tools


hidd.gif
Revealing from hidd.gif
Passphrase:
*****
Verify passphrase:
*****
Encryption algorithm:
IDEA
OK
Cancel
Help

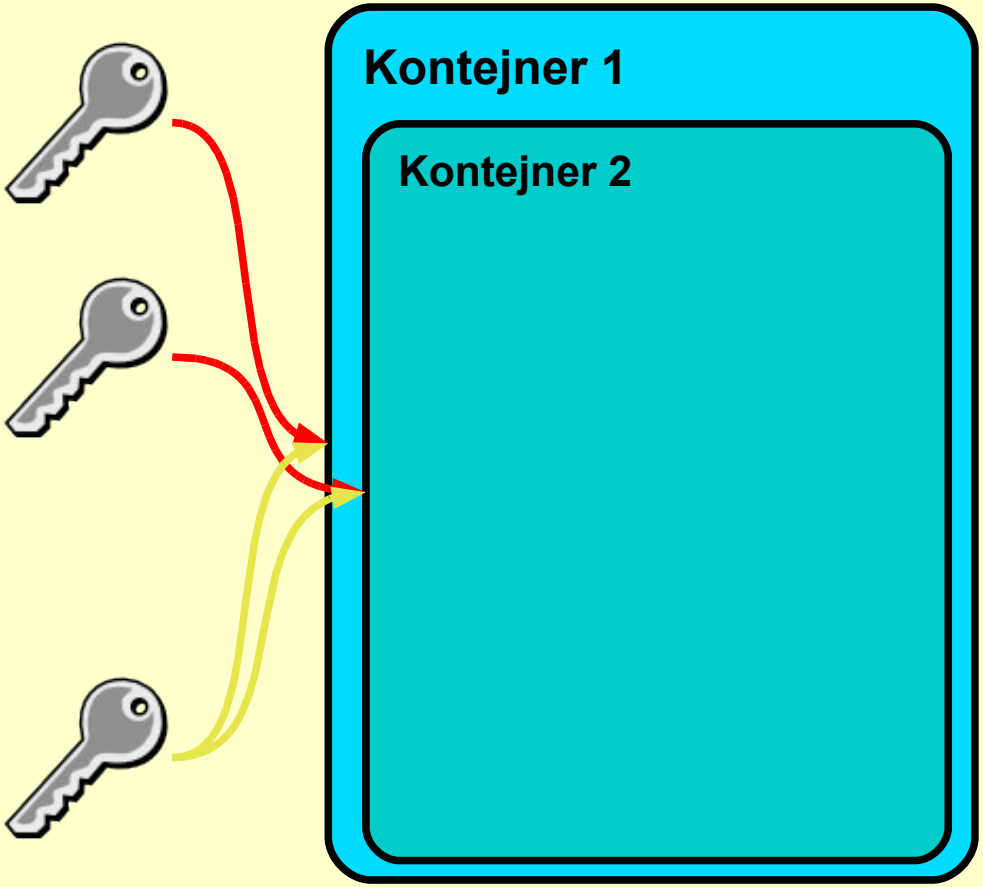
Skrivanje podatkov v gnezdene šifrirne kontejnerje (verodostojno zanikanje)



Vsak gnezdeni kontejner se "zaveda" svojih nadrejenih kontejnerjev.

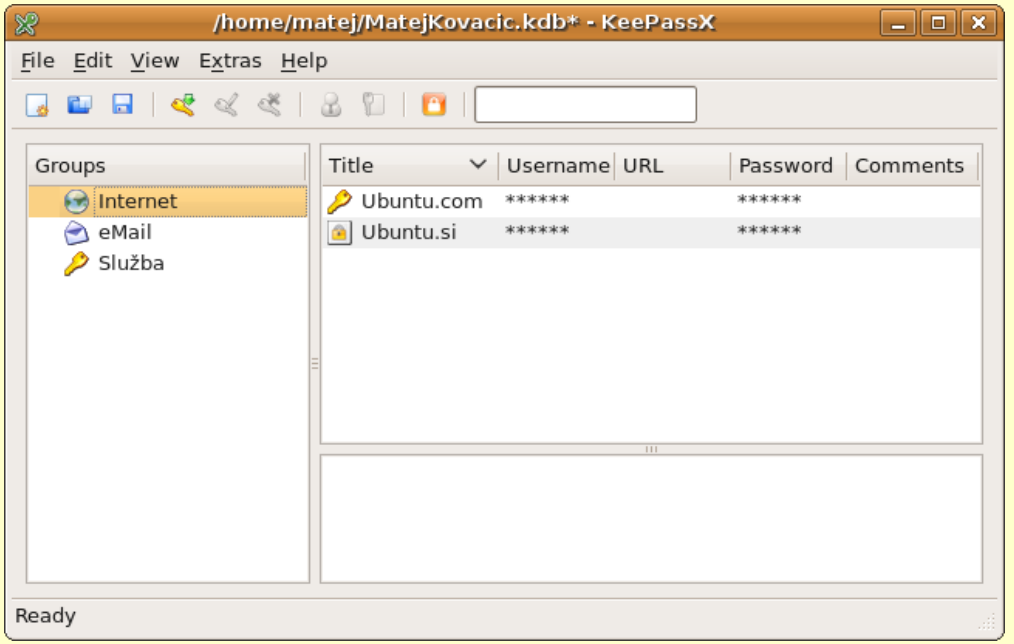
Skrivanje podatkov v gnezdene šifrirne kontejnerje (verodostojno zanikanje)

- **Prvi ključ** odklene prvi kontejner. Podatki se lahko zapisujejo v celoten kontejner, tudi v skritega.
- **Drugi ključ** odklene drugi kontejner, ki ne dovoli pisanja podatkov v nadrejeni, prvi kontejner.
- **Tretji ključ** odklene prvi in drugi kontejner: v prvi kontejner lahko zapisujemo, vendar ne po območju kjer se nahaja skriti drugi kontejner.



Shrambe gesel/ključev

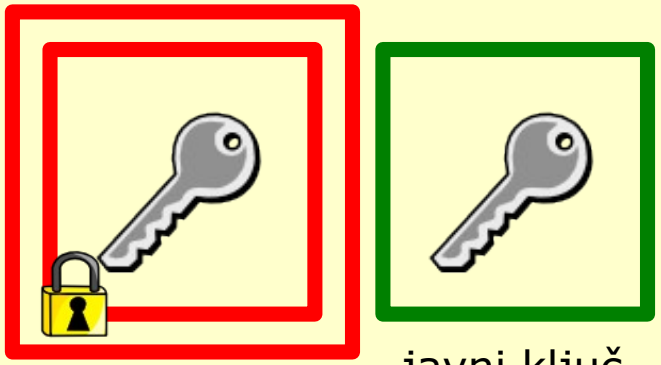
- Šifrirni ključi so lahko shranjeni:
  - kot kontrolna vsota (npr. SAM/SYSKEY, možno razbijanje!),
  - v posebnem programu (npr. *KeePassX*, vgrajena programska varnostna naprava v *Firefoxu*, itd.),
  - v kontejnerju,
  - v strojnih žetonih.



Hramba in distribucija javnih ključev

- Shramba ključev (ang. *keyring*): lokacija na uporabnikovem računalniku, kjer je shranjen uporabnikov par zasebnega in javnega ključa ter javni ključi ostalih s katerimi si uporabnik izmenjuje sporočila.
- Strežnik javnih ključev (ang. *keyserver*): strežnik, ki hrani javne ključe uporabnikov.
- Pomembno: lokalno shrambo ključev je potrebno varovati!
- Integriteto javnih ključev je mogoče zagotoviti tudi s podpisovanjem teh javnih ključev.

Asimetrična kriptografija: javni ključ, zasebni ključ ter geslo



zasebni ključ, zaščiten z geslom

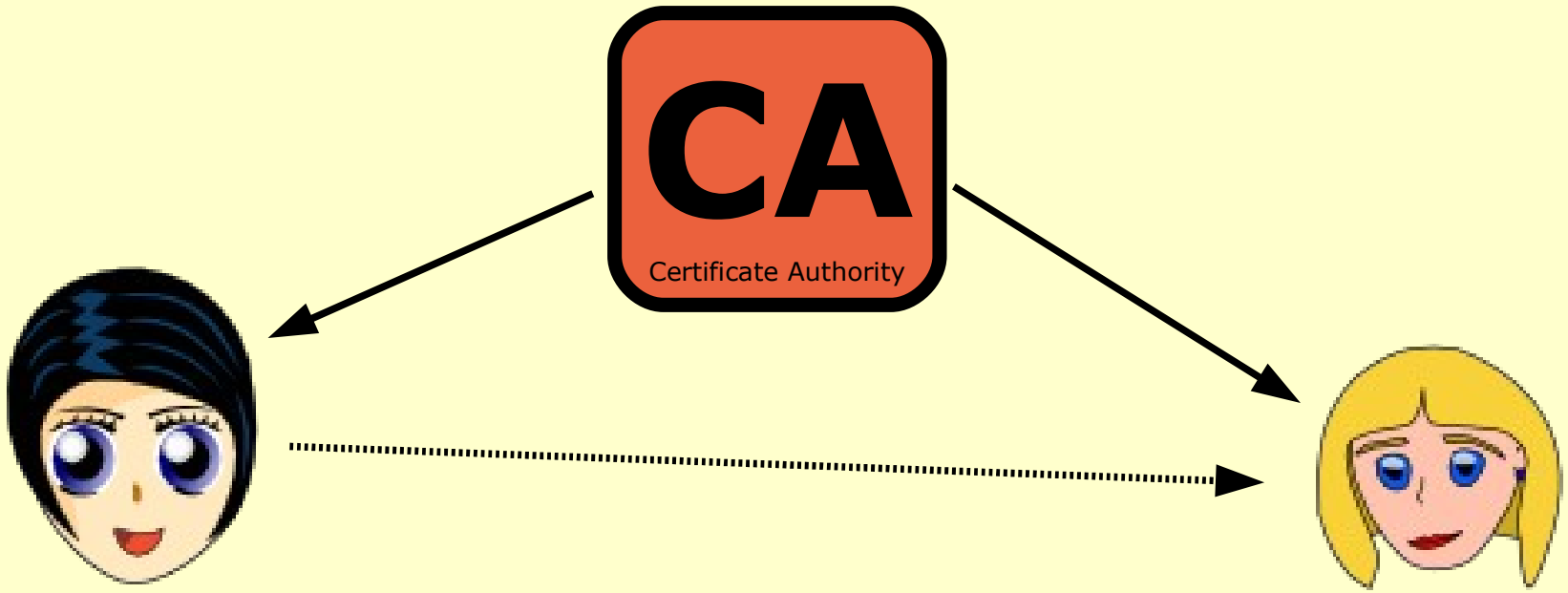
javni ključ

- Javni ključ (*public key*) lahko objavimo.
- Zasebni ključ (*private key*) je potrebno dobro zavarovati (fizični dostop!), npr. z geslom (*passphrase*). Geslo lahko spreminjamo.

Overovitev (avtentikacija)

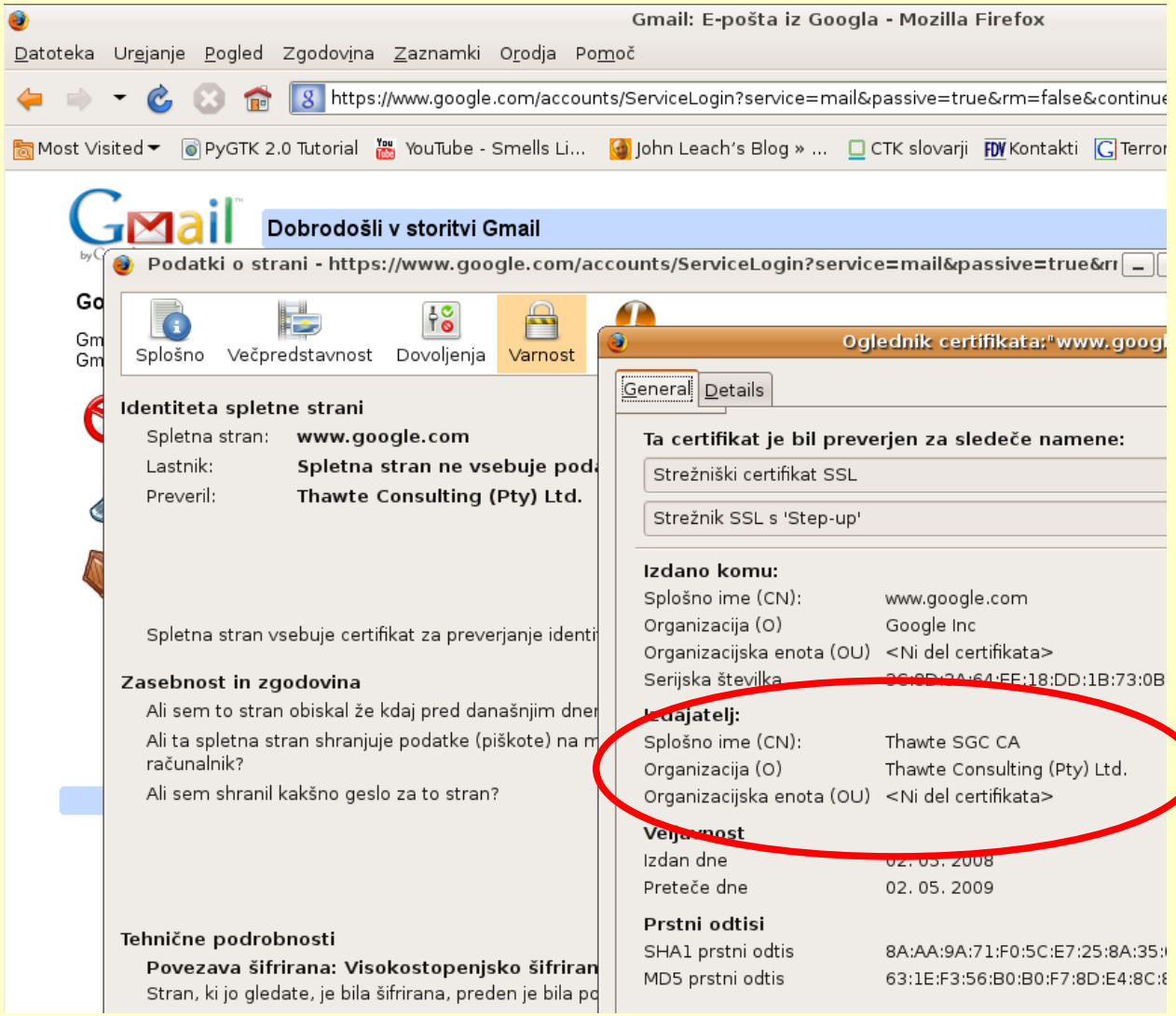
- **Digitalno potrdilo** (digitalni certifikat): s strani zaupanja vredne entitete (tim. *Certificate Authority*) digitalno podpisan dokument, ki povezuje javni ključ uporabnika z njegovo identiteto.
- **Infrastruktura javnih ključev** (ang. *public key infrastructure, PKI*): koncept zagotavljanja avtentikacije (overjanja) javnih šifrirnih ključev s pomočjo zaupanja vredne tretje stranke (*Certificate Authority* (*CA*) oz. *trusted third party*). CA preveri identiteto lastnika vsakega javnega ključa in veljavnost njegovega javnega ključa ter izda ustrezno digitalno potrdilo.
- **Omrežje zaupanja** (ang. *web of trust*): koncept zagotavljanja avtentikacije javnih šifrirnih ključev oziroma vzpostavljanja zaupanja vanje s pomočjo "omrežja zaupanja".

Infrastruktura javnih ključev (PKI – Public Key Infrastructure)



- CA je preveril identiteto in ključ Alice in Dore.
- Alice zaupa Dori, ker zaupa CA.

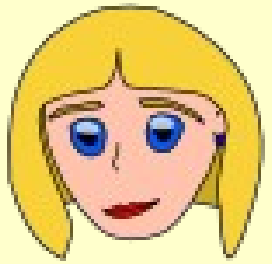
Infrastruktura javnih ključev



Omrežje zaupanja (web of trust)

Alice

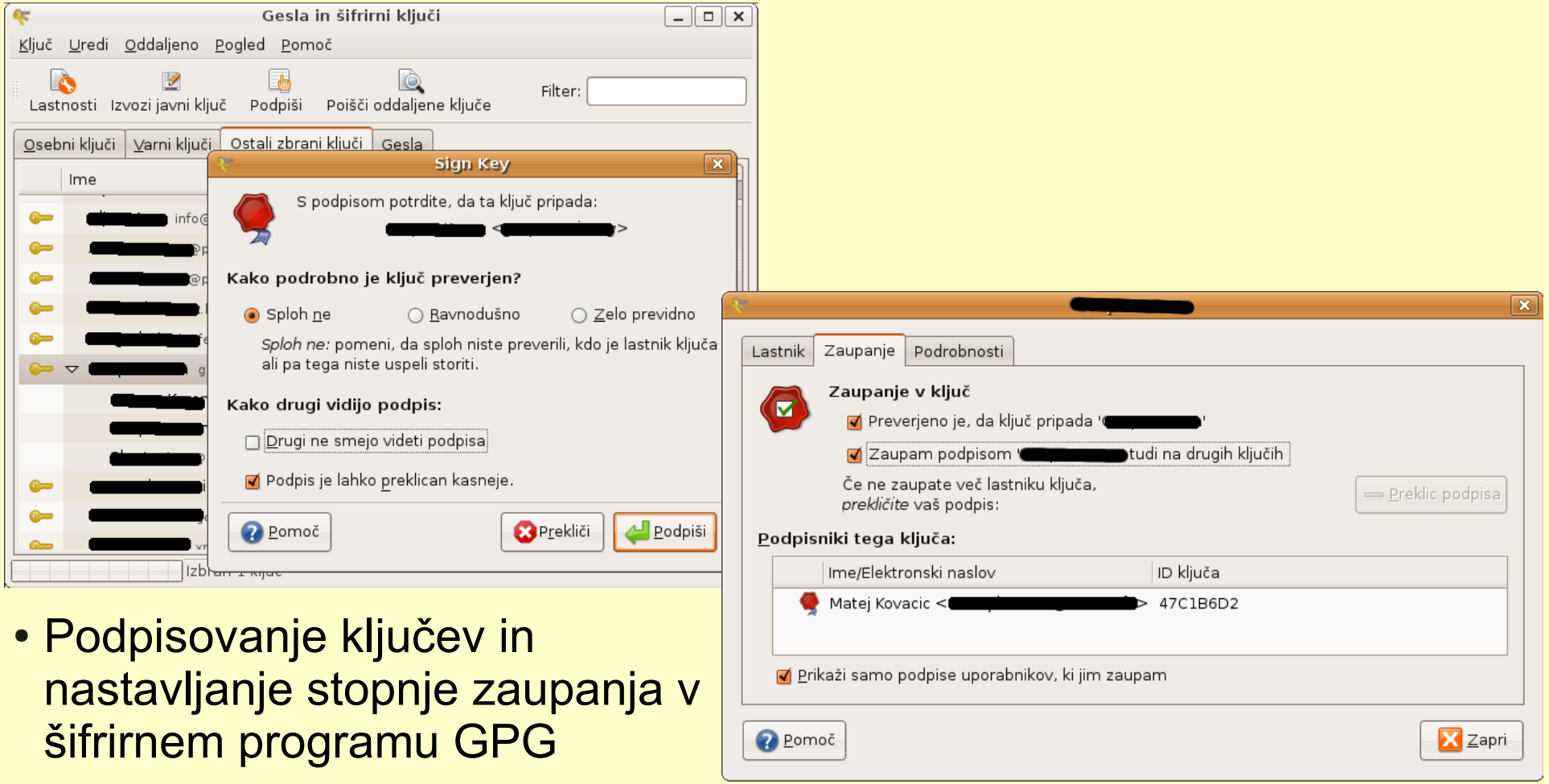
Bob



Dora

- Bob pozna Doro in je preveril ter podpisal njen javni ključ.
- Alice pozna Boba (je preverila njegov javni ključ) in mu zaupa.
- Ker Bob zaupa v identiteto Dore in Alice zaupa Bobu, Alice zaupa Dori.

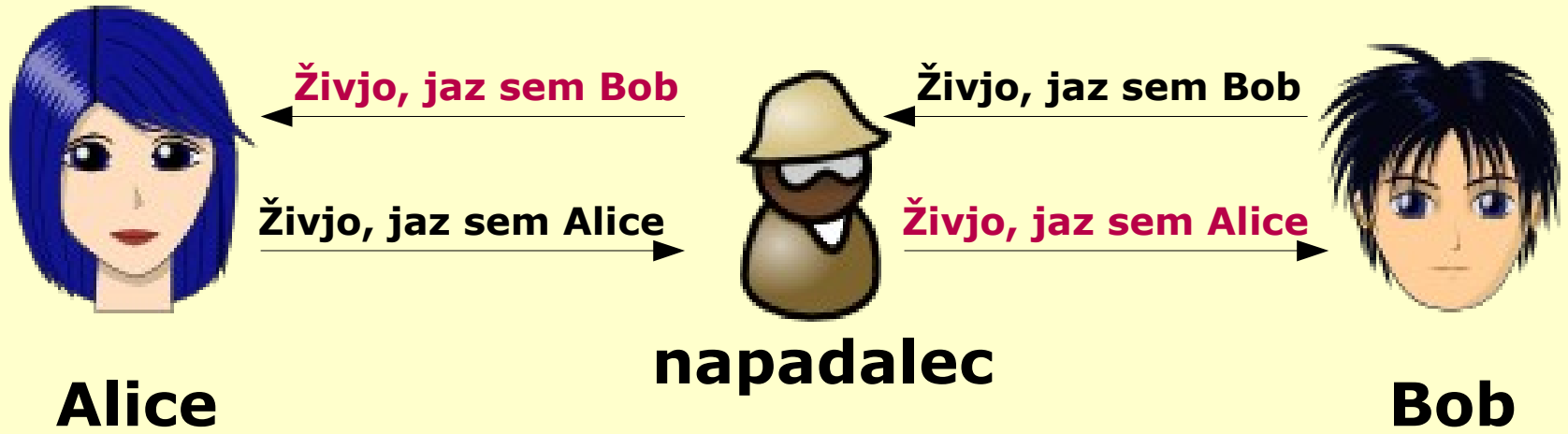
Omrežje zaupanja (web of trust)



- Podpisovanje ključev in nastavljanje stopnje zaupanja v šifrirnem programu GPG

Omrežje zaupanja

Pomen overovitve - problem napada s posrednikom



Avtentikacija uporabnika po imenu?

Zadeva: Remote Download server ;)
Od: [redacted]
Datum: 09. 07. 2007 01:52
Za: matej.kovacic@gmail.com

Zivjo!

Takole, v Win 2000 si najprej naloži Remote Desktop Client.
Dobiš ga na:
http://www.microsoft.com/downloads/details.aspx?FamilyID=80111f21-d48d-

Nato se z njim povežeš na [redacted]
user: [redacted]

LP, Darko

Avtentikacija uporabnika po imenu?

PERSPEKTIVA

PERSPEKTIVA, BORZNO POSREDNIŠKA DRUŽBA, d.d.
WTC, Dunajska cesta 156
1000 Ljubljana, Slovenija
T: + 386 (0) 1 / 56 88 225
F: + 386 (0) 1 / 56 88 141

Stran: 1 / 1

PETROL D.D.
DUNAJSKA CESTA 50

1000 LJUBLJANA

ID št. za DDV kupca: [redacted]

RAČUN: [redacted]

V Ljubljani, [redacted] 2007
Datum odpošiljanja blaga oz. opravljanja storitev: [redacted] 2007
Datum zapadlosti: [redacted] 2007

Predmet: Pogodba o svetovanju pri izvedbi in izvedbi prevzema javne družbe, z dne [redacted] 2007

Opis	Količina	EM	Šif. E.	Cena brez DDV	Znesek brez DDV
Na podlagi 8. člena pogodbe o svetovanju pri izvedbi in izvedbi prevzema javne družbe, z dne 19.09.2007, vam zaračunavamo:					
- fiksni del provizije za izvedbo prevzemnih opravil in za svetovanje	1			60.000,00	60.000,00
- variabilni del provizije za svetovanje v višini 0,40 % od transakcijske vred. delnic, ki predstavljajo prvih 29,99% delnic, za katere so akcep. sprejeli prev. pon.	1			683.760,00	683.760,00
- variabilni del provizije za svetovanje v višini 0,85 % od transakcijske vrednosti delnic , ki presegajo 30,00 % delnic za katere so akceptanti sprejeli prevzemno ponudbo	1			115.225,66	115.225,66
Vrednost brez DDV					858.985,66
1 - DDV - Osnovna stopnja 20,0 %			Osnova:	858.985,66	171.797,13
				SKUPAJ €	1.030.782,79
				Znese v SIT	247.016.787,79

Prosimo vas, da fakturni znesek nakažete na TRR : SI56 0600 0011 8721 024 pri Banki Celje, d.d.

PRI PLAČILU SE SKLICUJTE NA [redacted]

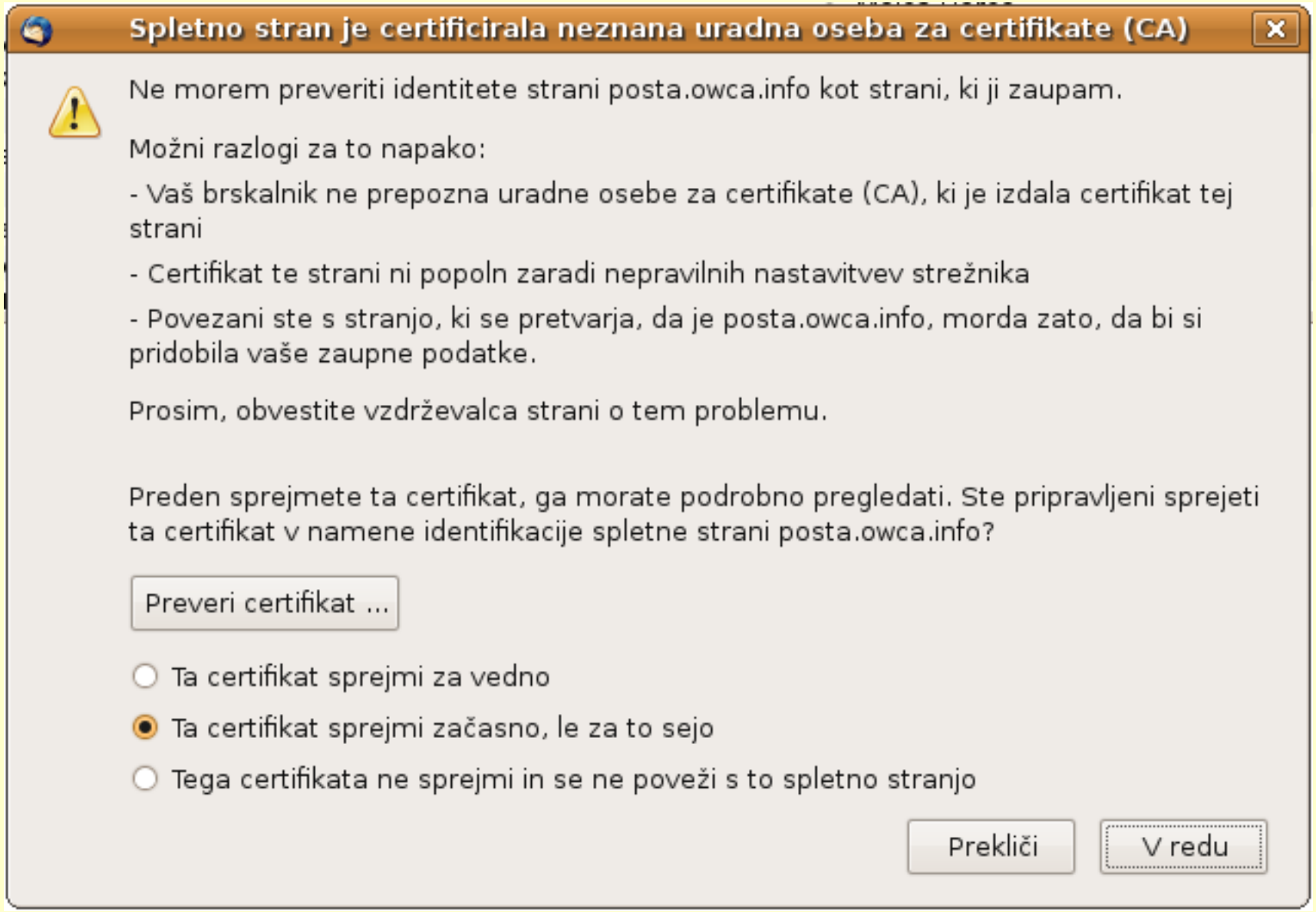
[redacted]

Pripravila: [redacted]

PERSPEKTIVA BORZNO POSREDNIŠKA DRUŽBA

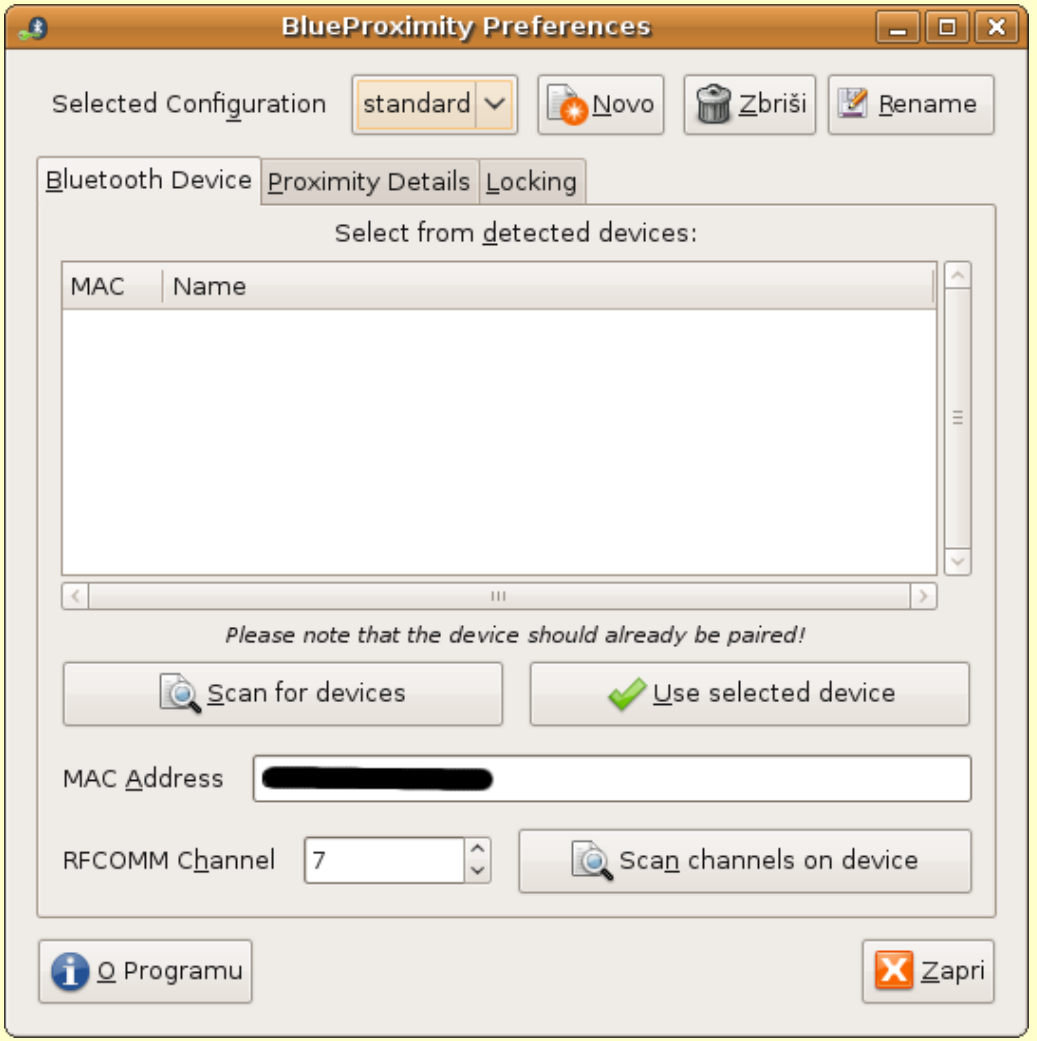
Član uprave:
Mladen Kaliterna

Identifikacijska številka za DDV: SI83064775 | Matična številka: 5754164 | Osnovni kapital: 150.246.000,00 SIT | Številka registerskega vložka: 1/30044/00 | Družba je vpisana pri Okrožnem sodišču v Ljubljani


Spletno stran je certificirala neznana uradna oseba za certifikate (CA)
Ne morem preveriti identitete strani posta.owca.info kot strani, ki ji zaupam.
Možni razlogi za to napako:
- Vaš brskalnik ne prepozna uradne osebe za certifikate (CA), ki je izdala certifikat tej strani
- Certifikat te strani ni popoln zaradi nepravilnih nastavitvev strežnika
- Povezani ste s stranjo, ki se pretvarja, da je posta.owca.info, morda zato, da bi si pridobila vaše zaupne podatke.
Prosim, obvestite vzdrževalca strani o tem problemu.
Preden sprejmete ta certifikat, ga morate podrobno pregledati. Ste pripravljeni sprejeti ta certifikat v namene identifikacije spletne strani posta.owca.info?
Preveri certifikat ...
Ta certifikat sprejmi za vedno
Ta certifikat sprejmi začasno, le za to sejo
Tega certifikata ne sprejmi in se ne poveži s to spletno stranjo
Prekliči
V redu

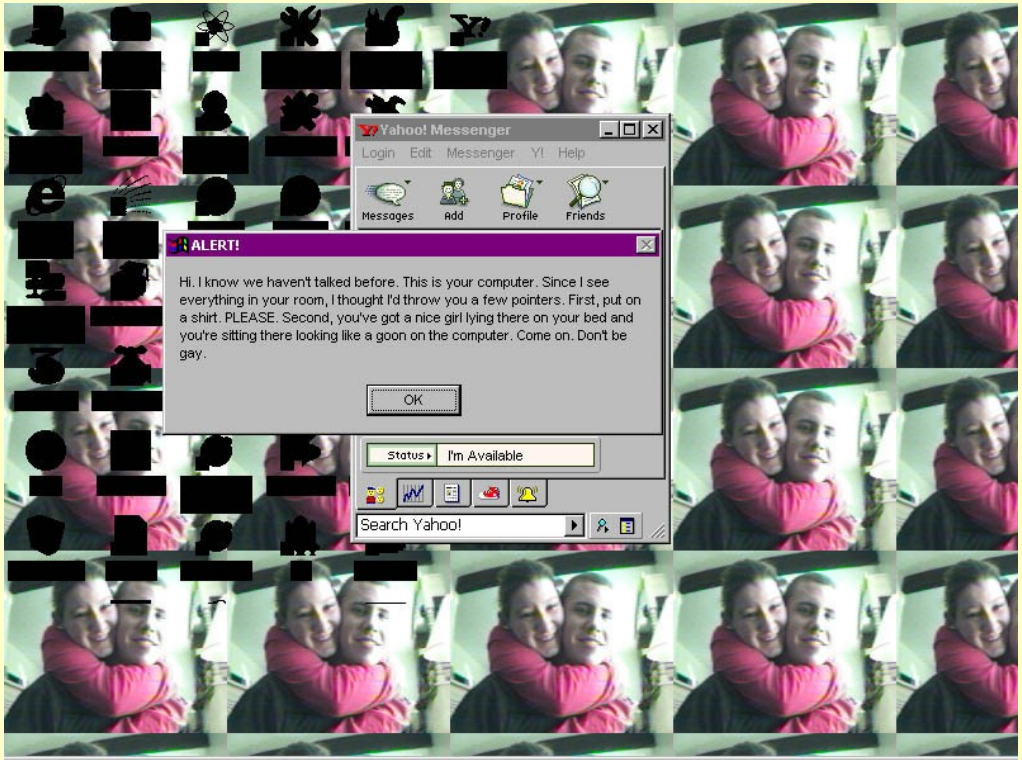
Deavtentikacija

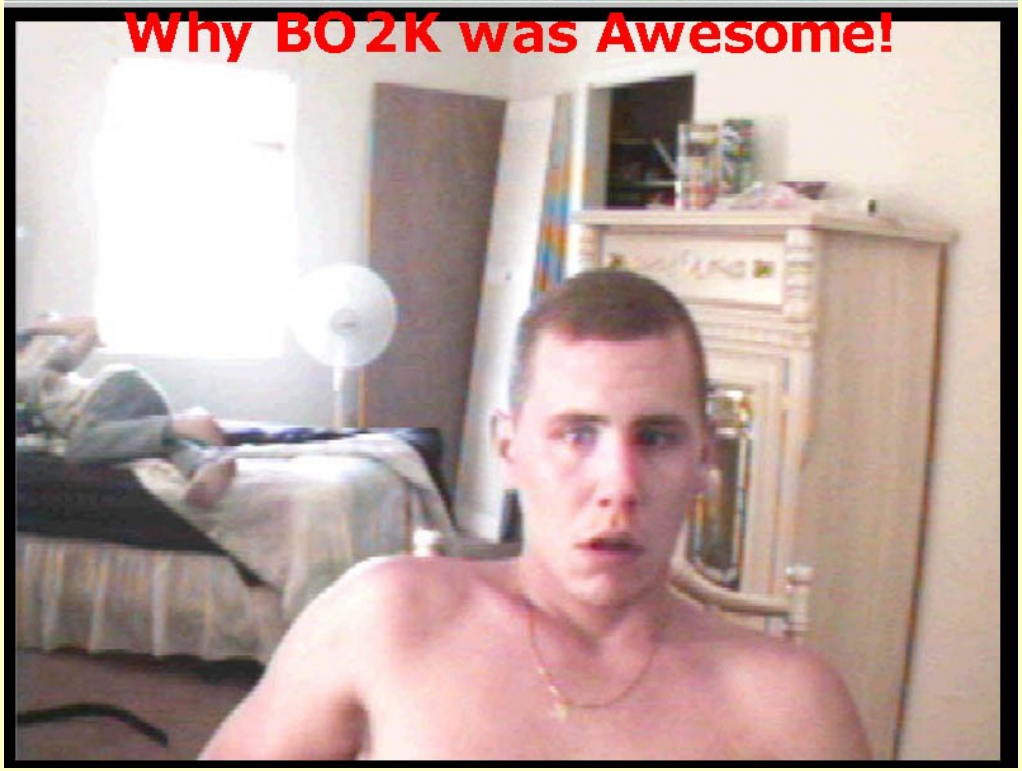
- Samodejna deavtentikacija po določenem času: varnost vs. uporabnost.
  http://www.schneier.com/blog/archives/2009/09/unauthenticatio.html
- Primer samodejne de/avtentikacije: BlueProximity.



Varnost terminalnih naprav

- **Pentagon of trust**.
- Tradicionalni štiristopenjski varnostni model:
  - *avtentikacija (authentication)*: kdo si
  - *avtorizacija (authorization)*: kaj ti je dovoljeno
  - *dostopnost (availability)*: so podatki dostopni
  - *celovitost (authenticity)*: so podatki nespremenjeni
- *Dopustnost (admissibility)*: zaupanje v varnost končne terminalne naprave.


Yahoo! Messenger
Login Edit Messenger Y! Help
Messages
Add
Profile
Friends
ALERT!
Hi. I know we haven't talked before. This is your computer. Since I see everything in your room, I thought I'd throw you a few pointers. First, put on a shirt. PLEASE. Second, you've got a nice girl lying there on your bed and you're sitting there looking like a goon on the computer. Come on. Don't be gay.
OK
Status
I'm Available
Search Yahoo!


Why BO2K was Awesome!

III: Praktični prikaz šifriranja

- Praktični prikaz šifriranja e-pošte in IM komunikacij.
- Šifrirano povezovanje med računalniki: SSH in VPN.
- Šifriranje trdih diskov:
  - Cryptsetup/LUKS,
  - eCryptfs (v *userspace*),
  - BitLocker,
  - FileFault,
  - PGPDisk,
  - TrueCrypt
  - problem izmenjalnega in začasnega prostora.
- Prikaz verodostojnega zanikanja.
- Prikaz uporabe steganografije.

IV: Napadi na kriptografijo

- Napadi na slabosti v algoritmu ali slabosti v implementaciji algoritma.
- Napadi na šifrirne ključe in gesla.
- Posredni napadi (ang. *channel side* napadi).
  - Napačna uporaba kriptografije.

Varnost

- Varnost v ožjem smislu (!) je odvisna od:
  - uporabljenega algoritma;
  - dolžine ključa;
  - v primeru, da je uporabljeno še geslo pa tudi od ustreznosti gesla.
- Neustrezen algoritem omogoča različne matematične napade (npr. frekvenčno analizo). Za vse dobre simetrične algoritme velja, da se izhoda ne da kompresirati za več kot nekaj odstotkov.
- Prekratek ključ ali neustrezno geslo omogočata učinkovito izvedbo napada z metodo grobe sile (ang. *brute force attack*) ali pa napada s slovarjem (ang. *dicionary attack*).

Varnost šifrirnih algoritmov - Kerckhoffsov zakon

- Leta 1883 flamski lingvist in kriptolog Auguste Kerckhoffs objavi članek *La Cryptographie Militaire*.
- V članku izpostavi šest načel:
  - 1. Šifrirni sistem mora biti v praksi, če že ne matematično nezlomljiv.
  - 2. Ne sme se zahtevati, da mora ostati tajen, če pa pade v roke sovražniku to ne sme predstavljati nevšečnosti.
  - 3. Njegov ključ mora biti sporočljiv, zapomniti naj si ga bo mogoče ne da bi ga bilo potrebno zapisati, biti mora spremenljiv ali prilagodljiv po volji komunikacijskih partnerjev.
  - 4. Mora biti uporaben za telegrafsko komunikacijo.
  - 5. Biti mora prenosen, za njegovo uporabo in delovanje pa ne sme biti potrebno delo več ljudi.
  - 6. In končno, potrebno je, da je sistem enostaven za uporabo in da za njegovo uporabo ni potreben miselni napor ali upoštevanje velikega števila pravil.

Varnost šifrirnih algoritmov - Kerckhoffsov zakon...

- Kerchoffsov zakon tako pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa.
- Kerchoffsov zakon zavrača načelo, da je mogoče varnost zagotoviti s skrivanjem (t. i. '*security through obscurity*').
- Kerchoffsov zakon ne zahteva, da je šifrirni sistem javen, temveč le opozarja na to, da skrivnost ne zagotavlja varnosti, marveč jo v resnici lahko celo ogroža.

… in nadaljevanje

- Claude Shannon je postavil tim. *Shannonovo maksimo*, ki pravi, da sovražnik pozna šifrirni sistem.
- Eric S. Raymond pravi: "*Vsaka varnostna programska oprema, ki ne predpostavlja, da sovražnik poseduje izvorno kodo, je nevredna zaupanja; zatorej: nikoli ne zaupaj zaprti kodi*".

Varnost skozi transparentnost

- Korist od javne objave šifrirnih algoritmov je predvsem v tem, da lahko drugi kriptologi algoritem ali zamisel ocenijo in kritično ovrednotijo.
- To pripomore k izboljšavi kakovosti in k hitrejšemu razvoju.
- Pri zaprtih sistemih je veliko večja verjetnost, da je v njih kakšna napaka, ki bi jo javni pregled verjetno odkril, avtorji pa bi s tem dobili možnost, da jo odpravijo.

Varnost skozi transparentnost

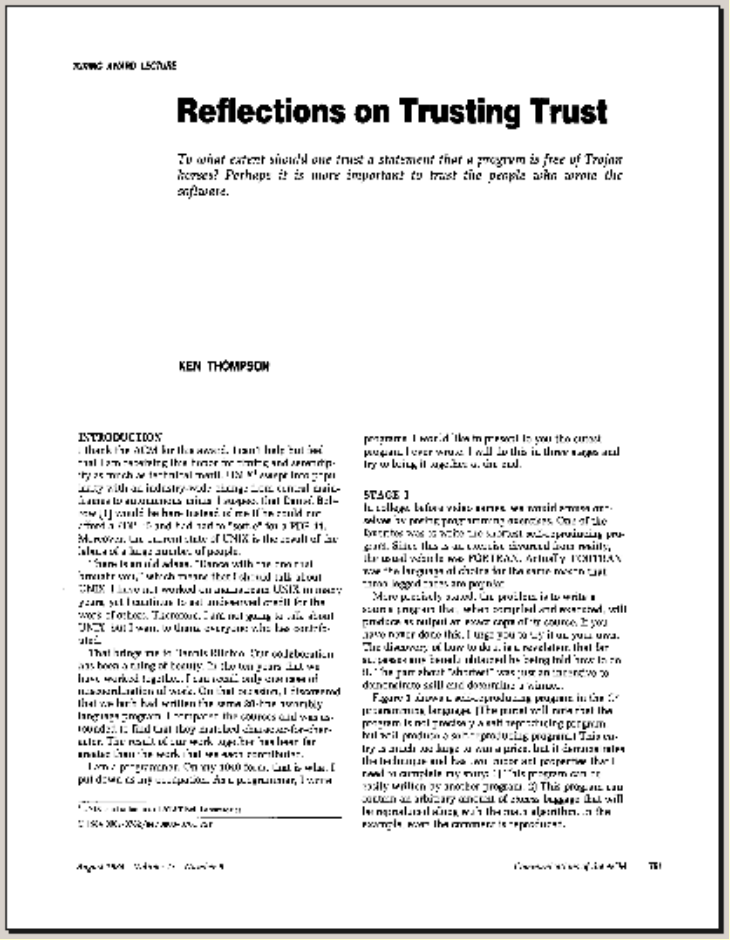
- Bruce Schneier: "*Ne spominjam se nobenega kriptografskega sistema, razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake.*".

- Bruce Schneier: "*The problem with bad security is that it looks just like good security. You can't tell the difference by looking at the finished product.*"
- Snakeoil – "kačja slina". Indici, s katerim lahko prepoznamo potencialno slabe produkte.

Ali transparentnost *zagotavlja* varnost

- **Transparentnost varnosti ne zagotavlja sama po sebi, pač pa jo *lahko* omogoča oz. olajšuje!**
- Primeri:
  - Open GPG ranljivost, odkrita marca 2006, prisotna je bila dlje časa. Omogočala je ponarejanje digitalno podpisanih elektronskih sporočil.
  - V maju 2008 je bila odkrita ranljivost v Debianovem generatorju naključnih števil. Ranljivosti ni nihče opazil približno 9 mesecev. Prizadeti so bili SSH, OpenVPN, DSNSEC, SSL/TLS, DSA ter ključi uporabljeni v X.509 certifikatih.

Ali transparentnost *zagotavlja* varnost



TURING AWARD LECTURE

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

INTRODUCTION

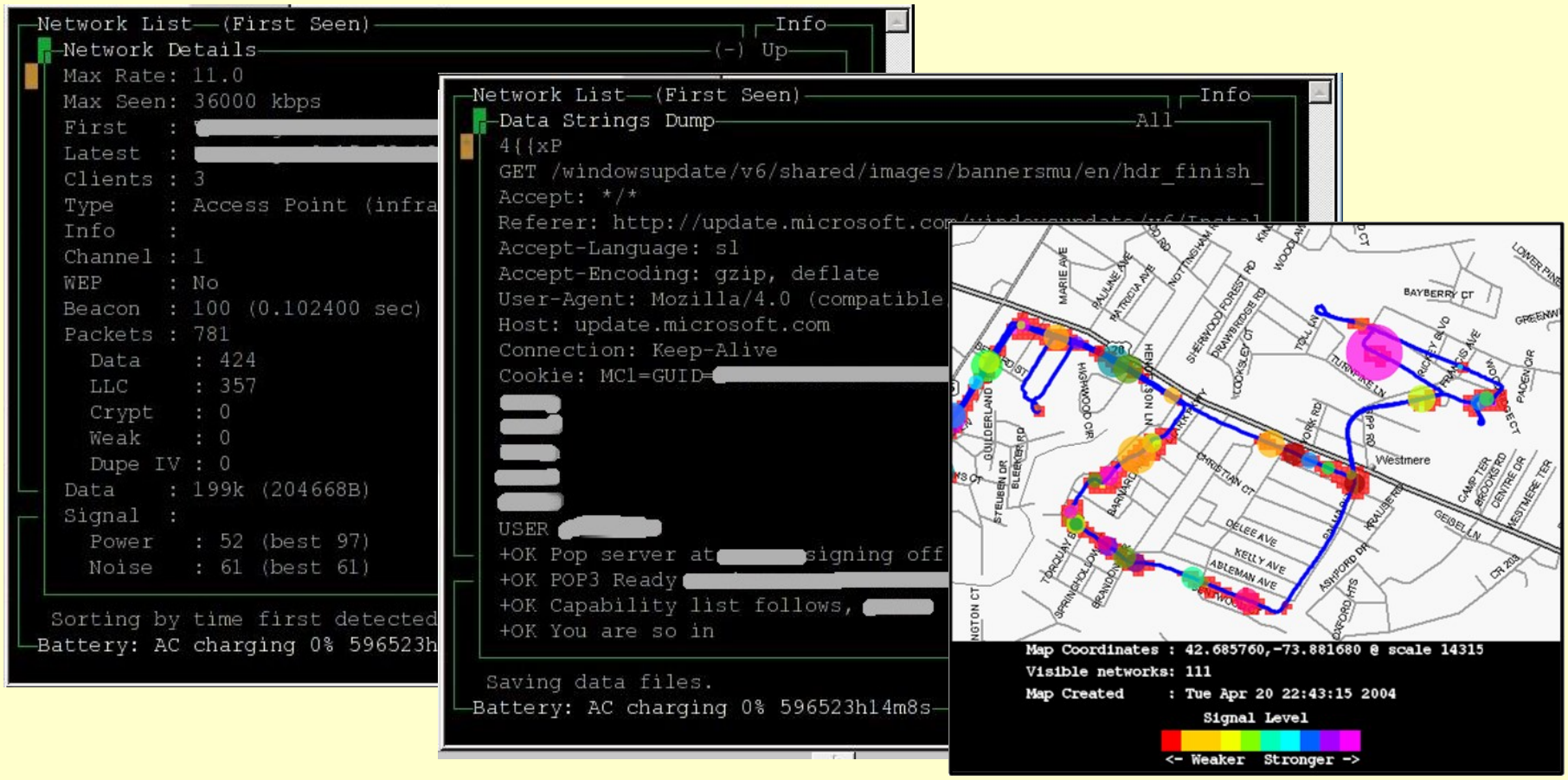
STAGE I

- Ken Thompson. 1984. Reflections on Trusting Trust. Communication of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763.
- Virus: Win32.Induc.a, ki okuži prevajalnik Delphi (<http://www.h-online.com/security/Virus-infects-development-environment--/news/114031>)

IV: Napadi na slabosti v algoritmu ali slabosti v implementaciji algoritma

- Ranljivosti algoritmov (primer: napadi na DES, AES, SHA-1, MD5, WEP, WPA,...).
- Ranljivosti v implementaciji algoritmov (primer: Debian PRNG, DSA ranljivost, OpenGPG)
- Napadi na algoritem A5 (v uporabi v GSM omrežju; A5/3 - Kasumi).

Primer: varnost v brezžičnih omrežjih



Prestrezanje v brezžičnih omrežjih s pomočjo programa *Kismet Wireless*. S programi kot so Airodump, Aircrack, Wepcrack, itd. je mogoče tudi razbijati zaščito brezžičnih omrežij (izvajati kriptoanalizo, itd.). Vir in avtorstvo: Matej Kovačič in dokumentacija programa Kismet Wireless. [FILM]

Primer: varnost v brezžičnih omrežjih

- WEP zaščito so strli strli leta 2001... od leta 2007 je za to potrebna le minuta.
- Leta 2004 so v WPA našli nekaj ranljivosti...
- Leta 2008 sta Martin Beck in Erik Tews WPA zaščito strla. Za razbitje TKIP ključa (*Temporal Key Integrity Protocol*) sta potrebovala približno 15 minut.
- Od letos je za razbitje WPA potrebna le še minuta.
- Priporoča se uporaba WPA2...

Primer: Data Encryption Standard

- V poznih 60-tih letih 20. stoletja so pri IBM zaradi strahu pred računalniškim kriminalom pričeli razvijati kriptografijo za komercialne namene.
- Leta 1971 so razvili šifrirno napravo Lucifer - poseben algoritem, ki je bil implementiran v majhnem čipu. V tistem času je bila to najmanjša šifrirna naprava na svetu.
- Leta 1973 je ameriški *National Bureau of Standards* želel pripraviti standard za šifriranje civilnih komunikacij.

Primer: Data Encryption Standard

- Uslužbenci NSA so redno obiskovali IBM in spremljali njihov napredek.
- Lucifer je uporabljal 128-bitni šifrirni ključ, vendar pa je NBS v sodelovanju z NSA Lucifer za civilno uporabo priredila.
- 128-bitni šifrirni ključ so skrajšali na 64 bitov, pri čemer pa je bilo 8 bitov kontrolnih in je bila torej dejanska dolžina ključa samo 56 bitov, poleg tega pa so priredili še nekatere matematične postopke v samem algoritmu (S-boxe).

Primer: Data Encryption Standard

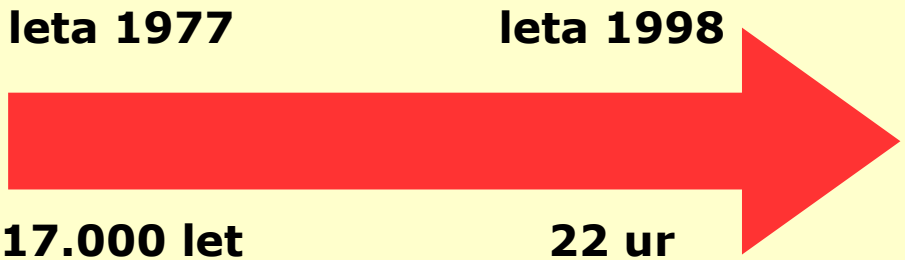
- Revizija NSA ugotovila, da v algoritmu ni nobenih statističnih ali matematičnih slabosti, januarja 1977 je algoritem postal *Data Encryption Standard*.
- Pred tem je bil algoritem deležen številnih kritik. Hellman in Diffie sta izračunala, da bi bilo mogoče s posebnim računalnikom za 20 milijonov USD 56-bitni DES v povprečju razbiti v manj kot pol dneva, vsako razbitje pa bi stalo 5000 USD.
- V 10 letih bi tak računalnik stal samo 200.000 USD, vsaka rešitev pa le 50 USD.

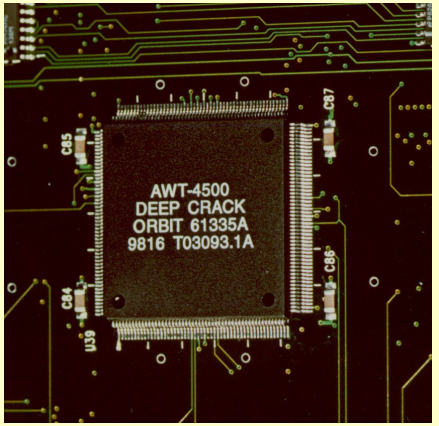
Primer: Data Encryption Standard

- NBS je v odgovor kritikam osnoval dve delavnici na temo DES-a, na katerih so prišli do zaključka, da bi razbijanje DES-a trajalo 17.000 let.
- V letih 1990 in 1991 sta kriptografa Eli Biham in Adi Shamir predstavila novo vrsto kriptoanalize, ki sta jo poimenovala diferencialna kriptoanaliza (ang. *differential cryptanalysis*).
- Civilna različica DES naj bi bila prirejena tako, da je bila učinkovitost do tedaj neznanega napada z diferencialno kriptoanalizo povečana.

Primer: Data Encryption Standard

- Julija 1998 so pri EFF predstavili napravo DES Cracker, ki je s pomočjo metode grobe sile in distribuiranega procesiranja podatkov prek interneta razbila DES v 22 urah.
- Istega leta je skupina kriptografov predstavila tudi DES Cracker za 250.000 dolarjev, ki je DES razbila v manj kot treh dneh.





EFF-jev DES Cracker
Vir in avtorstvo: Wikipedia.

Primer: varnost GSM telefonije

- Šifrirni algoritem A5/1 je bil razvit leta 1987, A5/2 pa leta 1989.
- Oba algoritma sta bila razvita na skrivaj in ob sodelovanju tajnih služb.
- Ross Anderson iz *University of Cambridge* je leta 1994 izjavil, da so v tajnih službah zveze NATO v sredi 1980-tih let precej razpravljali o vprašanju ali naj bo GSM šifriranje močno ali šibko.
- Problem namerno šibke varnostne zasnove GSM: prisluškovanje brez sodne odredbe.

Primer: varnost GSM telefonije

- Algoritem A8 sta Ian Goldberg in David Wagner teoretično razbila aprila 1998.
- Avgusta 1999 dokazala, da je razbitje A5/2 mogoče v realnem času.
- Prvi uspešni teoretični napad na algoritem A5/1 je izvedel Jovan Golić maja 1999 neodvisno od njega pa tudi Marc Briceno, ki je izvedel reverzni inženiring na GSM telefonu.
- Biryukov in Shamir sta dokazala, da ga je mogoče razbiti v manj kot sekundi z uporabo računalnika z vsaj 128 Mb RAM ter dvema 73 Gb diskoma.

Primer: varnost GSM telefonije

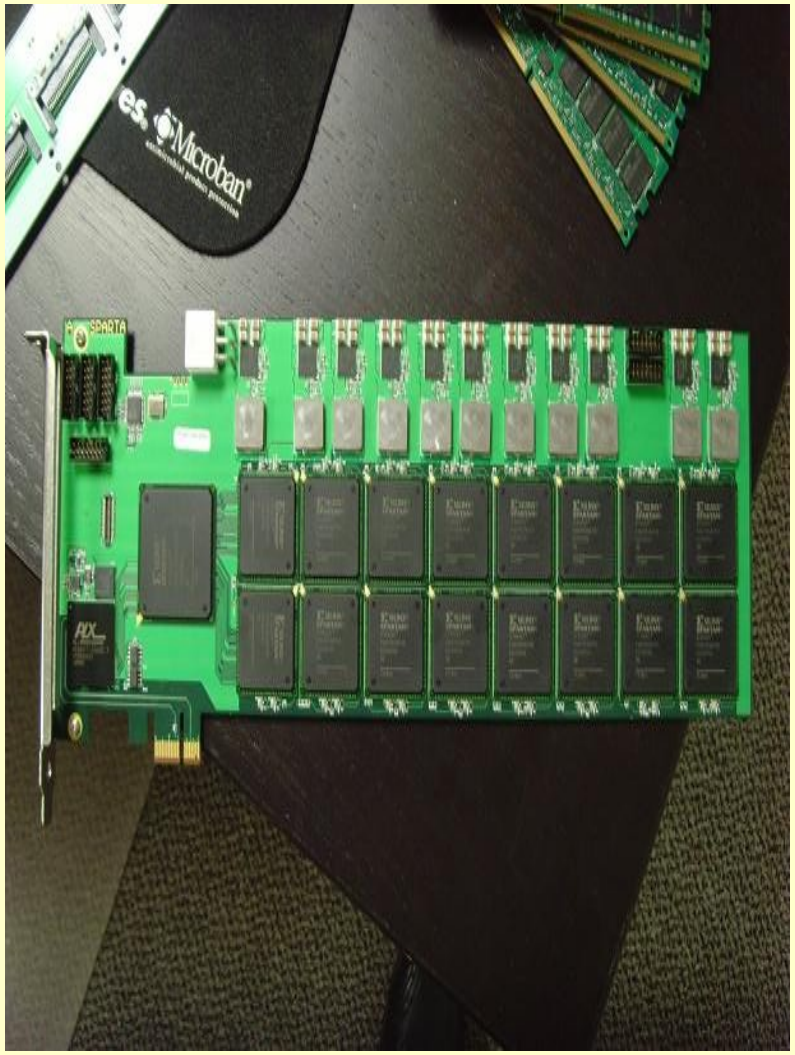
- David Hulton in Steve Muller leta 2007 začneta z razvoje odprtokodne GSM prisluškovalne naprave za manj kot 1000 USD (The A5 Cracking Project, The GSM Software Project).
- V začetku leta 2008 so Timo Gendrullis, Martin Novotny in Andy Ruppiz iz nemškega Inštituta za IT varnost na Ruhr-University Bochum objavili članek z naslovom A Real-World Attack Breaking A5/1 within Hours v katerem opisujejo praktičen napad, ki ga je mogoče izvesti s posebno napravo, COPACOBANA (*Cost-Optimized Parallel Code Breaker*).

Primer: varnost GSM telefonije

- Raziskovalci v članku trdijo, da je uspešen napad mogoče izvesti v povprečju v okrog sedmih urah, predstavljajo pa tudi optimizacijo, ki omogoča še približno 16% pohitritev napada.
- THC -> AirProbe (izračun tabel s CUDA)...

- Danes GSM uporablja več kot 2 milijardi uporabnikov, slabo zasnovano infrastrukturo pa bo izredno težko v kratkem času nadgraditi v varnejšo.

GSM Cracking Project -> AirProbe

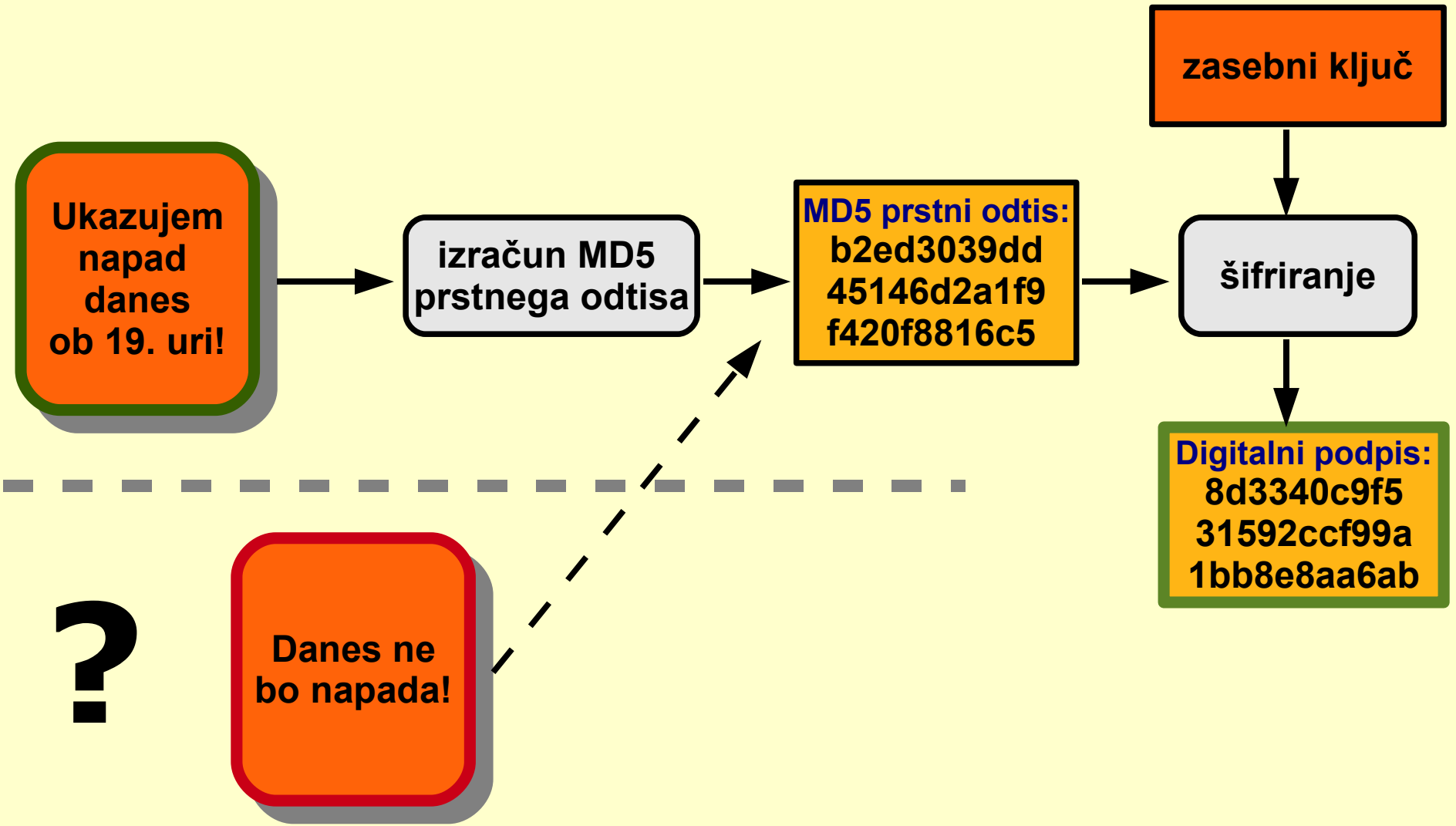


FPGA (Field-Programmable Gate Array) in *The A5 Buster*.
Vir in avtorstvo: thc.org

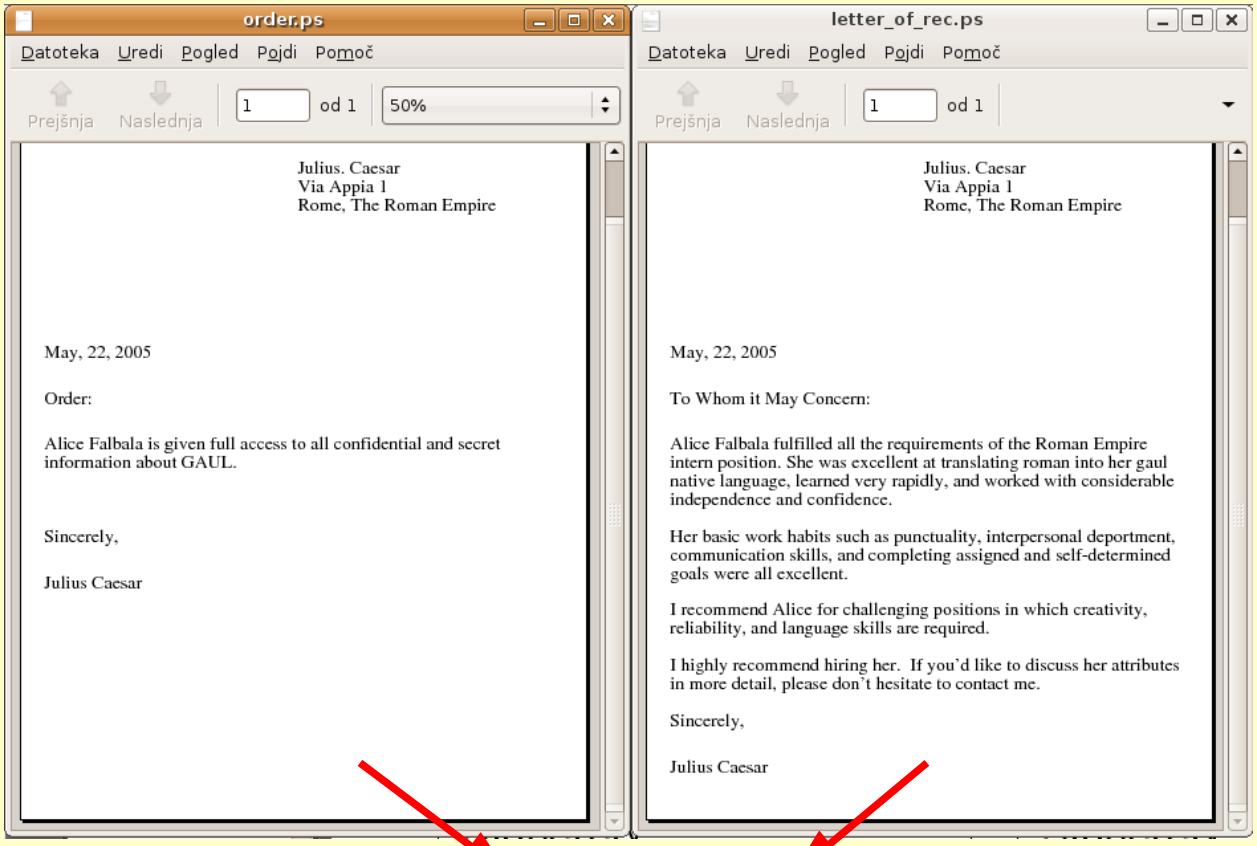
Primer: varnost zgostitvenih algoritmov

- Zgostitveni algoritmi se uporabljajo pri digitalnem podpisu – z njihovo pomočjo se prepričamo, da sporočilo med prenosom ni bilo spremenjeno.
- Problem: ne sme priti do kolizije (ne smeta obstajati dve različni sporočili, ki bi vrnili isto kontrolno vsoto).
  - Kolizijo v SHA-0 so našli leta 2004.
  - Kolizijo v SHA-1 so našli leta 2005.
  - Kolizijo v MD5 so našli leta 2005.

Primer: varnost zgostitvenih algoritmov



Primer: varnost zgostitvenih algoritmov



MD5: 5421a523481fdc6a2a1c832e72c7b8a5

Vir: Magnus Daum in Stefan Lucks: The Story of Alice and her Boss: Hash Functions and the Blind Passenger Attack (Eurocrypt 2005, http://th.informatik.uni-mannheim.de/People/lucks/HashCollisions/rump_ec05.pdf).

Primer: varnost zgostitvenih algoritmov

```
matej@kovacic-m:~/Desktop$ md5sum hello.exe
cdc47d670159eef60916ca03a9d4a007  hello.exe
matej@kovacic-m:~/Desktop$ md5sum erase.exe
cdc47d670159eef60916ca03a9d4a007  erase.exe

matej@kovacic-m:~/Desktop$ wine hello.exe
Hello, world!
(press enter to quit)q
matej@kovacic-m:~/Desktop$ wine erase.exe
This program is evil!!!
Erasing hard drive...1Gb...2Gb... just kidding!
Nothing was erased.
(press enter to quit)q
```

Vir: Peter Selinger, 2006, http://www.mscs.dal.ca/~selinger/md5collision/.

Napadi na sodobne algoritme

- **AES**: sredi leta 2009 sta Biryukov in Khovratovich prikazala prvi napad na AES-256, ki je uspešnejši od napada z grobo silo. Kompleksnost napada je bila 2^119, kasneje so jo še izboljšali. Napad je zaenkrat zgolj teoretičen.
- **OpenGPG**: v določenih okoliščinah je bilo mogoče delno rekonstuirati digitalno podpisano in šifrirano sporočilo.

Napadi na sodobne algoritme

- **DSA ranljivost**: varnost DSA zelo odvisna od varnosti tim. naključnega izziva (ang. *random challenge*) k. Če je ta parameter znan, je mogoče izračunati celoten zasebni ključ uporabnika.
- Zaradi napake v Debianovem generatorju naključnih števil so ranljivi tudi vsi DSA ključi, ki so bili zgolj *uporabljeni* v sistemih z okvarjenim generatorjem naključnih števil.
- To pomeni, da napadalec lahko v arhivu poišče DSA podpise uporabnika, ki jih je ta naredil (s sicer varnim ključem) na ranljivem sistemu ter tako retroaktivno rekonstruira uporabnikov zasebni ključ.

IV: Napadi na šifrirne ključe in gesla

- Napad z grobo silo (brute force).
- Napad s slovarjem (dictionary attack).
- “Obnavljanje” gesel (varnostno vprašanje).
- Ugibanje gesel.
- Kraja gesel.

Neustrezna gesla

- Večji ključ – večja varnost.
- Večje in bolj kompleksno geslo – večja varnost.
- Bolj kompleksno geslo – težje za zapomnit (večja verjetnost, da si ga bo uporabnik zapisal).
- Neustrezno hranjena gesla.
  - Primer: listki na monitorju ali pod tipkovnico.
- Uporaba istih gesel na različnih sistemih!

Neustrezna gesla

- Avtentikacija z znanim podatkom (“varnostna vprašanja” za obnovo gesla).
  - primer: sosed sosedu ukradel geslo za dostop do elektronske pošte.
- Napad na geslo:
  - z metodo grobe sile (*bruteforce attack*);
  - s slovarjem (*dictionary attack*).
- Cain & Abel, L0pht crack (LC5), Advanced PDF Password Recovery,...

Ugibanje gesel

- Top 20 gesel: password1, abc123, myspace1, password, blink182, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 in monkey.
- 1,000 korenov “letmein”, “temp”,... + 100 dodatkov (“1”, “abc”,...) obnovi okrog 24% vseh gesel.
- Z upoštevanjem osebnih podatkov, datumov, itd., je mogoče v mesecu dni uganiti 2/3 vseh gesel.

Način izbire gesel

We hacked Dan's assets first through finding bugs and writing 0day, and then through abusing him giving away passwords and his silly password scheme. Check out just some of his passes:

fuck.hackers, 0hn0z (root account on his mail box), fuck.omg, fuck.vps, ohhai

Five character root password? Niiiiiiice.

From .mysql_history:

SET PASSWORD FOR 'root'@'localhost' = PASSWORD('fuck.mysql');

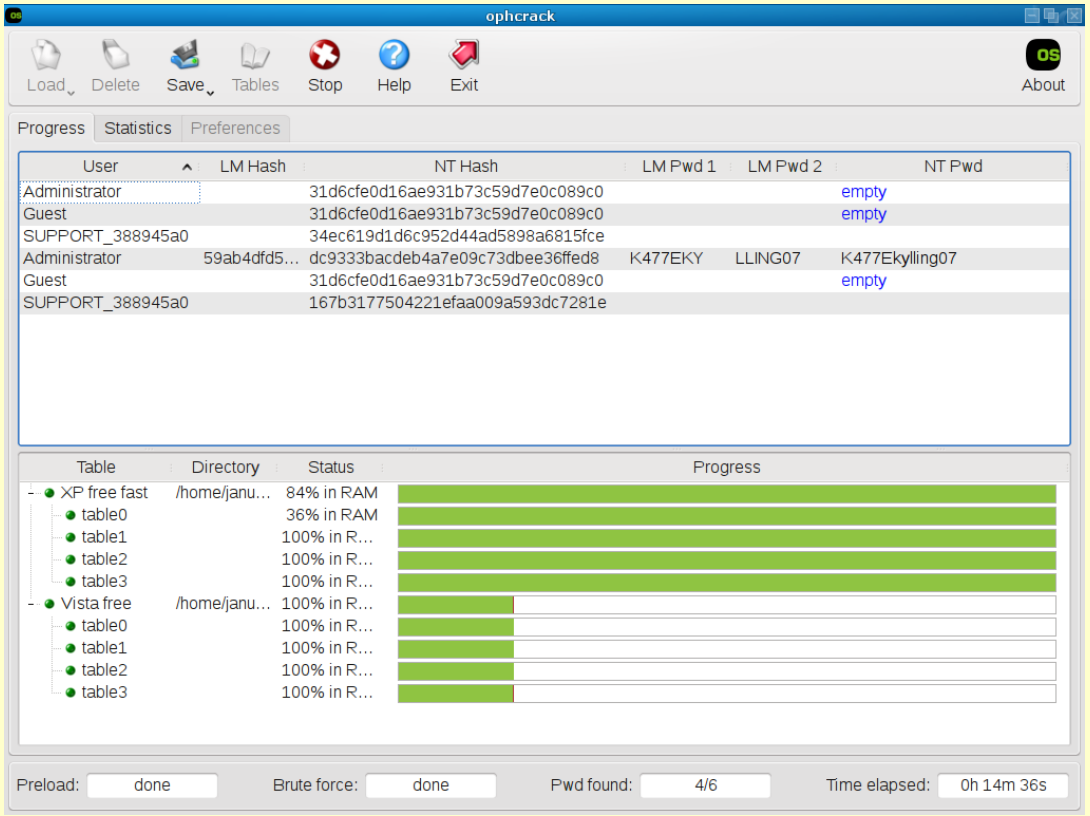
See the pattern?

Zero for Owned, Vol. 5, <http://www.rec-sec.com/files/zf05.txt>


IN THE PRESS CENTRE
A FREE WLAN
CONNECTION IS
AVAILABLE
WIFI: skoda
PASSWORD: skodaskoda
ŠkodaYeti
PRESS-LAUNCH 2009

Razbijanje gesel

- John the Ripper, Cain and Abel, Ophcrack, LOphtCrack,...



Vir in avtorstvo: Ophcrack.

Kopije ključev

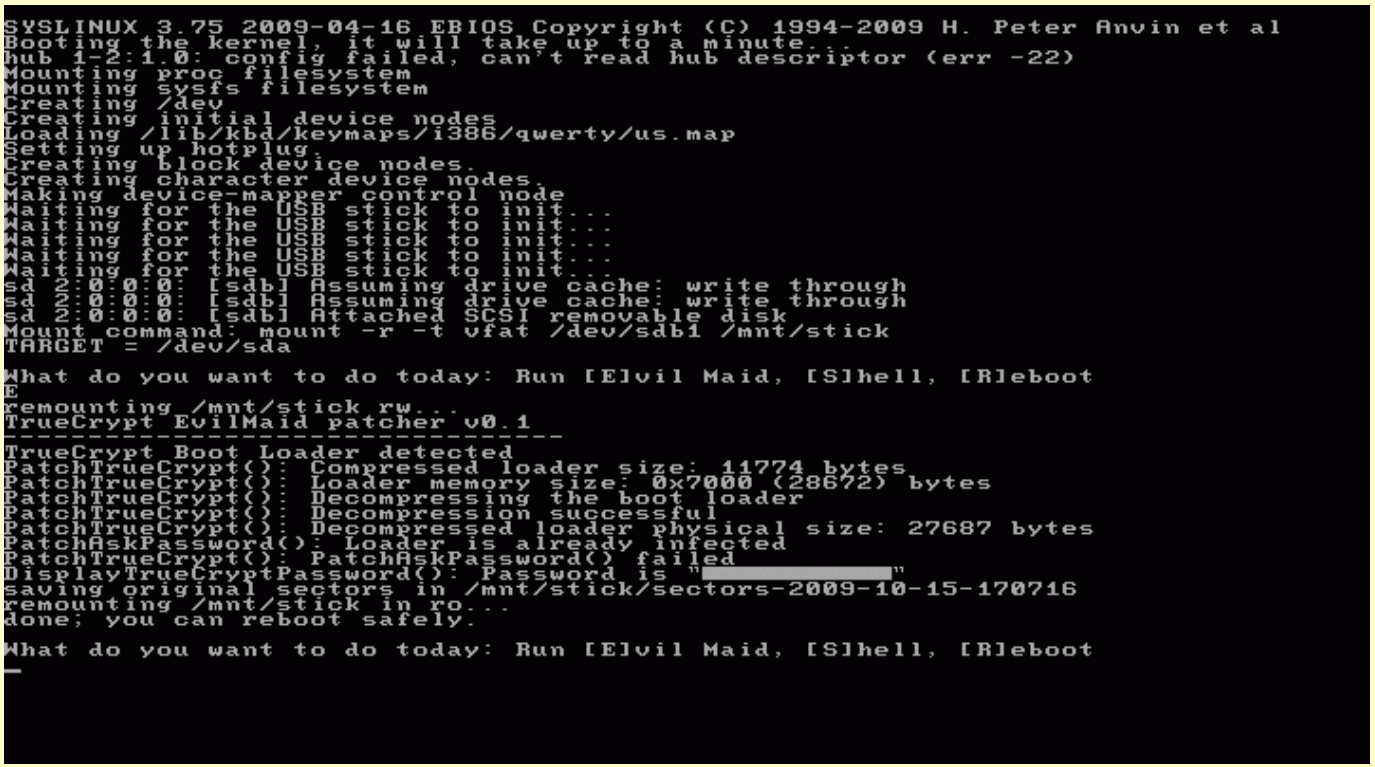
- Key Escrow v ZDA.
- Primer BlackBerry:
  - Leta 2008 se je kanadsko podjetje *Research In Motion* odločilo, da bo indijski vladi izročilo kopije šifrirnih ključev s katerimi komunicirajo BlackBerry naprave individualnih uporabnikov.

Kraja ključev

- Benjamin Laxton, Kai Wang, in Stefan Savage: Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding, ACM CCS 2008, Alexandria, VA, October 2008.

Kraja ključev

- Evil Maid napad na TrueCrypt.



V: Napačna uporaba kriptografije

- Primeri:
  - Lorenz SZ 40,
  - primeri neupoštevanja varnostnih politik,
  - napačen način delovanja v bločnih šifrirnikih,
  - napačna uporaba varnostnih mehanizmov (Snakes-On-A-Tor, zaščita e-pošte).

Primer: Lorenz SZ 40

- Leta 1941 so Nemci pričeli testirati šifrirano teleprintersko povezavo med Dunajem in Atenami.
- 30 avgusta 1941 je nemški operater poslal dve 4000 znakov dolgi sporočili, pomotopa pa sta bili obe zašifrirani z istim ključem.
- Britanci so sporočili prestregli in se lotili kriptoanalize.
- Ob predpostavki, da je bil uporabljen isti ključ, velja: čistopis1 – čistopis2 = šifropis1 – šifropis2.

$$p' - p'' = c' - c''$$

Primer: Lorenz SZ 40

c''		Q	I	2	4	5		G	R	J	M	L		C	Y	5	0	H		K	A	S	1	I
c'		T	G	2	H	H		1	Q	J	X	V		K	1	B	J	M		K	2	O	M	Z
d		u	m	0	m	p		s	x	0	e	n		e	r	3	j	4		0	u	x	a	q

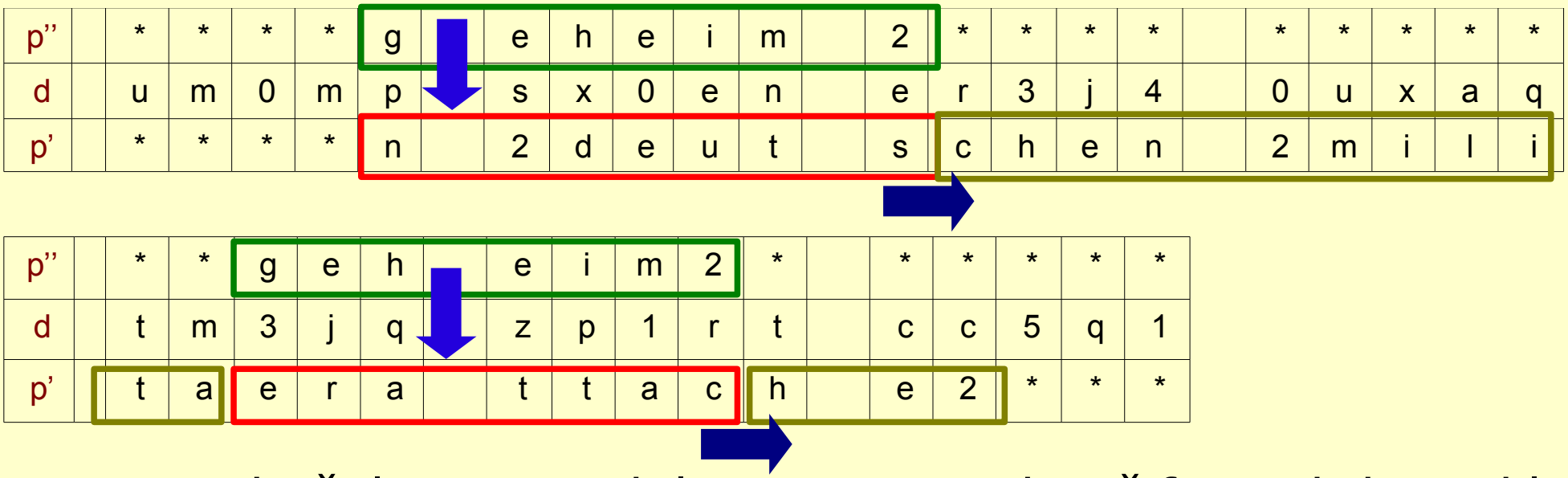
c''		S	5	X	U	N		S	R	Z	Z	B		D	B	B	1	C
c'		Y	V	I	N	3		H	M	C	3	D		U	Q	3	4	Z
d		t	m	3	j	q		z	p	1	r	t		c	c	5	q	1

Britanci so najprej izračunali razliko (*d*) med šifriranima besediloma *c′* in *c″*...

(Velja, da je ta razlika enaka razliki med nešifriranima besediloma.)

Vir: Friedrich Ludwig Bauer, Decrypted Secrets, 2007.

Primer: Lorenz SZ 40



Nato so skušali uganiti del enega izmed nešifriranih besedil (*p''*). Začeli so z najbolj pogostimi ali verjetnimi besedami (npr. *geheim* – nem. tajnost; številka 2 je oznaka za presledek) ter od tega besedila odšteli razliko *d* ter gledali ali se v drugem besedilu (*p'*) pojavi smiselna beseda.

Preostanek besedila so skušali uganiti.

Primer: Lorenz SZ 40

p''		*	*	*	*	g		e	h	e	i	m		2	2	k	r	2		2	3	3	z	z
d		u	m	0	m	p		s	x	0	e	n		e	r	3	j	4		0	u	x	a	q
p'		*	*	*	*	n		2	d	e	u	t		s	c	h	e	n		2	m	i	l	i

p''		0	1	g	e	h		e	i	m	2	2		k	r	*	*	*
d		t	m	3	j	q		z	p	1	r	t		c	c	5	q	1
p'		t	a	e	r	a		t	t	a	c	h		e	2	*	*	*

Nato so z odštevanjem drugega nešifriranega besedila (*p'*), ki so ga uganili, rekonstruirali del prvega nešifriranega besedila (*p''*).

****geheim22kr2233zz01geheim22kr**
****n2deutschen2militaerattache2**

spruchnummer 7027 30.8. *1210 ++ 7027 30.8. *1210 ++ * geheim kr ++geheim kr +an deutschnem_militaarattache in athen+lage nr.2997

Neupoštevanje varnostnih politik

- Neustrezno zavarovanje terminalne opreme.
- Neustrezno zavarovanje ključev in gesel.
- Neustrezno zavarovanje dešifriranega sporočila, neustrezna hramba varnostnih kopij.
- Neuporaba šifriranja pri prenosu čez omrežje.
- Primeri:
  - projekt Venona: NSA je okrog leta 1946 uspela razbiti kriptograme sovjetske tajne službe KGB, ki so nastali s pomočjo metode *one-time pad*. Do razbitja je prišlo zaradi nemarnosti sovjetske tajne službe, ki je dele šifrirnih ključev uporabila večkrat.

Neupoštevanje varnostnih politik

- 5. avgusta 1914 so Britanci presekali morske kable Nemčije, zato so Nemci nekaj časa morali komunicirati po kanalih, ki niso bili varni (vir: Kahn, The Codebreakers, 1973: 129)
- Nemška vojska je med 2. svetovno vojno za pomembnejše komunikacije uporabljala šifrirni stroj *Lorenz SZ (Schlüsselzusatz) 40* in *Lorenz SZ 42*. 30 avgusta 1941 je nemški operater poslal 4000 znakov dolgo sporočilo, vendar sporočilo ni pravilno prispelo do prejemnika.

Neupoštevanje varnostnih politik

- Prejemnik je zato v nešifriranem načinu prosil za ponovno pošiljanje, pošiljatelj pa je nato naredil napako: sporočilo je ponovno poslal in sicer z istim ključem (HQIBPEXEZMUG), vendar ga je malce spremenil. Iz teh dveh kriptogramov je potem John Tiltman uspel obnoviti nešifrirano besedilo in ključ. S pomočjo ključa je nato W. T. Tutte rekonstruiral celotno šifrirno napravo (vir: Bauer, Decrypted Secrets, 2007: 389).

Neupoštevanje varnostnih politik

- Leta 1941 je bila italijanska vojska, ki je okupirala Albanijo za nekaj časa močno izpostavljena jugoslovanski vojski. Jugoslavija bi namreč lahko italijanski vojski zadala močan udarec, saj je 7. aprila 1941 iz Cetinja napotila eno divizijo proti Skadarju, drugo pa iz Kosovske Mitrovice proti Kukesu.
- Italijanska *Servizio Informazione Militare* je zato obema divizijama 13. aprila 1941 ob 10 uri poslala telegram naj se umakneta na izhodiščne položaje. Sporočilo je zašifrirala z šiframi jugoslovanske vojske in dodala podpis generala Dušana Simoviča.

Neupoštevanje varnostnih politik

- Divizija, ki je napredovala proti Kukesu se je nemudoma ustavila, divizija iz Cetinja pa je od generalštaba zahtevala potrditev. Potrditve ni bilo, zanikanja pa tudi ne, in naslednji dan so začeli z umikom.
- Italijanska vojska je zato lahko od Kotorja proti Cetinju hitro napredovala. Dan zatem je jugoslovansko vojaško vodstvo sporočilo, da ni ukazalo umika, vendar je bilo že prepozno. Tudi razkritje zloma šifrirnega sistema je v naslednjih dneh, ko je štela vsaka ura postalo nerelevantno, saj je Jugoslavija 17. aprila 1941 kapitulirala. (vir: Kahn, The Codebreakers, 1973: 246-247).

Neupoštevanje varnostnih politik

- NSA je v Vietnamu izvajala monitoring komunikacij (Comsec) ameriške vojske z namenom svetovati kako izboljšati varnost.
- Nekoč se je eden izmed poveljnikov *1st Infantry Division* pogovarjal po telefonu, ko je nekdo vstopil in omenil, da se bo naslednji dan izvedla specifična vojaška operacija 35 milj severno.
- NSA je o tem takoj obvestila poveljnika, ki pa ni spremenil načrtov. Naslednji dan so v operaciji naleteli na nenavadno močan odpor in imeli 58 mrtvih in 82 ranjenih (vir: Bamford, Body of Secrets, 2001: 311).

Neupoštevanje varnostnih politik

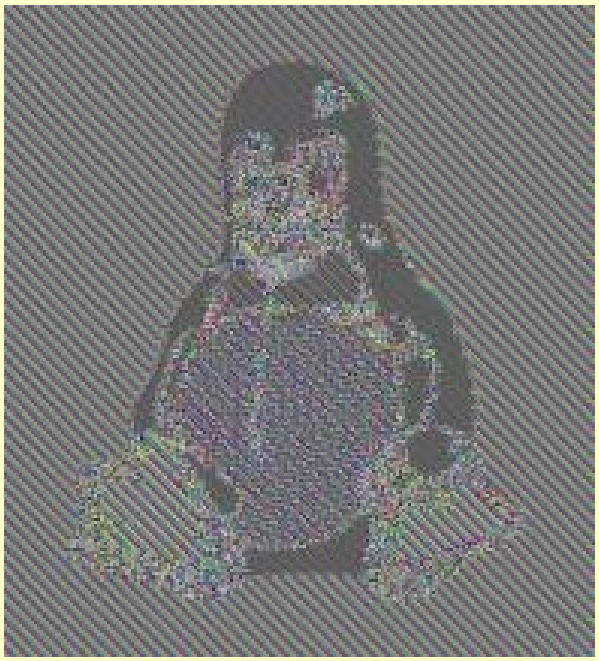
- Novembra 2007 v Britaniji pri pošiljanju iz enega urada v drugega izgubijo diske s podatki o vseh prejemnikih otroškega dodatka, osebne podatke vseh družin z manj kot 16 let starimi otroci ter imena, naslove, rojstne podatke, številko zdravstvenega zavarovanja ter bančne podatke o 25 milijonih posameznikov.
- Julija 2008 uslužbenec obveščevalno-varnostnega oddelka britanskega urada predsednika vlade na vlaku pozabi kopijo zaupnih dokumentov o teroristični mreži Al-Kajda.
- itd. ...

Primer: uporaba napačnega načina delovanja v bločnih šifrirnikih

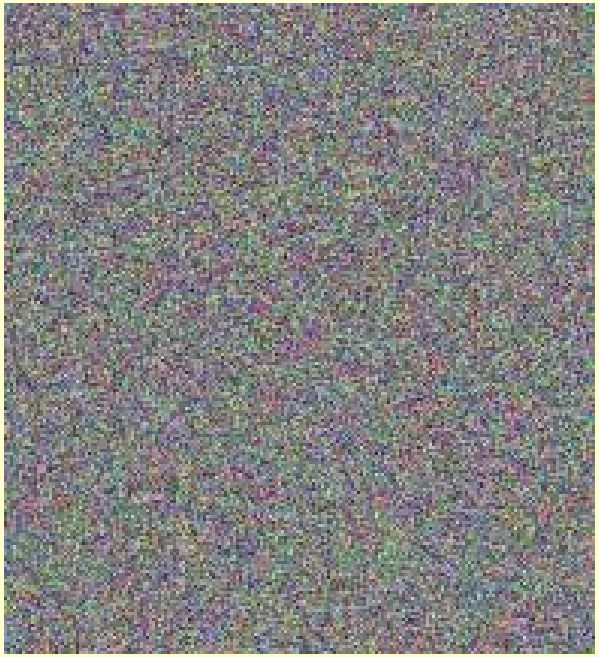
- Bločni šifrirniki (ang. *block cipher*) šifrirajo bloke fiksne dolžine (navadno 64 ali 128 bitov). Ker šifriranje istega čistopisa z istim ključem privede do istega tajnopisa, se pri šifriranju uporablja razlilčne načine delovanja bločnih šifrirnikov (ang. *modes of operation*), s katerimi se skuša zagotoviti tajnost sporočil poljubne dolžine.
- Način *electronic codebook* (ang. *ECB mode*) sporočilo razdeli na bloke, kjer zašifrira vsakega posebej.
- Enaki bloki imajo enak tajnopis. Včasih to lahko privede do katastrofalnih posledic...

Primer: neustrezna uporaba načina delovanja v bločnih šifrirnikih

nešifrirana slika



slika šifrirana v ECB načinu



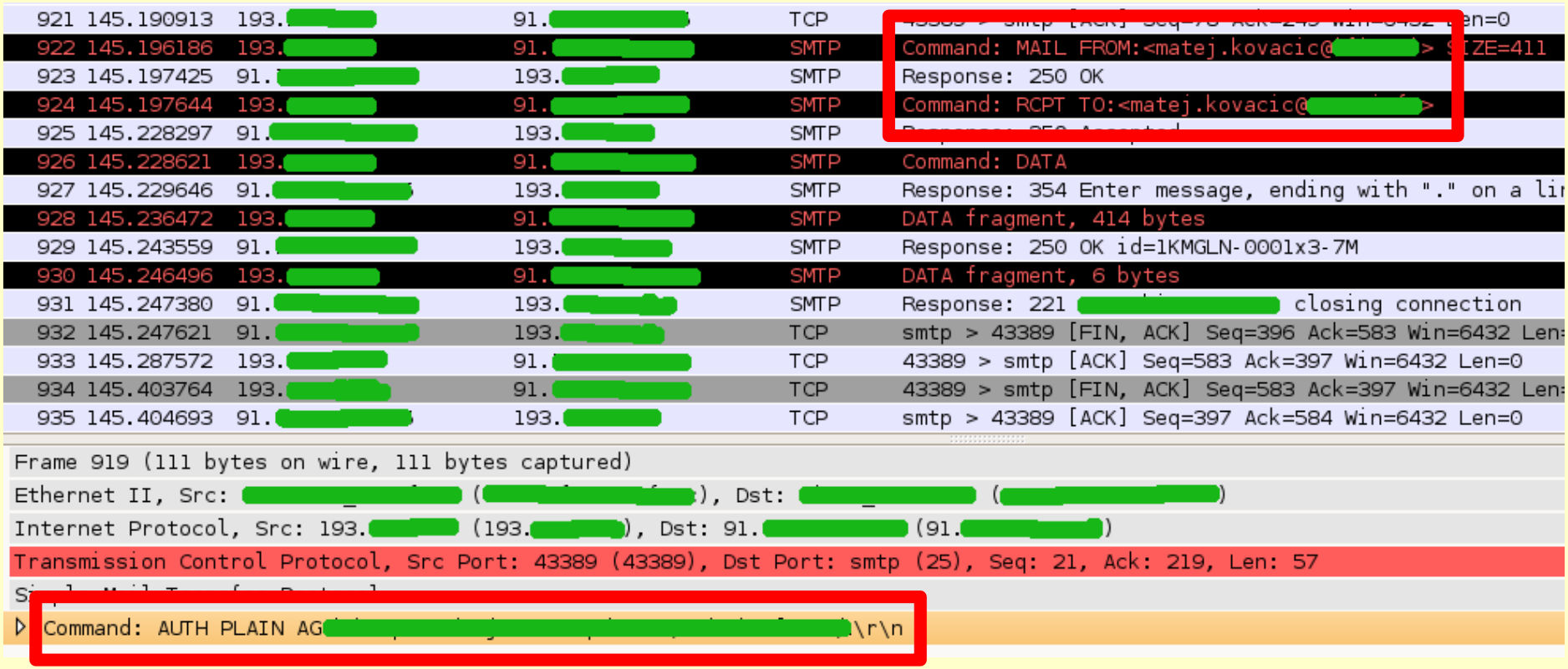
slika šifrirana v drugem načinu

Vir in avtorstvo: Wikipedia, geslo: Block cipher modes.

Napačna uporaba varnostnih mehanizmov

- Snakes-On-A-Tor (več o tem kasneje...);
- Uporaba SMTP avtentikacije na nezaščiteni povezavi: primer ponudnika elektronske pošte, ki ponuja varno POP3 povezavo (SSL), ne ponuja pa varne SMTP povezave, pač pa celo zahteva SMTP avtentikacijo...

Napačen način uporabe varnostnih mehanizmov za zaščito e-pošte



`Command: AUTH PLAIN AG1hdGVqLmtvdmFjaWNAKioqKiouc2kAZ2VzbG8hrg==`

Uporabniško ime in geslo sta Base64 kodirana...

`Command: AUTH PLAIN` **`matej.kovacic@*****.si|geslo!`**

V: Posredni napadi (ang. *channel side*)

- Problem fizičnega dostopa.
  - Tempest napad.
- Napadi na programsko kodo.

Kje je lahko šibki člen?

- *"On the other hand, the NSA has made significant progress against less cryptologically sophisticated countries and, from them, gained insight into plans and intentions of countries about which the US has greater concerns. Thus, when a Chinese diplomat at the United Nations discusses some new African venture with a colleague from Sudan, the eavesdroppers at the NSA may be deaf to the Chinese communications links but they may be able to get that same information by exploiting weaknesses in Sudan's communications and cipher systems when the diplomat reports the meeting to Khartoum."*

James Bamford, Who's in Big Brother's Database?, <http://www.nybooks.com/articles/23231>

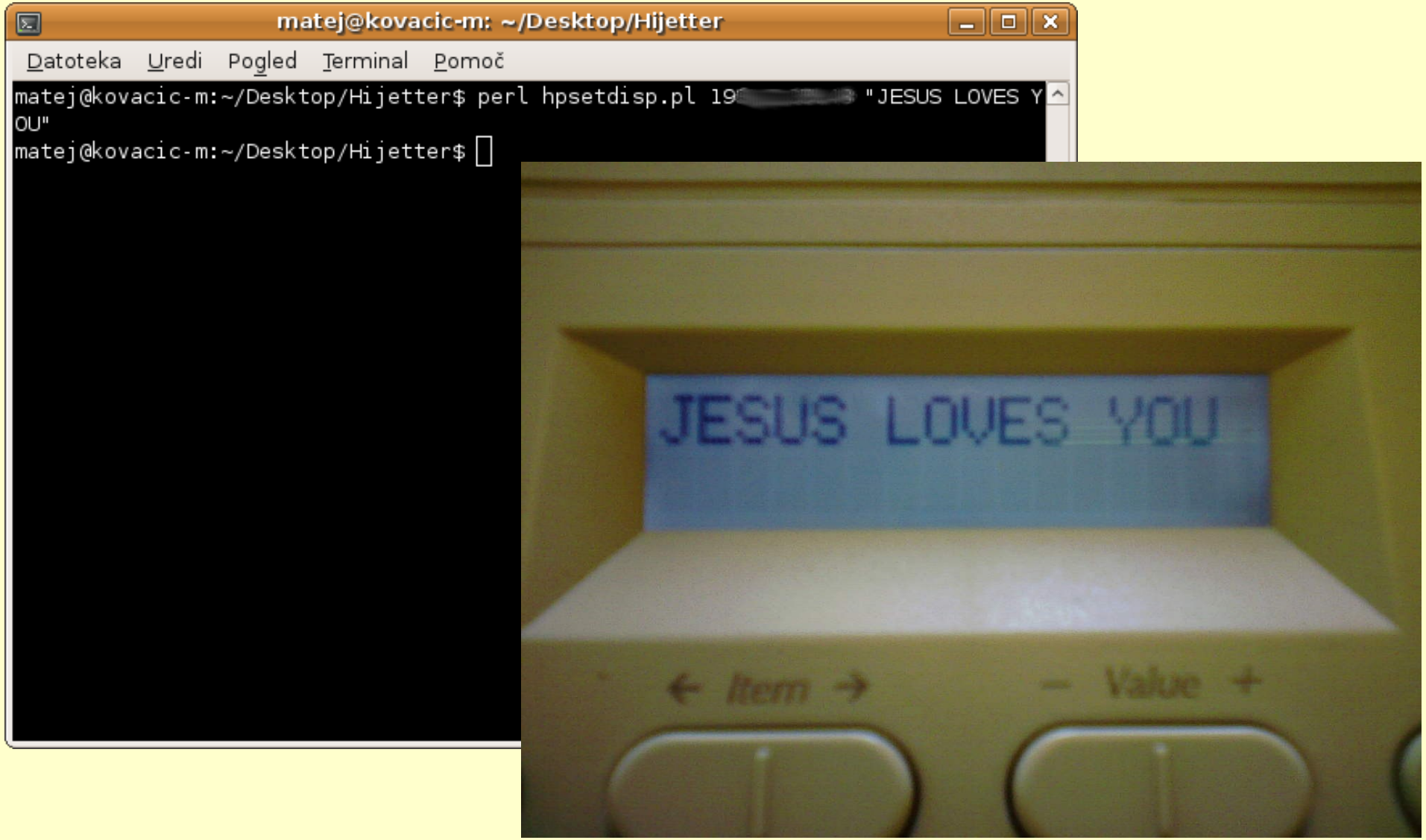
Fizični dostop in okolica sistema

- Kdo ima kopije ključa?
  - Primer: servis za “vnebovzetje” (Schneier, 2. junij 2008).
- Kdo ima kopije nešifriranega sporočila?
  - Primer: je tiskanje preko omrežnega tiskalnika varno?
  - Google Desktop Search index?
- Nevarnost zasega kopije ključa (npr. z živim CD-jem).
  - Izognitev varnostnim mehanizmom za zaščito dostopa do šifrirnega ključa: primer “Utilman hack” v Windows Vista. [FILM]

Fizični dostop in okolica sistema

- Zaupanja (ne)vredna strojna oprema:
  - sodobni tiskalniki niso periferne naprave, pač pa strežniki in delovne postaje z lastnim operacijskim sistemom,... Nekateri tiskalniki dokumente skrivaj označujejo z digitalnim vodnim tiskom, ki vsebuje serijsko številko tiskalnika, kar omogoča identifikacijo dokumenta).
  - Primer: *Hijetter*, orodje za izrabo tiskalnikov, ki omogoča spreminjanje napisa na zaslonu, zaklepanje tipkovnice, shranjevanje datotek na tiskalnik, itd...

Fizični dostop in okolica sistema



Fizični dostop in okolica sistema

- Okolica šifriranega sistema:
  - Schneier je leta 2008 s sodelavci pokazal, da okolje šifrirnega programa beleži določene podatke zunaj *Deniable File System* sistema. Tako operacijski sistem Windows Vista (pa tudi ostali) npr. hranijo bližnjice z imeni datotek. Programi za neposredno urejanje datotek, npr. urejevalnik besedil MS Office, hranijo začasne kopije podatkov. Nevarne pa so tudi ostale aplikacije, npr. iskalnik *Google Desktop*, ki zunaj DFS hranijo indekse z vsebine datotek shranjenih na DFS sistemu.

Fizični dostop in okolica sistema

- Kje se nahajajo varnostne kopije?
- Varnost/fizična varnost končnih naprav (terminalne opreme)!
- Nevarnost podtikanja prikritega mehanizma (npr. programske aplikacije ali strojnega dodatka), s katerim napadalec pridobi dostop do informacijskega sistema ali si ustvari možnosti za krajo gesel ali ključev (npr. prestrezniki tipkanja).
- Obnavljanje podatkov iz zavrženih pomnilniških komponent (trdi diski, tiskalniki, mobilni telefoni,...).
- Kraja (prenosnika, USB ključka,...)?
- Večuporabniška okolja – zaupamo ostalim uporabnikom?

Fizični dostop in okolica sistema

- Primer Scarfo:
  - agenti FBI so osumljencu januarja 1999 zasegli podatke, vendar so bili le-ti šifrirani;
  - maja 1999 so na njegov računalnik namestili programski prestreznik tipkanja in mu prestregli geslo.
- Primer aktivističnih organizacij Autistici in Inventati:
  - junija 2004 je italijanska policija začasno ugasnila strežnik ter iz njega prekopirala šifrirne ključe;
  - administratorji sistema so to odkrili šele leto dni po incidentu.

Fizični dostop in okolica sistema

- Primer Hushmail:
  - Kanadsko podjetje Hushmail je leta 1999 pričelo ponujati pošiljanje PGP/GPG šifrirane elektronske pošte preko spletnega vmesnika. Šifriranje je s pomočjo Java appleta potekalo na odjemalčevi strani.
  - Leta 2006 so zaradi večje enostavnosti ponudili možnost, da uporabniki uporabljajo šifriranje in dešifriranje na strežniški strani.
  - Novembra 2007 je podjetje ameriškim pravosodnim organom v okviru primera *U.S. v. Tyler Stumbo* izročilo dešifrirana elektronska sporočila kitajskega prodajalca steroidov.

Fizični dostop in okolica sistema

- Pregledi prenosnih računalnikov na mejah...
- Pregledovanje iPodov in računalnikov v okviru multilateralnega sporazuma o intelektualni lastnini...
- Mossad naj bi v Londonu na računalnik sirskega uradnika (bival je v hotelu) podtaknil zlonamerni program, s pomočjo katerega so uspeli ukrasti podatke o gradnji jedrskega reaktorja al-Kibar...

Fizični dostop in okolica sistema

- Nepazljiva uporaba programske opreme:
  - Vodstvo japonske jedrske elektrarne je svojemu pogodbenemu sodelavcu leta 2006 dovolilo, da je v njihovo interno omrežje vključil svoj prenosni računalnik. Na njem je imel nameščen program za razdeljevanje datotek preko P2P, zaradi česar so bili zaupni dokumenti kar nekaj časa na voljo celotnemu internetu.
  - Peter Ferrie v članku *Attacks on Virtual Machine Emulators*, 2007 opisuje znane napade na virtualne stroje VMware in VirtualPC ter emulatorje Bochs, Hydra, QEMU in Xen.

Fizični dostop in okolica sistema

- Podtikanje strojne opreme:
  - Konec leta 2003 se je zgodil vlom v poštno banko v Haifi v Izraelu. Ko je policija prišla na kraj dogodka, niso odkrili nič sumljivega, kljub temu pa je čez dober mesec na tej pošti iz bančnih računov nenadoma izginilo okrog 13.000 USD. Kasnejša preiskava je pokazala, da so vlomilci ob prvem vlomu v omrežje pošte podtaknili brezžično dostopno točko, preko katere so lahko nezakonito vstopili v sicer močno zaščiteno bančno omrežje.

Fizični dostop in okolica sistema

- Primer dostopa do mobilnega telefona
  - FBI je leta 2006 zaprosil za uporabo tim. klateške prisluškovalne naprave. Sodnik je uporabo odobril, ter dovolil namestitev prisluškovalne naprave v mobilni telefon. Najverjetneje je šlo za namestitev programske opreme preko mobilnega omrežja.

Tempest napad

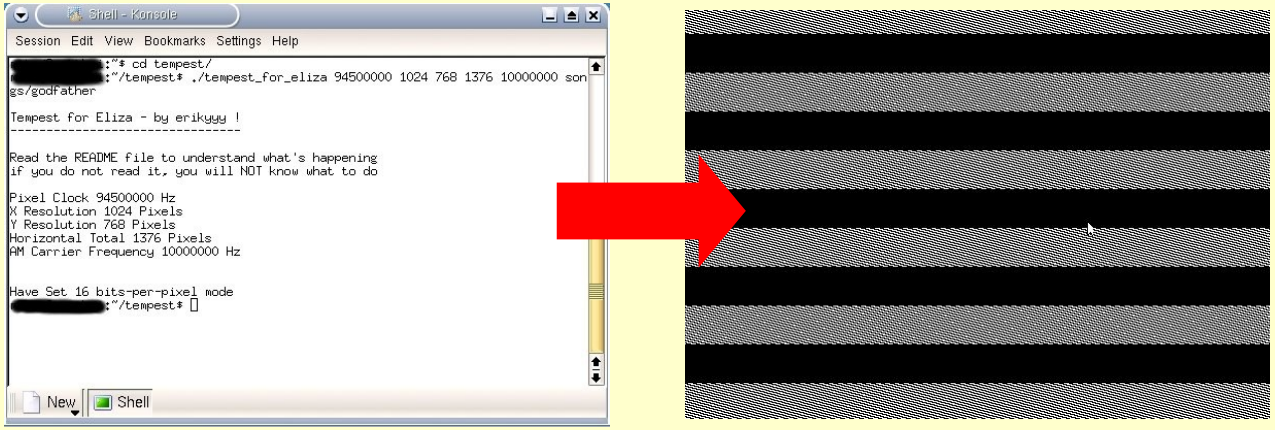
- Prvič naj bi bila tehnika uporabljena v 1950-tih letih, ko naj bi britanska tajna služba MI5 prisluškovala ambasadam Francije in tedanje Sovjetske zveze (Vir: Kuhn in Anderson, Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, 1998).
- Leta 1985 je Nizozemec Wim van Eck v članku "*Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*" tehniko podrobneje opisal in demonstriral obnavljanje slike s TV-zaslona iz oddaljenosti več sto metrov.

Tempest napad

- Prisluškovati je mogoče *kablom* (Peter Smulders, The Threat of Information Theft by Reception of Electromagnetic Radiation from RS232 Cables, 1990), *monitorjem* (Markus G. Kuhn, Optical Time-Domain Eavesdropping Risks of CRT Displays, 2002), *kontrolerju trdega diska*, itd.
- **Antipiratski virus!** (Kuhn in Anderson, Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, 1998)

Tempest napad na monitor

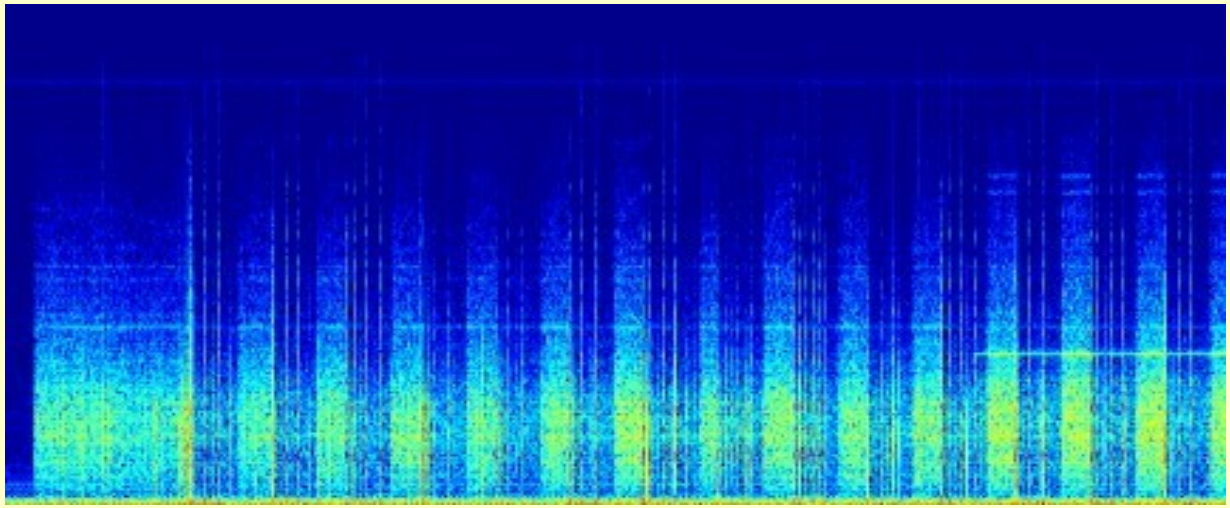
Vir: prosojnice Markusa G. Kuhna in Rossa J. Andersona "Soft Tempest: Hidden Data Transmission Using Elecromagnetic Emanations"



Tempest napad na monitor. [FILM]

Tempest napad na kontroler trdega diska

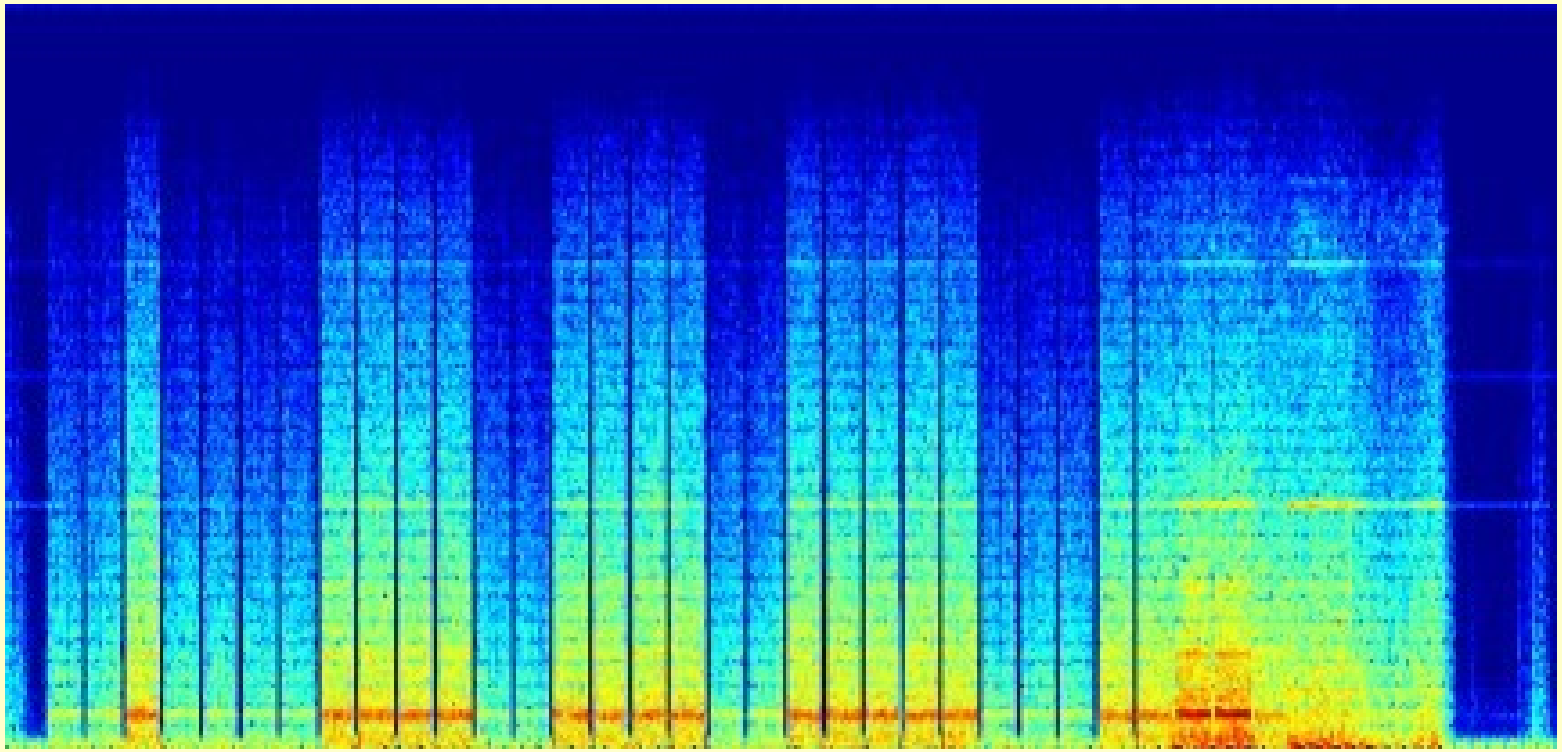
- Prestrezanje elektromagnetnih signalov kontrolerja trdega diska (tempest napad), za kar ni potreben fizičen ali mrežni stik z računalnikom.



Sonogram elekgromagnetnih signalov ob pisanju na trdi disk. Avtor je na podlagi spremljanja elektromagnetnih signalov lahko rekonstruiral kdaj se zapisujejo enke in kdaj ničle. Vir in avtorstvo: Oğuz Berke Durak, Hidden Data Transmission by Controlling Electromagnetic Emanations of Computers, <http://abaababa.ouvaton.org/tempest/>.

Tempest napad na RAM

Poslano: 00100001111001111001111100011001



Sprejeto: 00100001111001111001111100011110

Vir in avtorstvo: Oğuz Berke Durak, Hidden Data Transmission by Controlling Electromagnetic Emanations of Computers.

Tempest napad

- Tempest napad na volilne naprave na Nizozemskem, 2006

Vir in avtorstvo: Wels, Wessling, Gonggrijp in Németh, organizacija "*We don't trust voting computers*", <http://www.wijvertrouwenstemcomputersniet.nl/English>
Video na YouTube: <http://www.youtube.com/watch?v=B05wPomCjEY>. **[FILM]**

Napadi na programsko kodo

- Zaupanje programski opremi: odprtokodni in zaprtokodni.
- Avtentikacija programske opreme - digitalno podpisovanje programske opreme.
- Vsiljevanje programskih posodobitev?
- Avtentikacija skladišč programskih paketov v Linuxu.
- Primeri:
  - stranska vrata v BackOrifice;
  - stranska vrata v Linux rootkite;

Napadi na programsko kodo

- *packetstormsecurity.org: openssh-4.5p1_backdoored.tar.gz* (november 2006): Backdoored version of OpenSSH 4.5p1 that logs passwords to /var/tmp/sshbug.txt;
- *openssh-4.6p1-backdored.tar.gz* (april 2007): The backdoored version of OpenSSH 4.6p1. It logs passwords to /tmp/.sshell and also has the typical magic password;
- ...

Napadi na programsko kodo

- Hekeska skupina je vdrla v spletišče *SourceForge* in zamenjala izvorno kodo *sshd* s svojo različico, ki pa je imela nameščena "stranska vrata" (ang. *backdoor*).
- Ko je bila okužena različica *sshd* nameščena, je napadalcem poslala ICMP paket. Programska koda je vsebovala tudi rootkit, ki je skril podatke o tem, kam se pošlje ICMP paket.
- Eden izmed strežnikov, ki so namestili okuženo različico sshd-ja je bil tudi apache.org. Napadalci so tako preko modificiranega sshd demona leta 2001 uspešno vdrli v apache.org (vir: pogovor z napadalcem leta 2007).

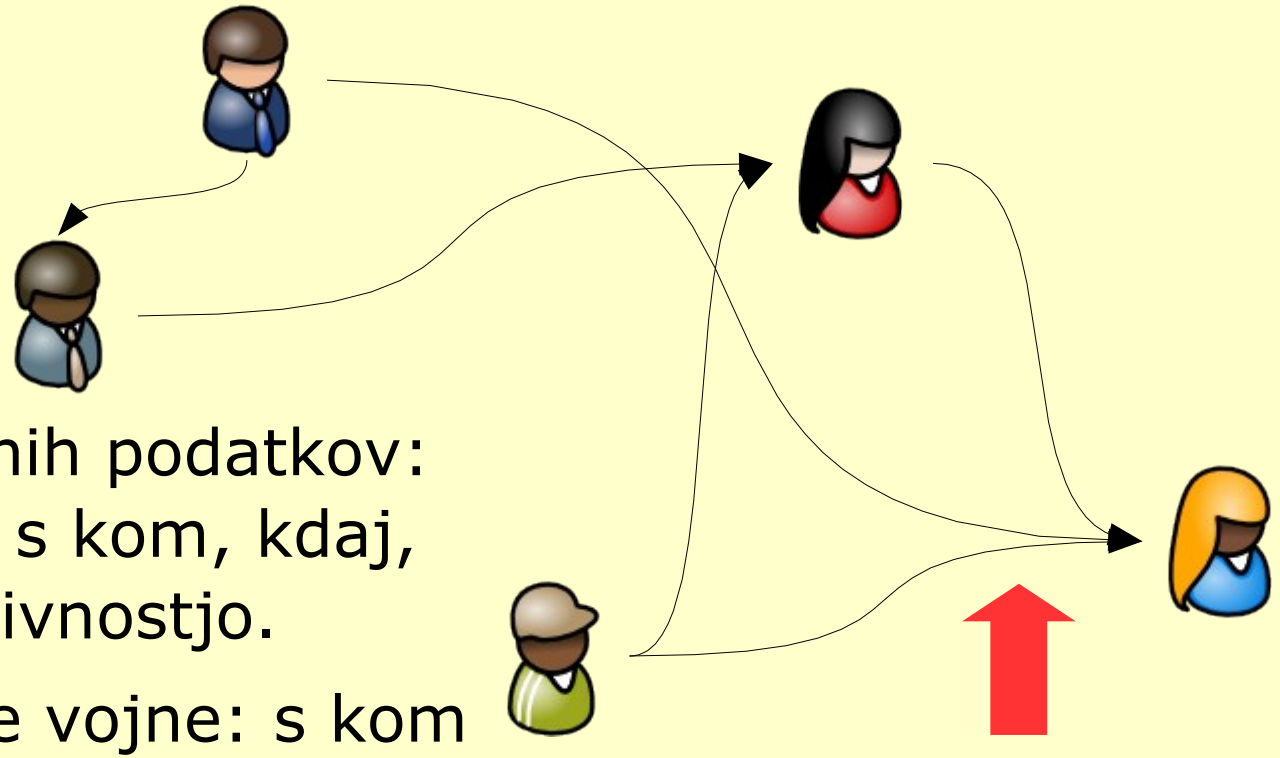
V: Posredni napadi (ang. *channel side*)

- Analiza prometa:
  - ugotavljanje centralne komunikacijske točke,
  - prestrezanje vsebine VOIP pogovorov z analizo prometa).
- MITM napadi
  - napad na DECT protokol (brezžična telefonija)
  - Pharming napadi,
  - napredni MITM napadi (Comodo CA, napad na BGP,...).

Vir: Schneier.com, <http://www.schneier.com/blog/archives/2009/07/information_lea_1.html>.

Pri 4-mestnem geslu je vseh možnih kombinacij 10.000. V zgornjem primeru je možnih kombinacij samo še 24. Levo geslo je najbolj verjetno 1986 ali 1968, desno pa 1234.

Analiza prometa

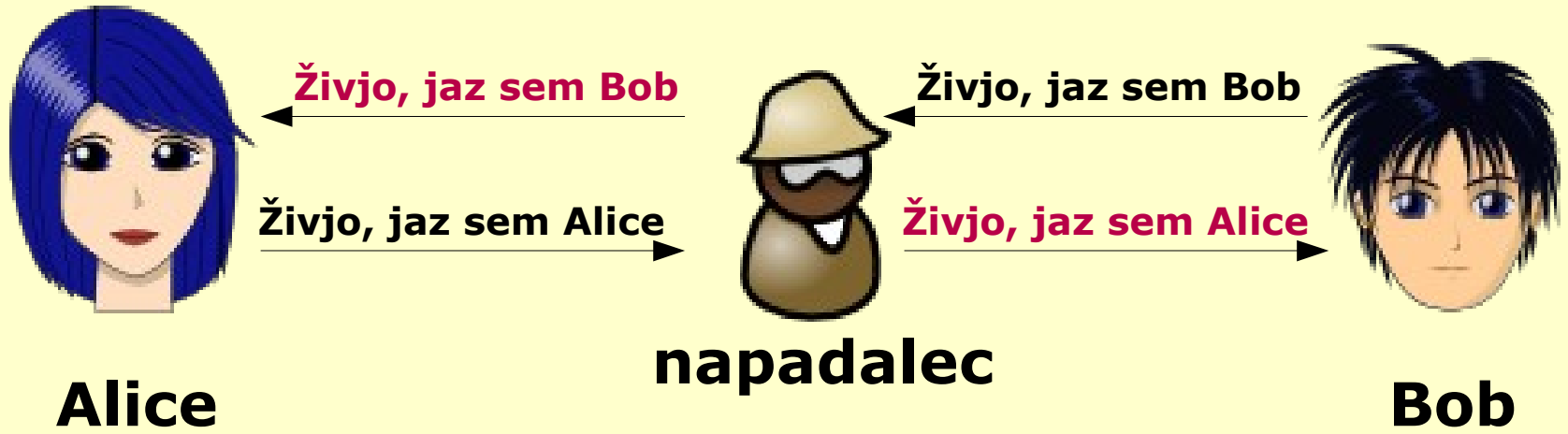


- Analiza prometnih podatkov: kdo komunicira s kom, kdaj, s kakšno intenzivnostjo.
- Primer iz hladne vojne: s kom komunicirajo vojaški radarji ko pride do kršitve zračnega prostora? Kje so locirane sovražne enote?
- Deluje tudi kadar je vsebina komunikacije šifrirana.

Analiza prometa

- Primer iz VoIP telefonije:
  - Junija 2008 je skupina raziskovalcev iz ameriške John Hopkins University je pokazala, da je mogoče z merjenjem dolžine paketkov VoIP komunikacije, ki uporablja variabilno kompresijo (ang. *variable bitrate compression*) brez dekodiranja in dešifriranja ugotoviti vsebino zvočne komunikacije pri VoIP povezavi.
  - V raziskavi so uspeli pravilno identificirati okrog 50% besed v pogovoru, pri čemer je odstotek prepoznanih besed za bolj zapletene besede bistveno višji - okrog 90%.

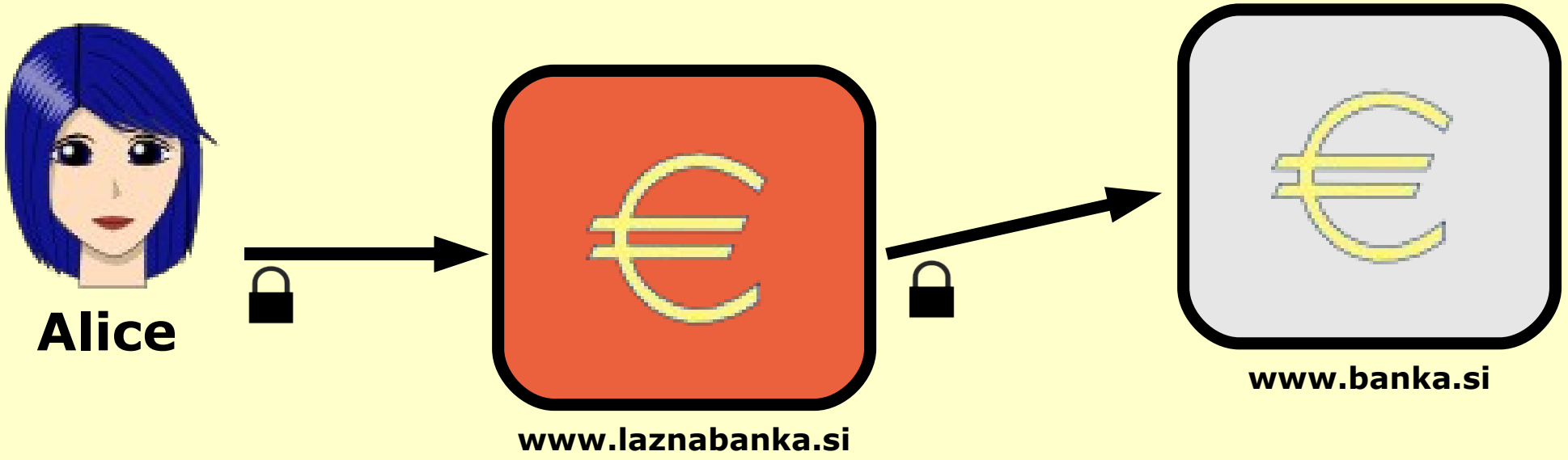
Napad s posrednikom (MITM - man-in-the-middle)



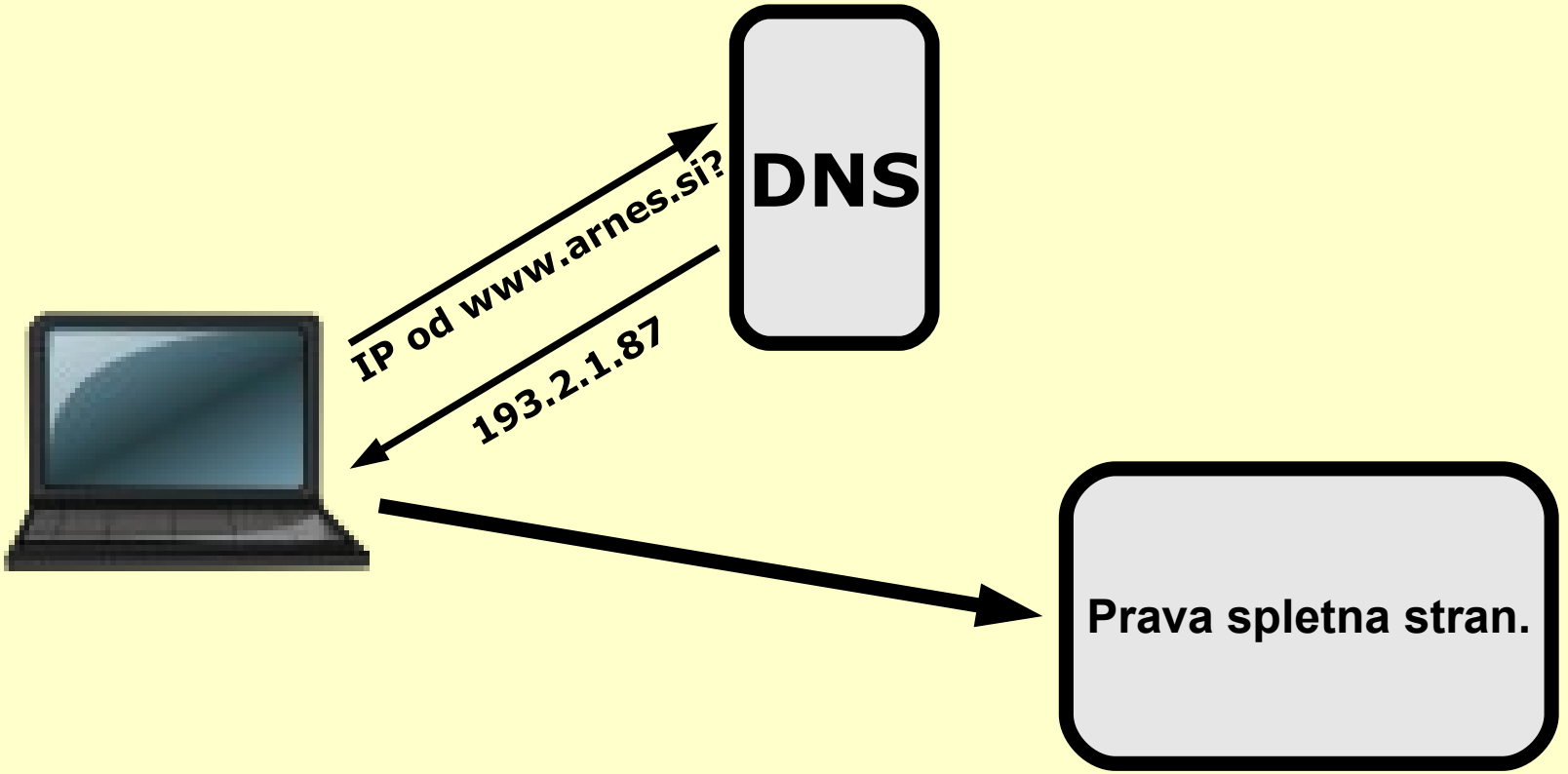
Napad s posrednikom (MITM - man-in-the-middle)

- Mogoč, kjer se komunikacijski točni ne avtenticirata med seboj oz. se avtenticirata z neustreznimi mehanizmi (npr. IP naslovom ali kakšnim drugim podatkom, ki ga je mogoče ponarediti).
- Primeri:
  - Kevin Mitnick in kraja identitete;
  - MITM na gverilsko organizacijo FARC;
  - Yahoo mail phishing;
  - DNS pharming / DNS poisoning;
  - MITM napad na GMail. [FILM]

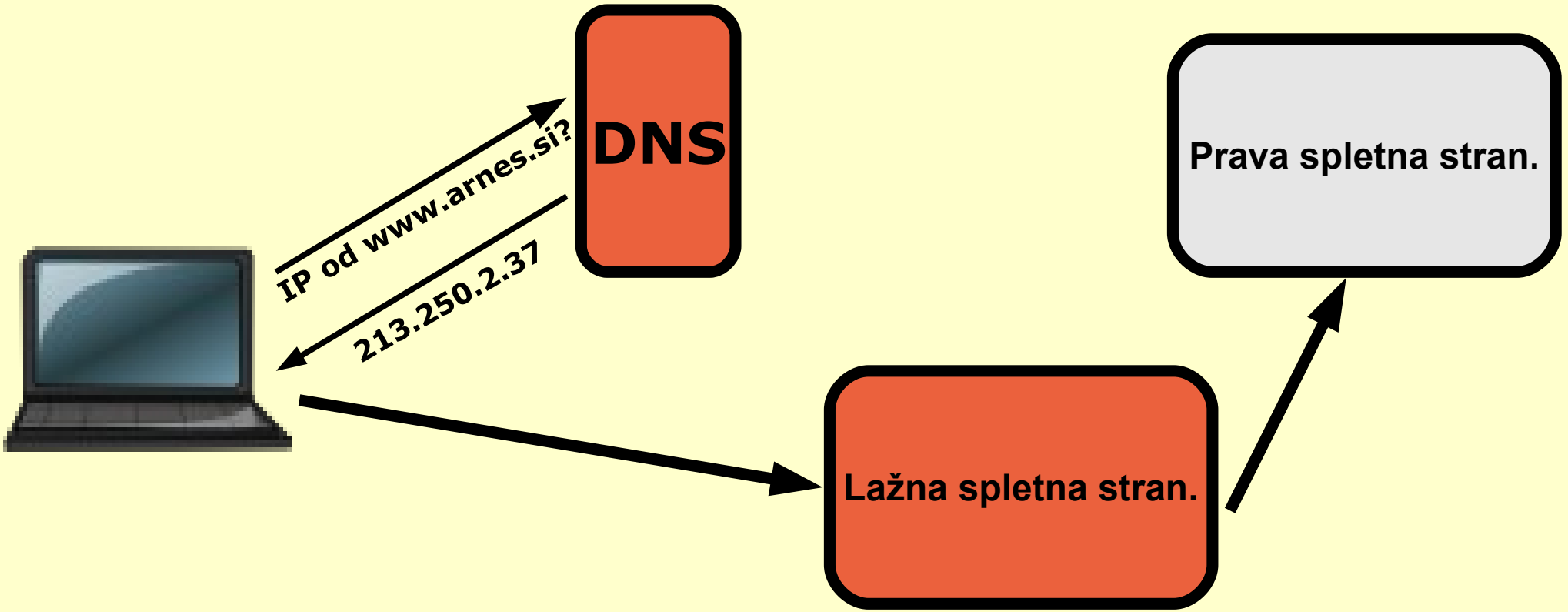
Napad s posrednikom (MITM - man-in-the-middle)



Napad s posrednikom (MITM - man-in-the-middle)



Napad s posrednikom (MITM - man-in-the-middle)



Napad na DECT protokol

- DECT je protokol, ki se uporablja za zaščito brezžičnih komunikacij pred prisluškovanjem. Uporablja se pri domačih brezžičnih telefonih, pri otroških telefonih (baby phone), sistemih za odpiranje vrat, klicih v sili, brezžičnih čitalcih bančnih kartic, itd..
- Leta 2008 so raziskovalci ugotovili, da je DECT mogoče razbiti s pomočjo navadnega računalnika z operacijskim sistemom Linux ter kartico *ComOnAir*.

Vir in avtorstvo: dedected.org

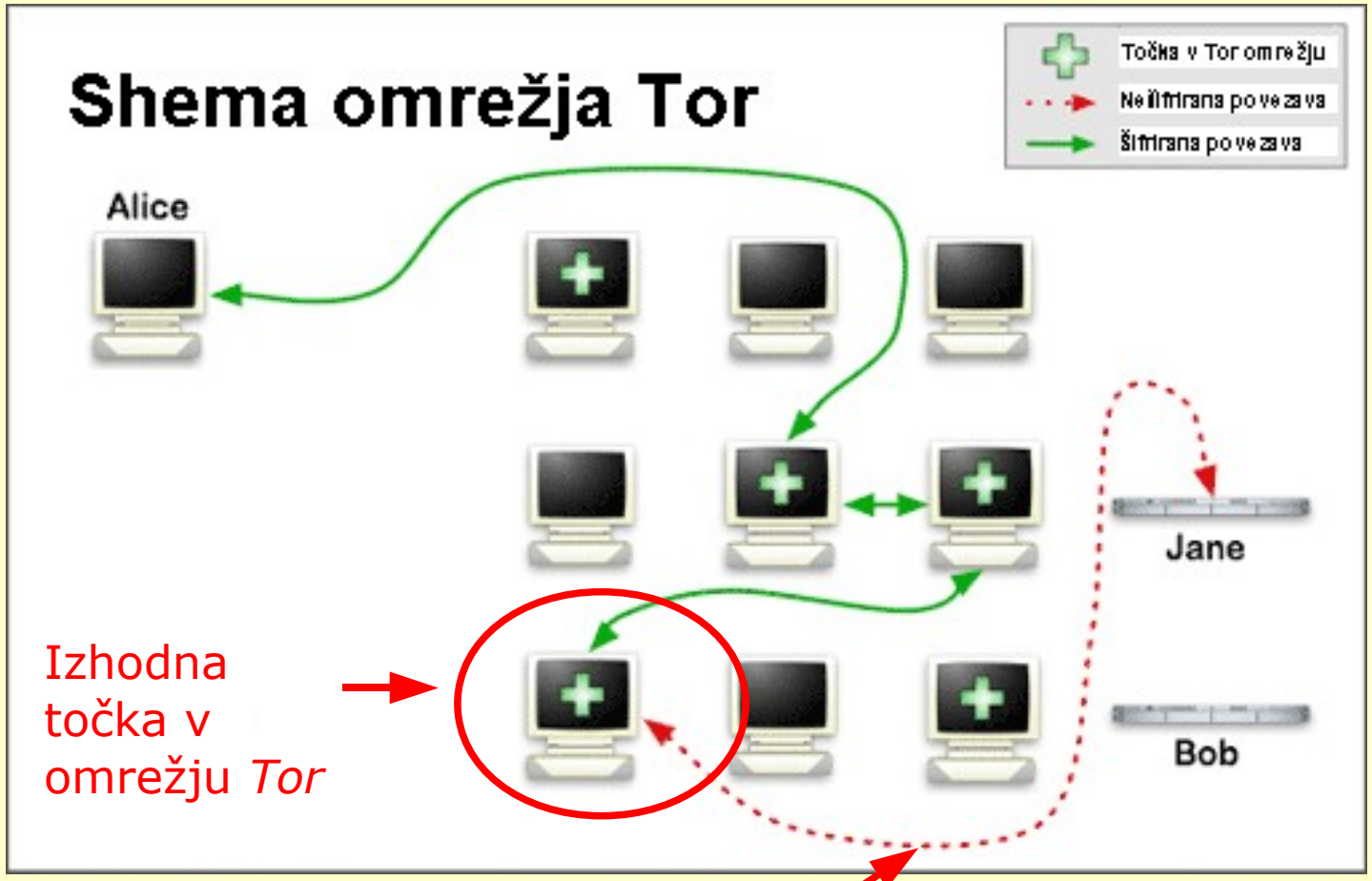
MITM napad na anonimizacijska omrežja

"At a 1996 conference here at Harvard indeed two speakers who worked for and/or closely with the US government said "on the record" that government agencies not just in the US but elsewhere as well run large remailers / anonymizers around the world. ... The statement was made in public and I explicitly asked whether it was "on the record", to which they said yes.

Later they publicly stated that the exchange never happened and the statement was never made, but an official transcript of the Harvard conference vindicates my version. They also mentioned in response to a question on code breaking capabilities by the US government that they themselves would use at least 1024 bit long public key encryption to safeguard their own personal emails."

-- harvardski profesor Viktor Mayer-Schoenberger o nadzoru anonimizacijskih sistemov (oktober 2006).

MITM napad na anonimizacijskem omrežju Tor



"End-to-end" šifriranje ni v uporabi!

Primeri:

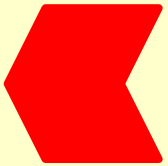
- tor.unixgu.ru, leta 2006.
- Snakes-on-a-Tor, avgusta 2006.
- Dan Egerstad in kraja gesel ambasade, leta 2007.

Varnost pred MITM: varnostni mehanizmi v SSH

- matthai@cryptobox:~$ ssh matthai@www.secret-service.si
- The authenticity of host 'www.secret-service.si (193.XXX.XXX.XXX)' can't be established.
  RSA key fingerprint is 1d:67:eb:42:08:92:11:22:11:7a:a0:de:79:49:6f:a6.
  Are you sure you want to continue connecting (yes/no)?

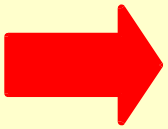
Smo preverili pristnost SSH ključa?

- *yes*
- Warning: Permanently added 'www.secret-service.si' (RSA) to the list of known hosts.



Bomo datoteko ~/.ssh/known_hosts ustrezno varovali?

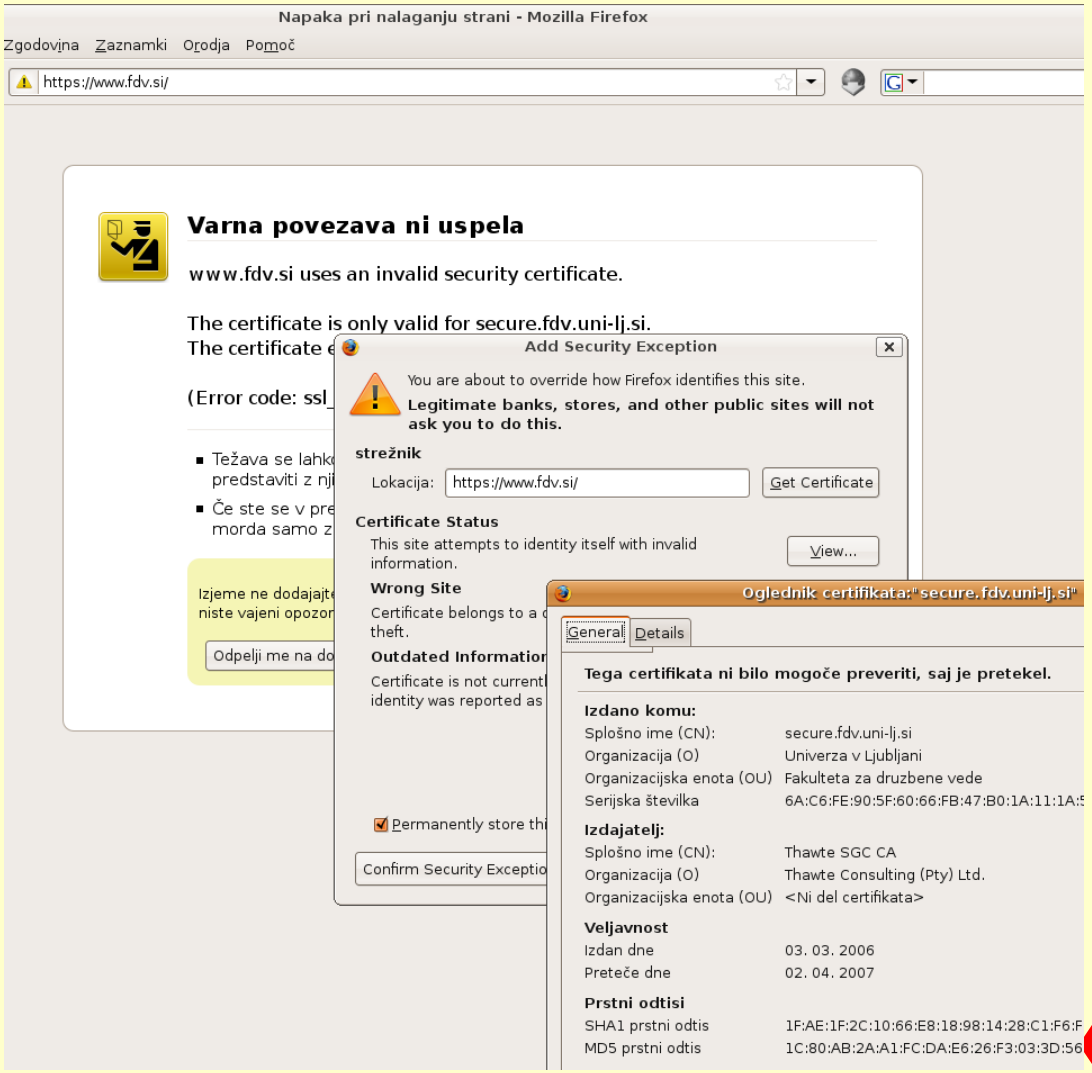
- matthai@www.secret-service.si's password:



Smo vnesli pravo geslo?

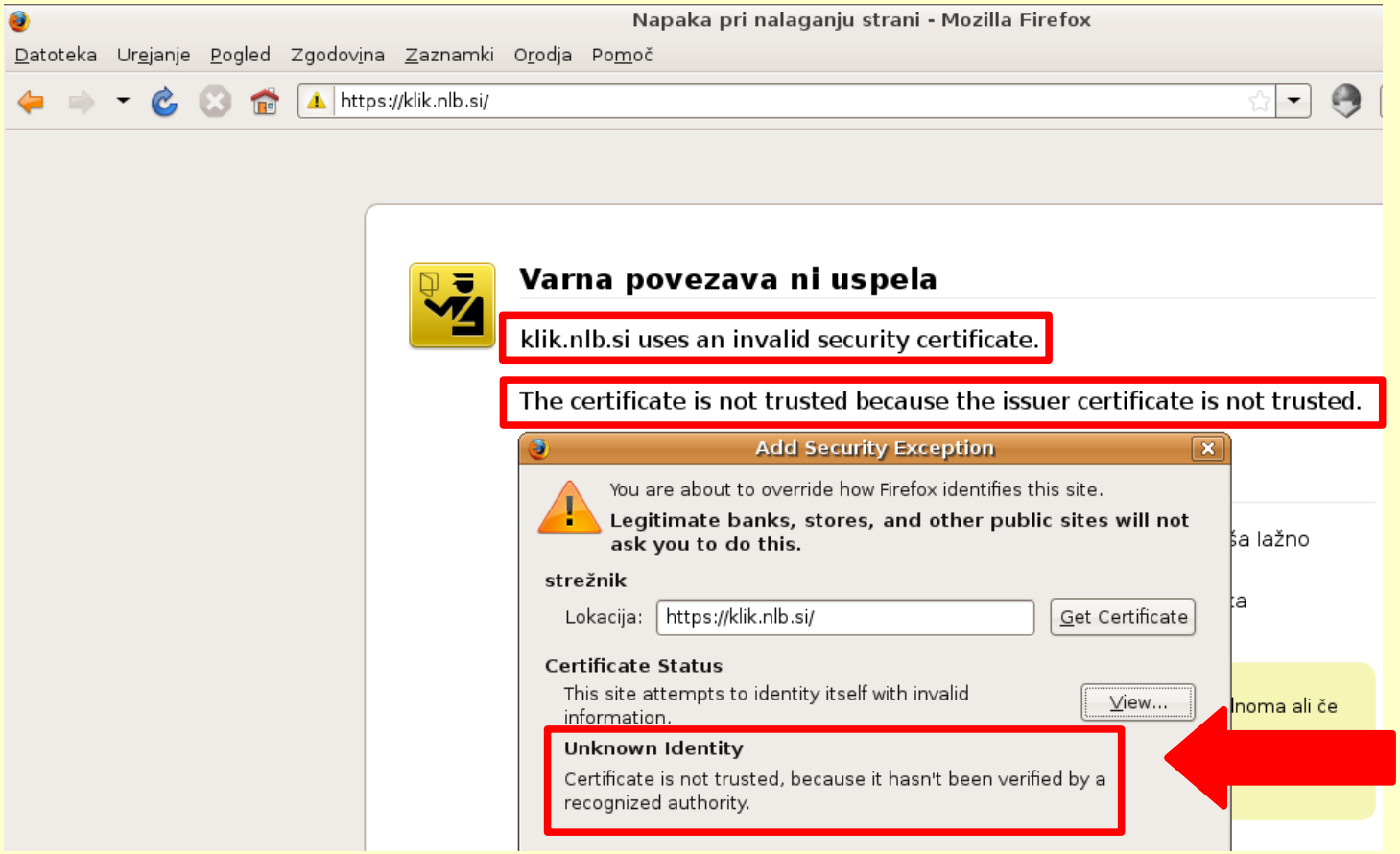
- matthai@secretservice:~$

Varnost pred MITM: varnostni mehanizmi v https



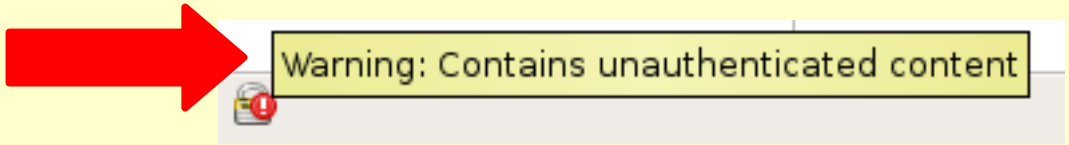
Je certifikat podpisan s strani CA oz. smo ga sami preverili, je potekel, je izdan za pravo domeno?

Varnost pred MITM: varnostni mehanizmi v https



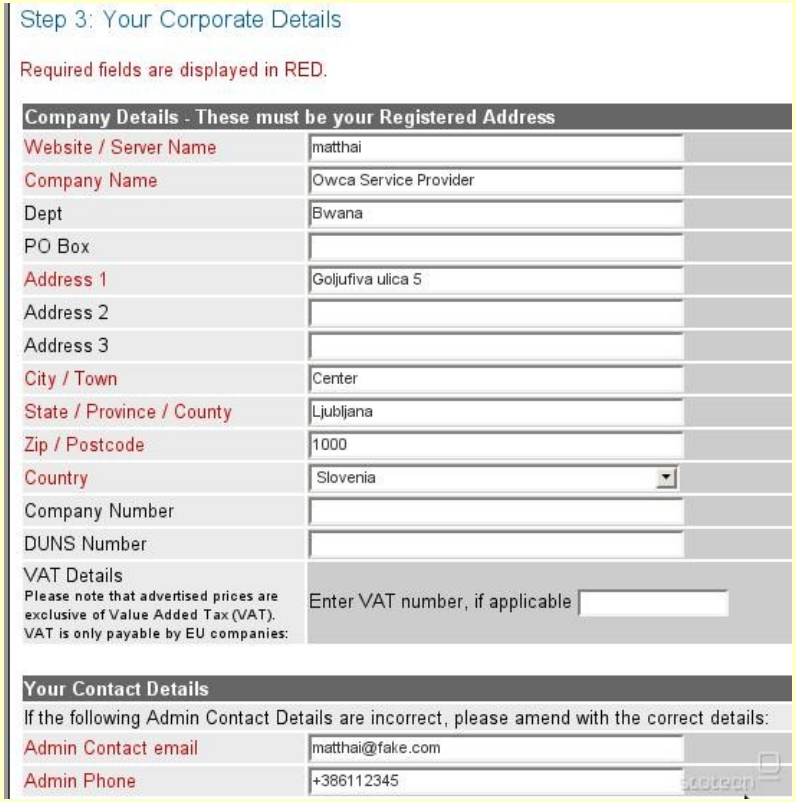
Certifikat je samopodpisan!

Firefox prikaže ustrezno obvestilo



Napredni MITM napadi

- Decembra 2008 je skupina sedmih raziskovalcev pokazala, da je z iskanjem MD5 kolizij mogoče izdelati ponarejen CA certifikat.
- Začasni certifikati "zaupanja vrednih" izdajateljev (Comodo): napadalec zgenerira lažno CRS (Certificate Request) datoteko, vsebino datoteke preko spletne strani pošlje izdajatelju certifikatov *Comodo* nakar dobi brezplačni 90-dnevni certifikat.
- Napad na Border Gateway Protocol...
- Rešitev: Pet Name Tool.



Step 3: Your Corporate Details

Required fields are displayed in RED.

Company Details - These must be your Registered Address	
Website / Server Name	matthai
Company Name	Owca Service Provider
Dept	Bwana
PO Box	
Address 1	Goljufiva ulica 5
Address 2	
Address 3	
City / Town	Center
State / Province / County	Ljubljana
Zip / Postcode	1000
Country	Slovenia
Company Number	
DUNS Number	
VAT Details Please note that advertised prices are exclusive of Value Added Tax (VAT). VAT is only payable by EU companies:	Enter VAT number, if applicable

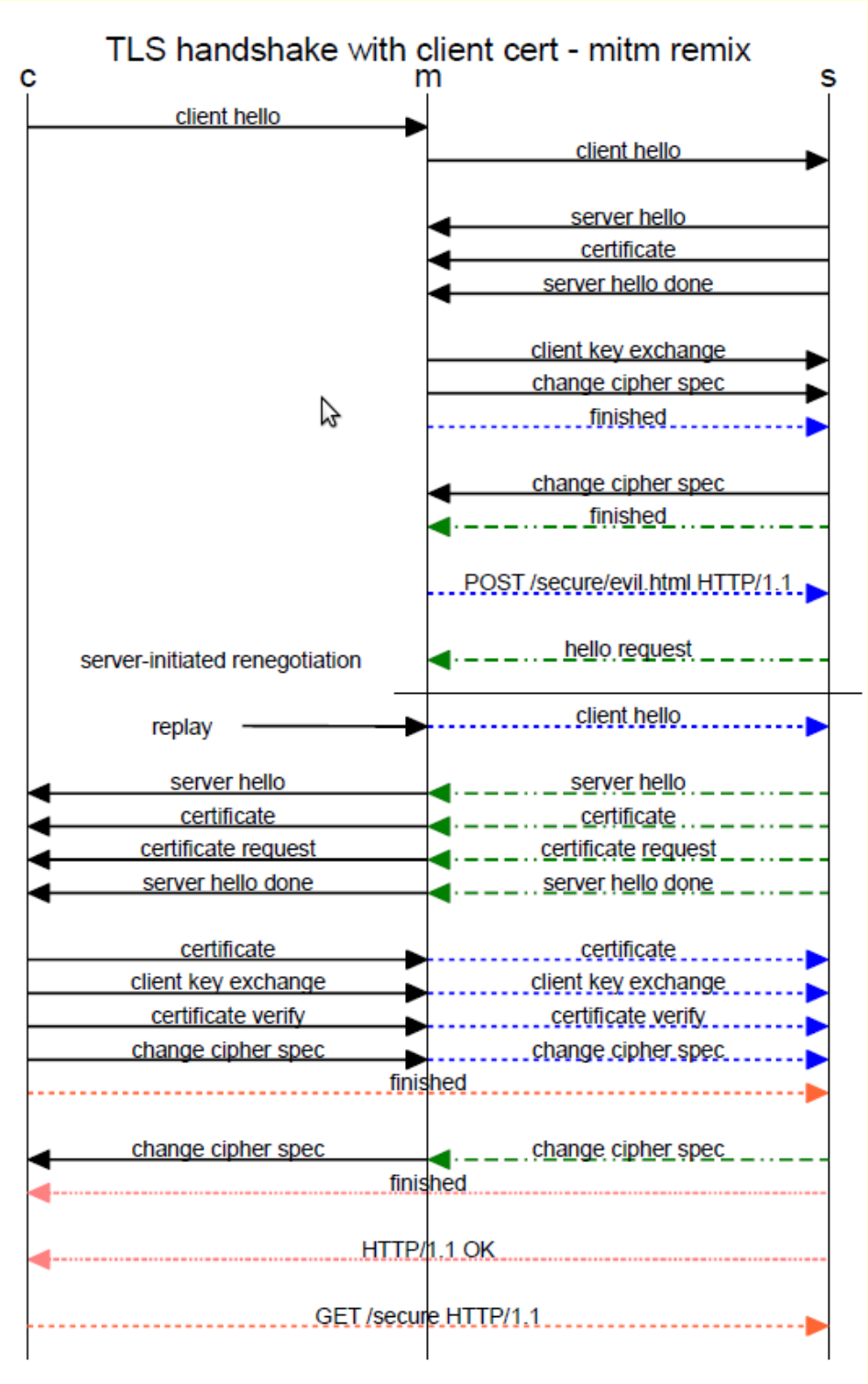
Your Contact Details	
If the following Admin Contact Details are incorrect, please amend with the correct details:	
Admin Contact email	matthai@fake.com
Admin Phone	+386112345

Napredni MITM napadi

- Napad z ničelno predpono na SSL/TLS certifikate (ang. *null prefix attack*): www.banka.si\0zlonamernastran.si; *\0zlonamernastran.si.
- Mozilla NSS, Microsoft CryptoAPI, GnuTLS: Firefox, Internet Explorer, Chrome, Thunderbird, Outlook, Evolution, Pidgin, AIM,...
- Plus - ranljivost v protokolu OCSP (*Online Certificate Status Protocol*), zaradi katere je ponarejene certifikate z ničelno predpono izredno težko preklicati.
- SSLsniff.

SSL/TLS ranljivost v “renegotiation phase”

- SSL 3.0+ in TLS 1.0+ ranljivost, ki izkorišča napako v "pogajalskem procesu" protokola (tim. *renegotiation phase*), omogoča pa napade s posrednikom (tim. MITM napade) oziroma napade na HTTPS seje podpisane s certifikatom odjemalca.
- Napadalec odpre povezavo do SSL strežnika, pošlje nekaj podatkov, zahteva ponovno pogajanje in SSL strežniku prične pošiljati podatke, ki prihajajo od žrtve. Spletni strežniki (IIS in Apache) podatke, ki so prišli od napadalca in podatke, ki so prišli od žrtve nato povežejo, posledica česar je, da napadalec lahko SSL strežniku pošlje poljuben zahtevek, ki ga nato avtenticira njegova žrtev.



http://extendedsubset.com/Renegotiating_TLS_pd.pdf
Marsh Ray in Steve Dispensa. 2009. Renegotiating TLS, <http://extendedsubset.com/Renegotiating_TLS.pdf>

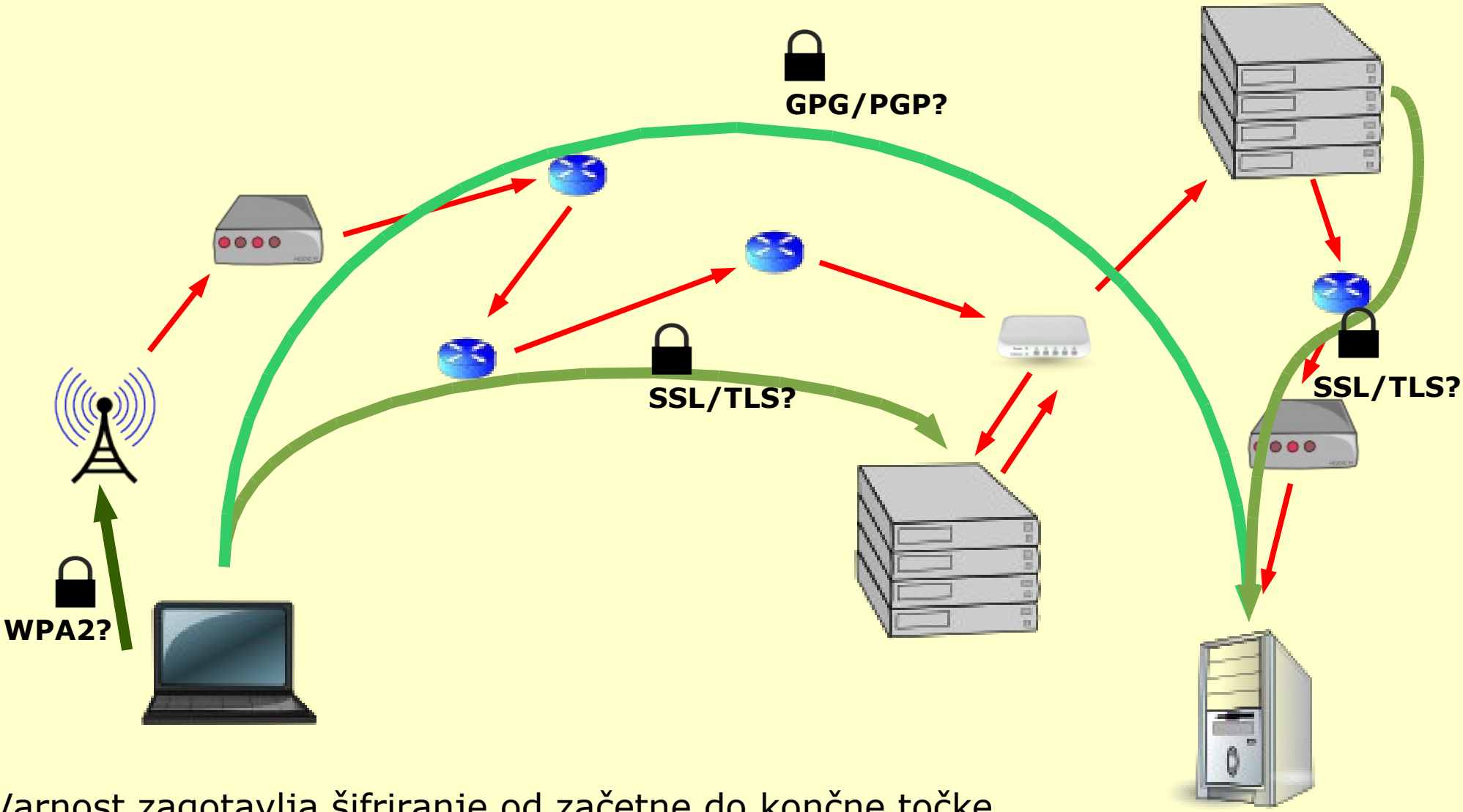
SSL/TLS ranljivost v "renegotiation phase"

- Ranljivost v protokolih torej omogoča, da napadalec v začetek podatkovnega toka aplikacije (v HTTPS seji) vrine poljuben niz nešifriranih podatkov. To mu omogoča izvedbo poljubne HTTP transakcije, žrtvi lahko prikaže poljubno vsebino v HTTPS seji ali pa njegov certifikat uporabi za povezovanje do poljubnega strežnika (in s tem izvede klasičen napad s posrednikom).
- GET /path/to/resource.jsp HTTP/1.0
- Dummy-Header: GET /index.jsp HTTP/1.0
- Cookie: sessionCookie=Token

Začetna in končna točka šifriranja?

- Kaj je končna točka?
  - prejemnik ali internetni strežnik?
- Ali končna točka lahko razkrije podatke/šifrirne ključe (npr. v sodnem postopku)?
- Danes se kriptografija uporablja predvsem v sferi elektronskega poslovanja in za zaščito avtorskih pravic.
- Za zaščito komunikacij posameznikov se množično uporablja le šifriranje povezav znotraj zaprtega omrežja (GSM <-> bazna postaja, uporabnik <–> bančni strežnik/poštni strežnik), kar **ne** onemogoča prestrezanja na izhodu sistema.

"End-to-end" šifriranje



Varnost zagotavlja šifriranje od začetne do končne točke
in vzajemna avtentikacija obeh točk. **Kaj je končna točka (*endpoint*)?**

V: Posredni napadi (ang. *channel side*)

- Napadi na generatorje naključnih števil
  - Windows (Dual_EC_DRBG), Linux
  - napadi na virtualne stroje.

Napadi na generatorje naključnih števil

- Varnost šifrirnih sistemov je odvisna tudi od posebnih skritih podatkov, ki so znani samo pooblaščenim osebam, ostali pa jih ne morejo predvideti. Te podatke sodobni šifrirni sistemi pridobijo z randomizacijo – z generiranjem naključnih števil.
- Povsem naključna števila je na običajni strojni opremi težko zgenerirati, zato se namesto generatorjev naključnih števil (RNG) pogosto uporabljajo generatorji psevdonaključnih števil (PRNG).

Napadi na generatorje naključnih števil

- V primeru, da napadalec uspe zmanipulirati proces generiranja naključnih števil tako, da le-ta zanj postane predvidljiv, lahko varnost šifrirnih sistemov popolnoma pade.
- Primeri:
  - Raziskava Dorrendorfa, Guttermana in Pinkasa iz novembra 2007 je pokazala, da generator naključnih števil v Windows 2000 (uporablja se za generiranje SSL ključev) ni varen. Analiza je pokazala, da je mogoče z razmeroma preprostimi napadi predvideti prihodnje "naključne" vrednosti in s tem uganiti npr. SSL šifrirne ključe.

Napadi na generatorje naključnih števil

- Raziskava Guttermana, Pinkasa in Reinmana iz marca 2006 je pokazala tudi pomanjkljivosti v generatorju naključnih števil v operacijskem sistemu Linux (predvsem v *OpenWRT*).
- Maja 2008 so odkrili resno varnostno pomanjkljivost v naključnem generatorju števil distribucije Debian (in izvedenk, npr. Ubuntu,...). Kompromitirani so bili kriptografski ključi za SSH, OpenVPN, DSNSEC, SSL/TLS, ključi uporabljeni v X.509 certifikatih ter DSA ključi uporabljeni za podpisovanje in avtentikacijo.

Napadi na generatorje naključnih števil

- Leta 1996 in 1997 sta raziskovalca Adam Young in Moti Yung predstavila idejo o **kleptografiji** oz. kriptovirologiji. Gre za tim. SETUP napad (*secretly embedded trapdoor with universal protection*), ki s pomočjo prirejenega algoritma zgenerira tak par šifrirnih ključev, da je na videz (matematično) povsem enak kakor navaden par ključev.
- Par ključev je tudi enako varen, razen pred napadalcem, saj tajno vključena stranska vrata predstavljajo napadalčev javni ključ. SETUP napad tako napadalcu daje ekskluzivno prednost.
- Napad je mogoče implementirati v RSA, DSA ter Diffie-Hellmanovo izmenjavo ključev.

Napadi na generatorje naključnih števil

- Ameriški National Institute of Standards and Technology je leta 2007 pripravil nov standard za generiranje naključnih števil. Pripravili so štiri standardizirane tehnike oz. algoritme, med katerimi je eden Dual_EC_DRBG.
- Leta 2007 sta Shumow in Ferguson iz Microsofta ugotovila, da algoritem uporablja konstante za definiranje eliptične krivulje, ki pa so povezane z nekim naborom skritih številk. Kdor pozna, ali bi poznal te številke, bi lahko s pomočjo poznavanja prvih 32 naključno generiranih znakov algoritma Dual_EC_DRBG uganil vse naslednje "naključno" generirane znake.

Napadi na generatorje naključnih števil

- V Dual_EC_DRBG, ki je eden izmed standardiziranih generatorjev naključnih števil je morda vrinjen "tajni ključ" napadalca, saj konstante morda predstavljajo javni ključ napadalca, skrito število pa predstavlja napadalčev tajni ključ, kar napadalcu omogoči uspešen napad na sam algoritem.
- S tem bi bilo mogoče razmeroma enostavno razbiti praktično vsak kriptografski algoritem, ki bi temeljil na generatorju naključnih števil Dual_EC_DRBG.

PRNG v virtualnih strojih

- Virtualni stroji pogosto nimajo dovolj dostopa do naključnih generatorjev števil oz. jim primanjkuje entropije.
- Zato so šifrirni ključi generirani na teh strojih veliko bolj ranljivi od šifrirnih ključev na fizičnih strojih.

V: Posredni napadi (ang. *channel side*)

- Primeri klasičnih posrednih napadov.
  - Strojni korenski kompleti (ang. *rootkit*):
    - napadi na hipervizorje,
    - napadi na NIC,
    - akustična kriptoanaliza,
    - Ring -3 rootkit,
    - Illinois Malicious Processor.
  - DMA preko firewire/USB.
  - Cold boot napad.

Primeri klasičnih “side channel” napadov

- Side channel napad je napad na fizično implementacijo šifrirnega sistema in ne na teoretično slabost šifrirnega algoritma. Primeri:
  - časovni napad (ang. *timing attack*): tehnika na podlagi merjenja časa, ki ga naprava porabi za procesiranje, omogoča napadalcu razkritje delovanja.
  - analiza električne aktivnosti (ang. *differential power analysis*), ki so jo opisali Kocher, Jaffe in Jun: na podlagi opazovanja električne aktivnosti naprave je mogoče ugotoviti nekatere skrite informacije (npr. onemogočiti zaklep pametne kartice ob vnosu napačne PIN kode);

Primeri klasičnih "side channel" napadov

- merjenje svetlobe monitorja (tim. *visible light attack*): opisal Markus G. Kuhn leta 2002 v članku *Optical Time-Domain Eavesdropping Risks of CRT Displays* (http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf)
- uhajanje elektromagnetnih signalov (tempest napad)
- akustična kriptoanaliza (ang. *acoustic cryptanalysis*),
- ...

Akustična kriptoanaliza

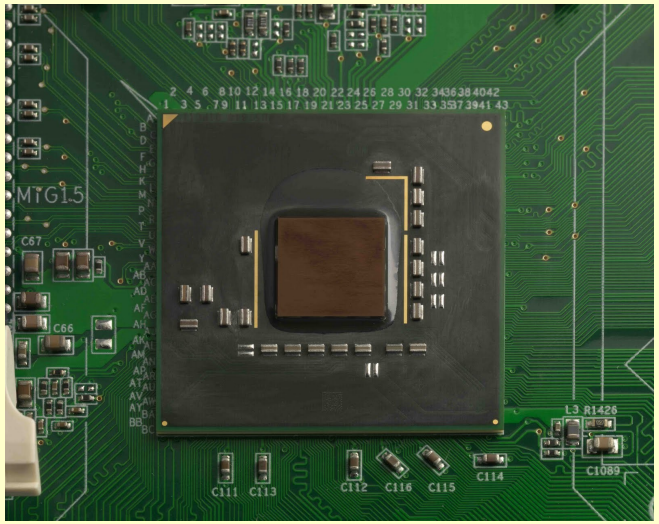
- Peter Wright v knjigi Spycatcher opisuje kako je britanska tajna služba MI5 je v času sueške krize v 50-tih letih prejšnjega stoletja (operacija ENGULF) s pomočjo prisluškovanja telefonom egiptovski ambasadi uspela ukrasti geslo šifrirnega stroja Enigma.
- Leta 2004 sta Adi Shamir in Eran Tromer odkrila, da je s snemanjem zvoka, ki ga oddaja računalnik mogoče ugotoviti kaj počne računalnik: ali je procesor aktiven ali pa je v prostem teku, različne vzorce procesorskih operacij in dostopov do pomnilnika v nekaterih primerih pa tudi RSA tajne ključe.

Hipervizorski korenski kompleti (Ring -1)

- Nitin in Vipin Kumar iz NVlabs, sta na konferenci Black Hat Europe 2007 v Amsterdamu predstavila Vboot Kit.
  - Gre za poseben zagonski nalagalnik (ang. *boot loader*), ki se zažene iz CD-ja, se naloži v pomnilnik ter nato naloži operacijski sistem Windows Vista. Pred tem prestreže interrupt 13, ki omogoča dostop do diskovnih pogonov.
- Hardware-Assisted Virtual Machine (HVM) Rootkits:, Dino Dai Zovi (*Vitriol* za Intel VT), Joanna Rutkowska (*Blue Pill Project*, za AMD-V), Michael Myers in Stephen Youndt,...

SMM korenski kompleti (Ring -2)

- Ring -2: System Management Mode (SMM) je najbolj privilegiran način delovanja procesorja na x86/x86_64 arhitekturah.
- Ring -3: napad na vPro/AMT čipe.



Slika Q35 čipa (MCH) v katerega so namestili korenski komplet.

Vir in avtorstvo: Joanna Rutkowska, <http://theinvisiblethings.blogspot.com/2009/08/vegas-toys-part-i-ring-3-tools.html>

Zlonamerna strojna oprema

- John Heasman, 2006, Implementing and Detecting a PCI Rootkit.
- King, Tucek, Cozzie, Grier, Jiang in Zhou, 2008, *Designing and implementing malicious hardware*:
  - z virusom RavMonE okuženi iPodi leta 2006,
  - Seagatovi trdi diski z "prednaloženimi" trojanci, leta 2007,
  - leta 1982 je CIA Sovjetski zvezi podtaknila modificirano strojno programsko opremo za nadzor plinovodov, ki je onesposobila sovjetske naftovode,

Zlonamerna strojna oprema

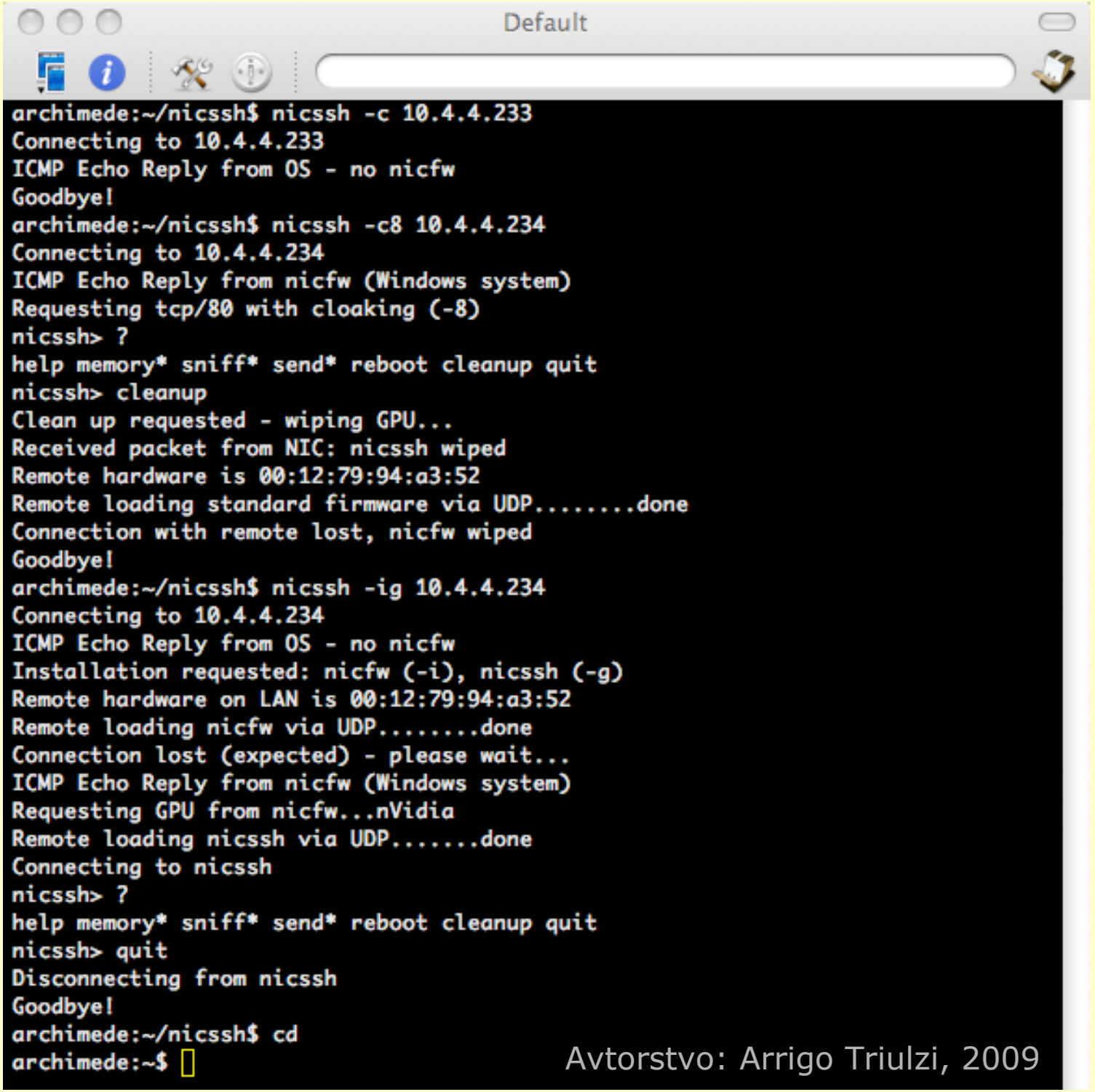
  - modificirani pisalni stroji, ki jih je KGB podtaknila ameriški ambasadi v Moskvi ter nato prestrezala vse, kar so Američani natipkali.
  - ...
- Raziskovalci so razvili procesor z imenom *Illinois Malicious Processor* (IMP), ki vsebuje spremenjen mehanizem za dostop do pomnilnika ter mehanizem, ki omogoča zaganjanje zlonamerne strojne programske opreme (tim. *firmware*).

Zlonamerna strojna oprema

- Procesor omogoča implementacijo eskalacije privilegijev, implementacijo stranskih vrat, skozi katera napadalec pridobi popoln dostop do računalnika brez vpisa ustreznega gesla ter implementacijo servisa, ki krade gesla in jih pošilja napadalcu.

Napadi na mrežno opremo

- Psyb0t (avtomatizirani napadi na Linux usmerjevalnike na MIPS arhitekturi).
- Phenoelitova raziskava o varnosti Ciscotovega operacijskega sistema IOS: s pomočjo enega paketka, ki ga pošljejo usmerjevalniku, prevzamejo kontrolo nad le-tem.
- Korenski komplet na mrežni kartici (Triulzi, 2008).



Zlonamerna strojna oprema

- Procesor omogoča implementacijo eskalacije privilegijev, implementacijo stranskih vrat, skozi katera napadalec pridobi popoln dostop do računalnika brez vpisa ustreznega gesla ter implementacijo servisa, ki krade gesla in jih pošilja napadalcu.

Branje vsebine monitorja iz odboja s pomočjo teleskopa

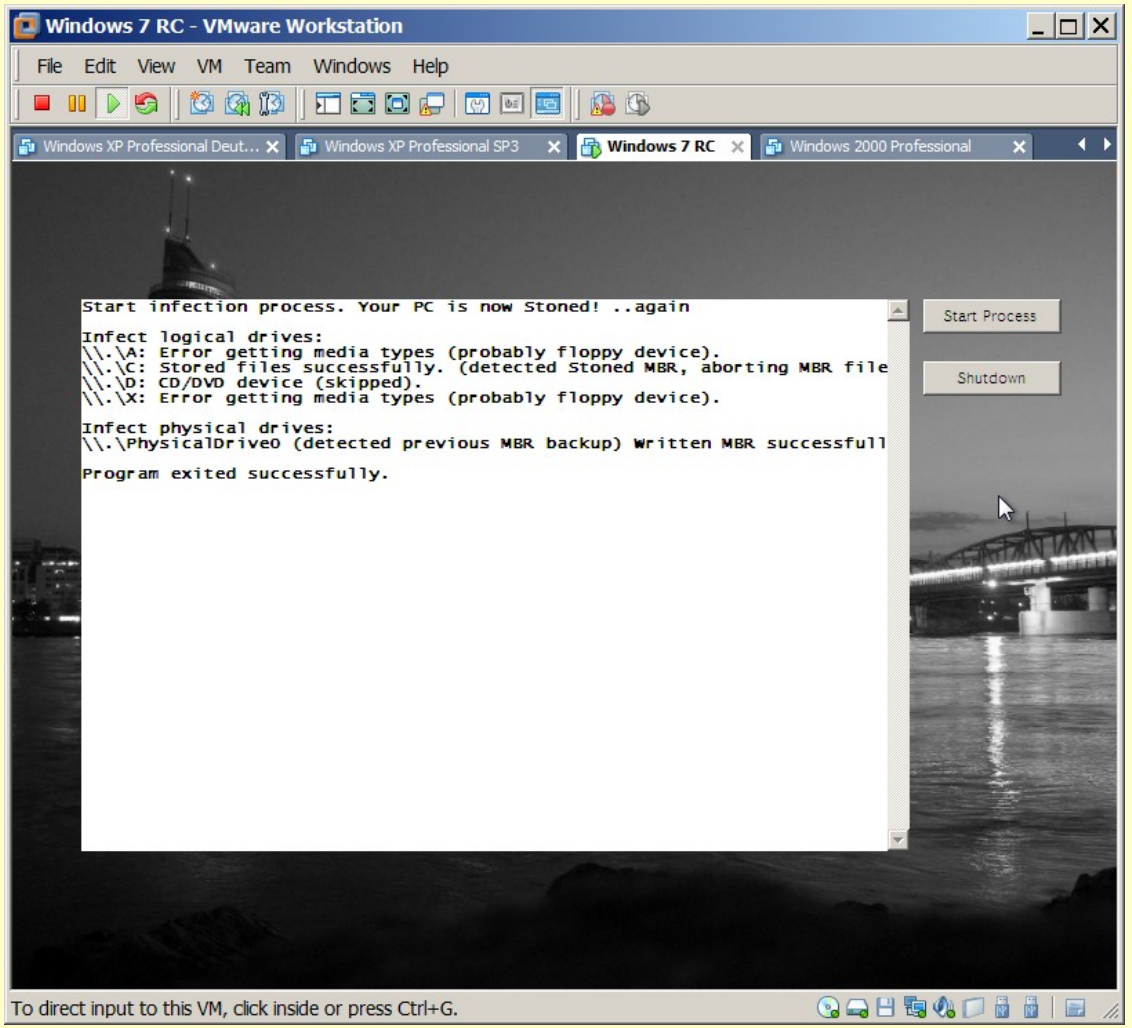
- Raziskovalci Backes, Dürmuth in Unruh so leta 2008 v članku *Compromising Reflections or How to Read LCD Monitors Around the Corner* opisali raziskavo, v okviru katere so s teleskopom prebrali vsebino monitorja iz odbleska svetlobe na gladkih (refleksnih) površinah.
- S teleskopom v vrednosti manj kot 1500 USD je mogoče prebrati zrcaljeno sliko Wordovega dokumenta z velikostjo fontov 12 pik iz oddaljenosti 10 metrov. Z Dobsonovim teleskopom za 27.500 USD pa so uspeli prebrati vsebino dokumenta iz oddaljenosti 30 metrov.

Kraja ključev iz RAM-a

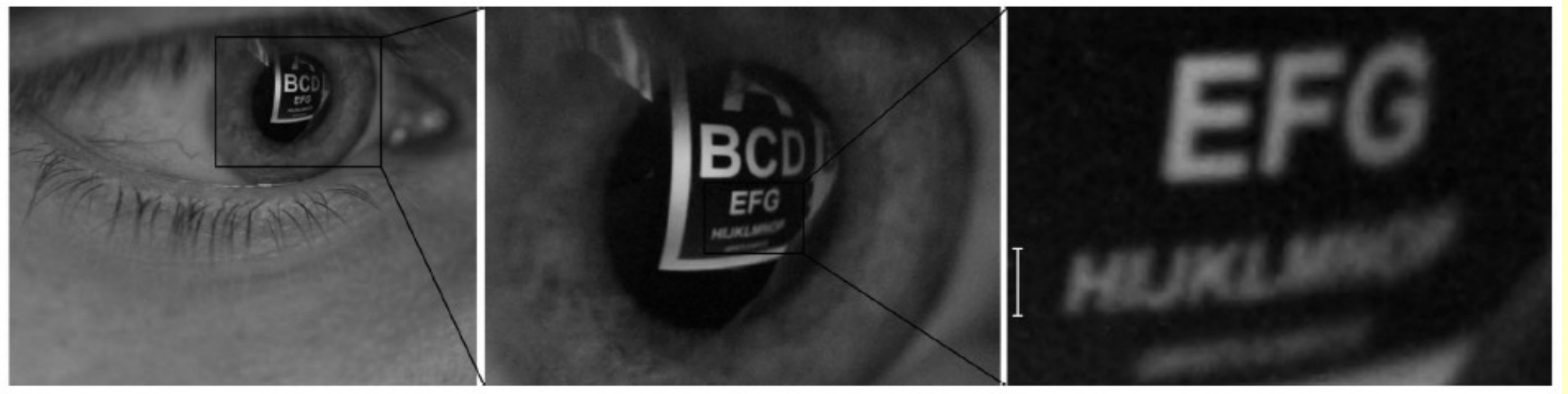
- Orodje Disk Decryptor za iskanje ključev v RAM-u.
  (Brian Kaplan, RAM is Key - Extracting Disk Encryption Keys From Volatile Memory, <http://www.andrew.cmu.edu/user/bfkaplan/KaplanRAMisKeyThesis.pdf>, glej tudi *Live View Forensics Tool* za zagon slike diska v virtualnem stroju brez spremembe slike)

Kraja ključev iz RAM-a

- Stoned Bootkit:
  okuži MBR - kraja TrueCrypt gesla, eskalacija privilegijev za CMD v okolju Windows po zagonu whoami.exe
- Okužba tudi preko PDF datoteke
  <http://www.stoned-vienna.com/downloads/PDF%20Spread/Stoned%20PDF%20Infector.pdf>



Branje vsebine monitorja iz odboja s pomočjo teleskopa



Vir in avtorstvo: Backes, Dürmuth in Unruh, *Compromising Reflections or How to Read LCD Monitors Around the Corner*, 2008 (http://www.infsec.cs.uni-sb.de/projects/reflections/)

Zaseg RAM-a preko FireWire vmesnika

- Specifikacija FireWire vmesnika (znan tudi kot IEEE 1394) določa, da imajo zunanje naprave priključene na FireWire vmesnik neposredni dostop do pomnilnika (mimo procesorja).
- Prvi program za branje in pisanje v pomnilnik RAM preko FireWire je leta 2002 napisal *Quinn "The Eskimo!"*. Program FireStarter je omogočal spreminjanje slike na zaslonu Mac računalnika preko vmesnika FireWire.
- Leta 2004 so Michael Becher, Maximillian Dornseif in Christian N. Klein na predavanju "*0wn3d by an iPod*" prikazali idejo forenzičnega zajema RAM-a preko vmesnika FireWire.

Zaseg RAM-a preko FireWire vmesnika

- Leta 2006 je Adam Boileau napisal program za branje vsebine RAM-a računalnika z Windows operacijskim sistemom preko FireWire vmesnika.
- Leta 2008 je Boileau objavil program *Winlockpwn*, ki omogoča odklepanje računalnika Windows Xp z vključenim ohranjevalnikom zaslona.
- Modificirana različica omogoča tudi odklepanje računalnika z operacijskim sistemom Windows Vista.
- Nekdo je uspel odkleniti tudi prenosnik brez FireWire vmesnika in sicer tako, da je v zaklenjen prenosnik vstavil Cardbus Firewire kartico, počakal da se je samodejno namestila ter nato računalnik odklenil.

Zaseg RAM-a preko FireWire vmesnika

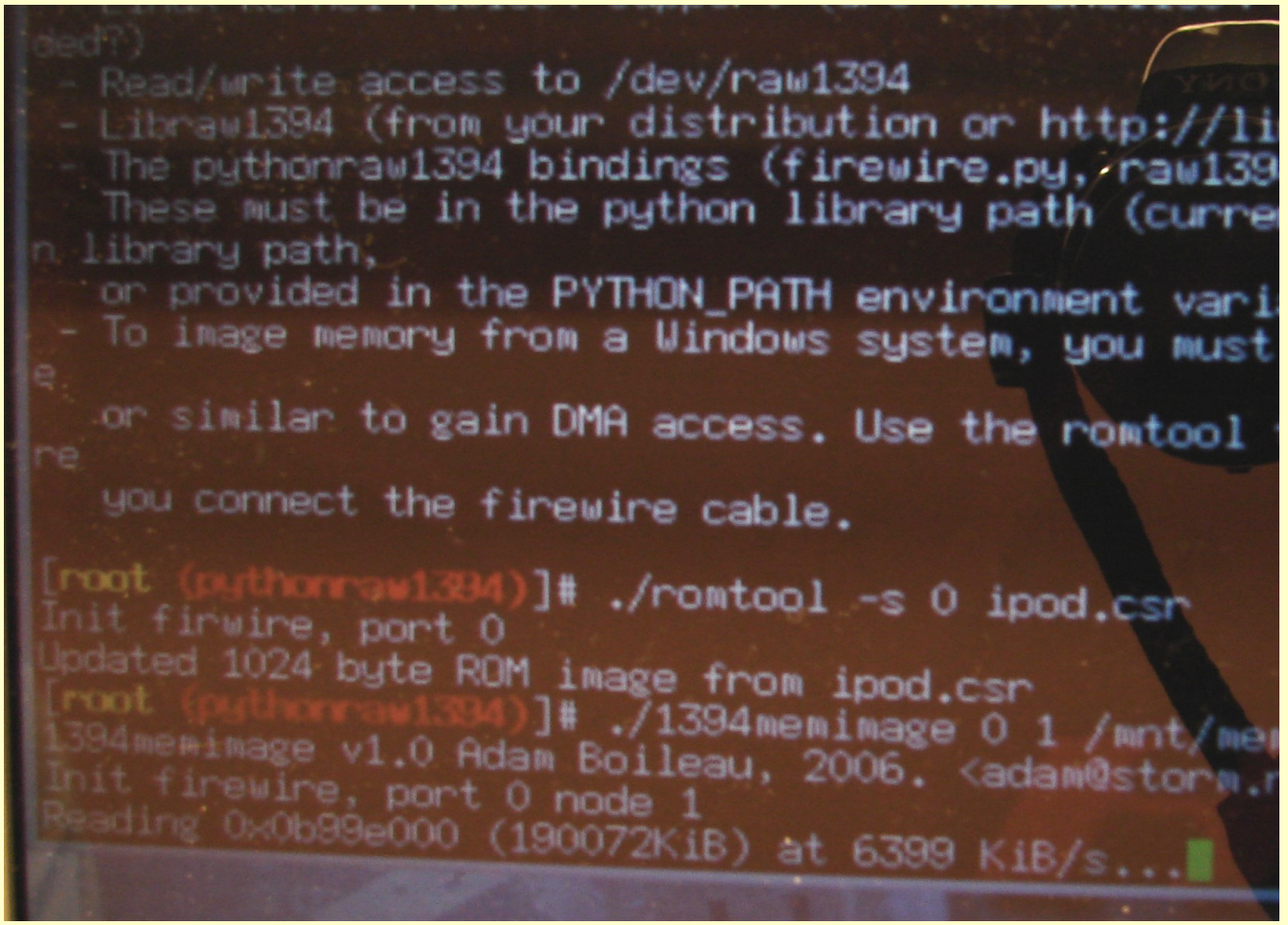
Root Terminal

```
[root (knoppix)]# cd /usr/local/pythonraw1394/
[root (pythonraw1394)]# modprobe ohci1394
[root (pythonraw1394)]# modprobe raw1394
[root (pythonraw1394)]# ./romtool -s 0 ipod.csr
Init firwire, port 0
Updated 1024 byte ROM image from ipod.csr
[root (pythonraw1394)]#
```

S programom romtool se v računalniku z Linuxom pretvarjamo, da smo iPod...

... in Windows Xp med priključenimi napravami prikažejo iPoda!

Zaseg RAM-a preko FireWire vmesnika



Z orodjem *1394memimage* prekopiramo vsebino RAM-a iz računalnika z Windows Xp preko FireWire vmesnika na trdi disk.

Analiza zaseženega RAM-a

- **strings fwramdump.img | grep banka**
  - Referer: http://www.abanka.si/sys/cmspage.aspx?MapaId=8010
  - Host: www.abanka.si
  - Cookie:ginger@abanka.si/
  - ginger@abanka[1].txt
  - Visited: ginger@http://www.abanka.si
  - Visited: ginger@http://www.google.si/search?hl=sl&q=abanka&meta=
  - Visited: ginger@http://www.abanka.si/sys/cmspage.aspx?MapaId=8010

Opomba: ime prijavljenega uporabnika je bilo "ginger".

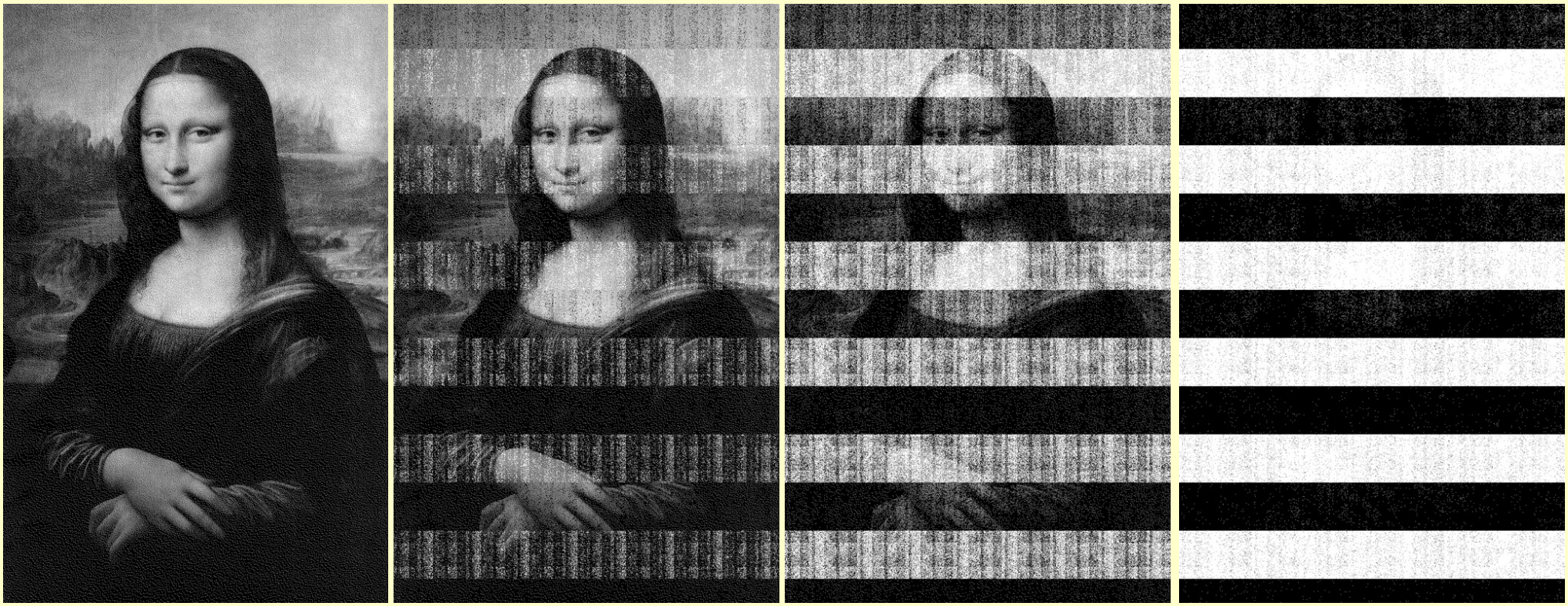
Zaseg RAM-a po izklopu računalnika

- Napad *Physical Memory Ghost* ali *Icemann attack* je omenil Douglas MacIver iz Microsofta leta 2006 v predstavitvi "*Penetration Testing Windows Vista Bitlocker Drive Encryption*".
- Aprila 2008 raziskovalci Princeton University objavijo članek "*Lest We Remember: Cold Boot Attacks on Encryption Keys*" (http://citp.princeton.edu/memory/).
- V raziskavi so pokazali da se vsebina pomnilniških modulov DRAM ne izgubi v trenutku, ko računalnik ugasnemo, pač pa se izgublja z časom.

Zaseg RAM-a po izklopu računalnika

- Vsebino DRAM modulov je mogoče prebrati še nekaj sekund, do nekaj minut po tem, ko je računalnik ugasnjen. Ta čas se da podaljšati s hlajenjem:
  - hlajenje na okrog -50 °C: vsebina se ohrani do več kot deset minut,
  - hlajenje s tekočim dušikom na do -196 °C: vsebina čipov brez napajanja se lahko ohrani nekaj ur.

Cold boot napad



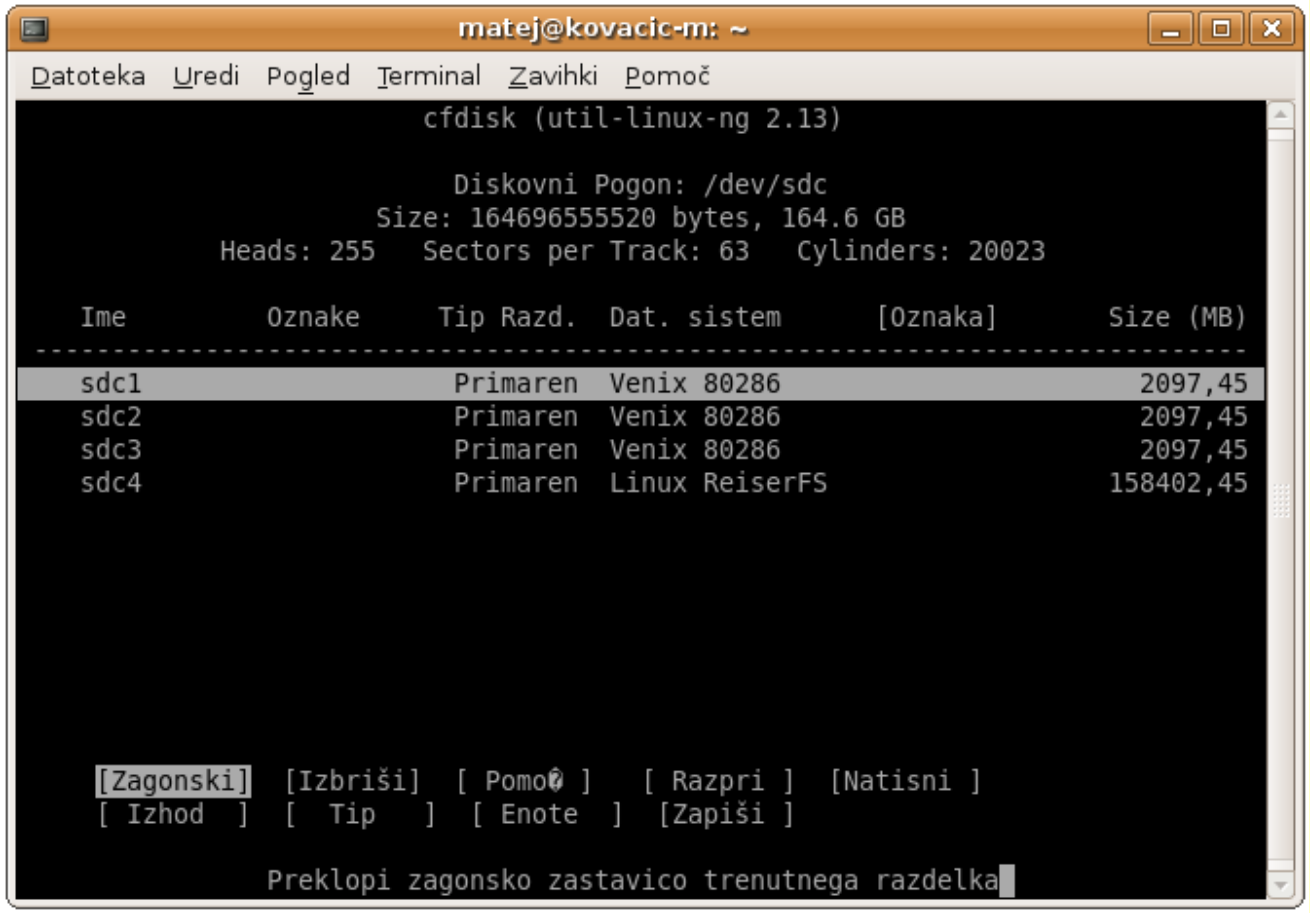
Zasežena slika po 5 sekundah, 30 sekundah, 60 sekundah in 300 sekundah.

Vir in avtorstvo: J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum in Edward W. Felten, Prineton University, 2008. <http://citp.princeton.edu/memory/>

Zaseg RAM-a po izklopu računalnika

- Kmalu nato Robert Wesley McGrew na svojem blogu objavi program za zaseg pomnilnika RAM na trdi disk z imenom "*msramdmp*" ter pripravi zagonski CD, ki samodejno zapiše vsebino pomnilnika RAM na trdi disk.
- Vsebina se zapiše na prvi razdelek označen kot tip razdelka 40 (Venix 80286), po zapisu se razdelek označi s tipom 41.
- Potrebno je pripraviti (USB) disk z razdelkom enakim ali večjim količini pomnilnika RAM.
- Za pripravo uporabimo orodje cfdisk. Razdelek prepišemo z ničlami (sudo dd if=/dev/zero of=/dev/sdc1 bs=512).

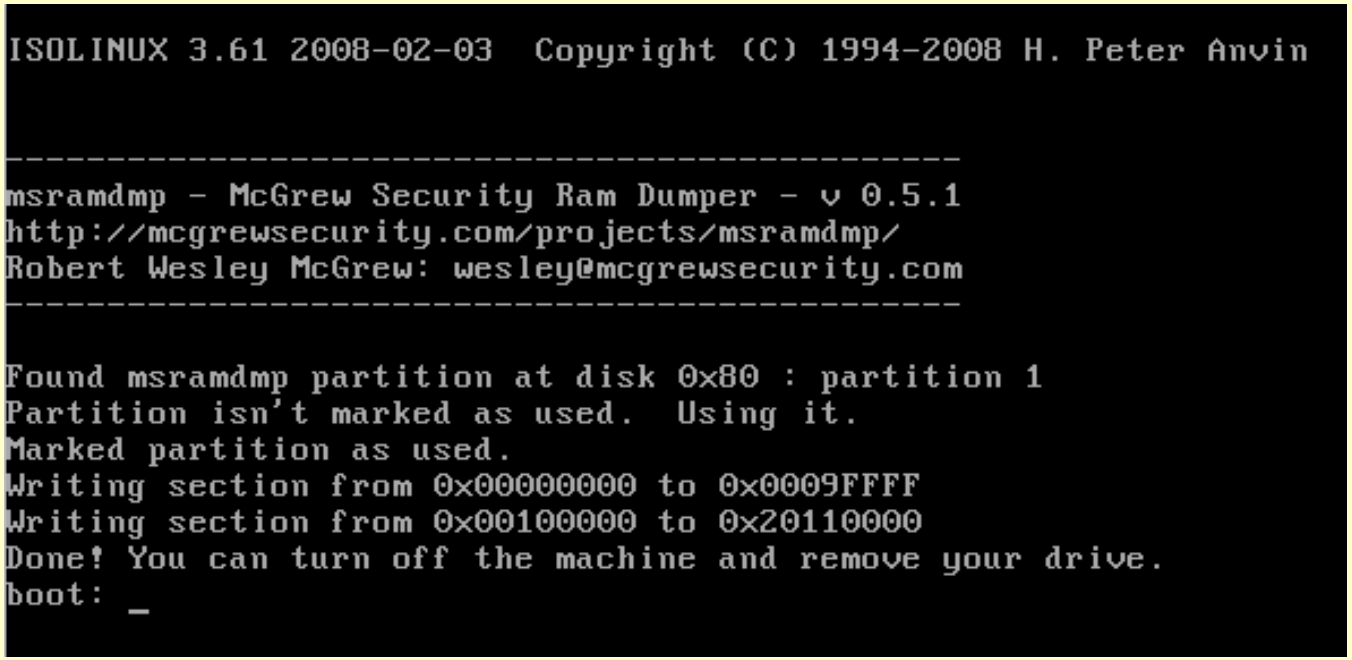
Zaseg RAM-a po izklopu računalnika



Priprava (USB) diska za zaseg.

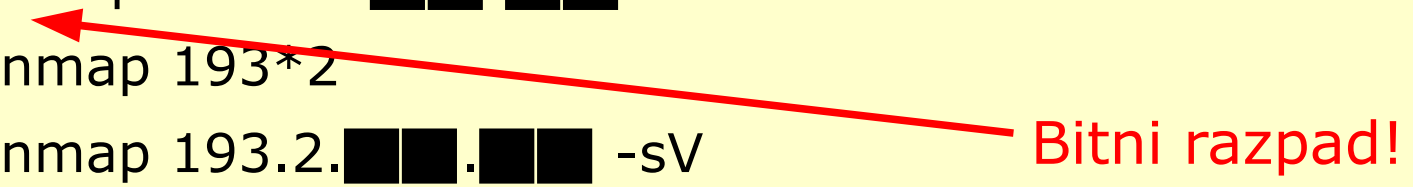
Zaseg RAM-a po izklopu računalnika

- Test zasega po metodi “giljotine” (izklopimo napajanje primarnega trdega diska ter računalnik resetiramo)
- Na testnem računalniku smo izključili napajanje, priključili USB disk ter računalnik zagnali s pomočjo živega Msramdmp CD-ja:



Analiza zaseženega RAM-a

- **strings ramdump.img | grep nmap**
  - sudo nmap 193.2.[redacted] -sV
  - sudo apt-get install wireshark nmap
  - sudo nmap 193.2&[redacted]
  - 3udo nmap 393.2.[redacted]
  - sudo nmap 88.200.[redacted]
  - sud/ nmap 88.200.[redacted] -PN
  - sudo nmap 193*2
  - sudo nmap 193.2.[redacted] -sV
  - sudo nmap 193.2.[redacted] -sV
  - sudo nmap 113.2.[redacted] -sU



Analiza zaseženega RAM-a

- **strings ramdump.img | grep /media**
  - fm|e:///media/MATEJ/emporium/IMG_1564.jpg
  - file:///media/MATEJ/emporium/IMG_1581.jpg
  - file:///media/MATEJ/empo
  - file:///media/Kingrton/banner_uplad.psd
  - file:///media/MATEJ/eduroam.txt
  - file:///media/MATGJ/emporium/IMG_15<3.jpg
  - file:///media/MATEJ/prap_serfi#e/u1.0ng
  - file:///media/MATEJ/emporium/MMG_1561.jpg
  - file:///media/LATEJ/texti_predavanja/SAFE-SI_ucitelji/EULA.odp
  - file:///media/Secure-USB/kismet-zd1211.conf

VI: Kakšno rešitev izbrati?

- Security through obscurity.
- Black box rešitve.
- Praktična področja uporabe kriptografije.

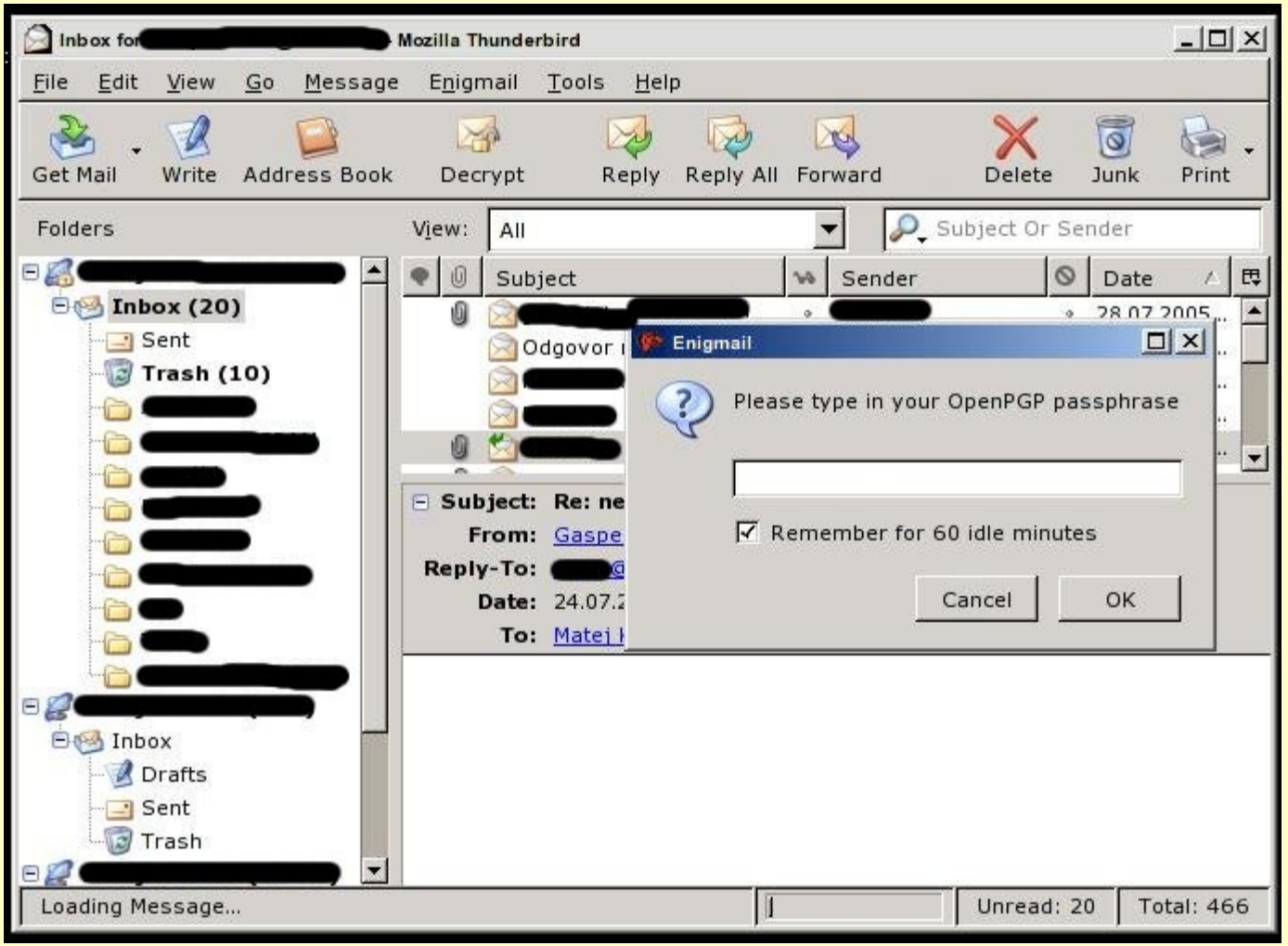
- Vprašanja in debata.

But there's an old saying inside the NSA: *"Attacks always get better; they never get worse."* --Bruce Schneier.

Uporaba šifriranja v praksi

- GPG, OpenPGP
- šifriranje e-pošte (Enigmail),
- šifriranje v sistemih za neposredno sporočanje (pidgin-encryption, off-the-record),
- uporaba varnih protokolov (https, pop3s, imaps,...)
- šifriranje povezav med računalniki (SSH, VPN...),
- šifriranje nosilcev podatkov,
- šifriranje celotnega sistema.

Šifriranje e-pošte

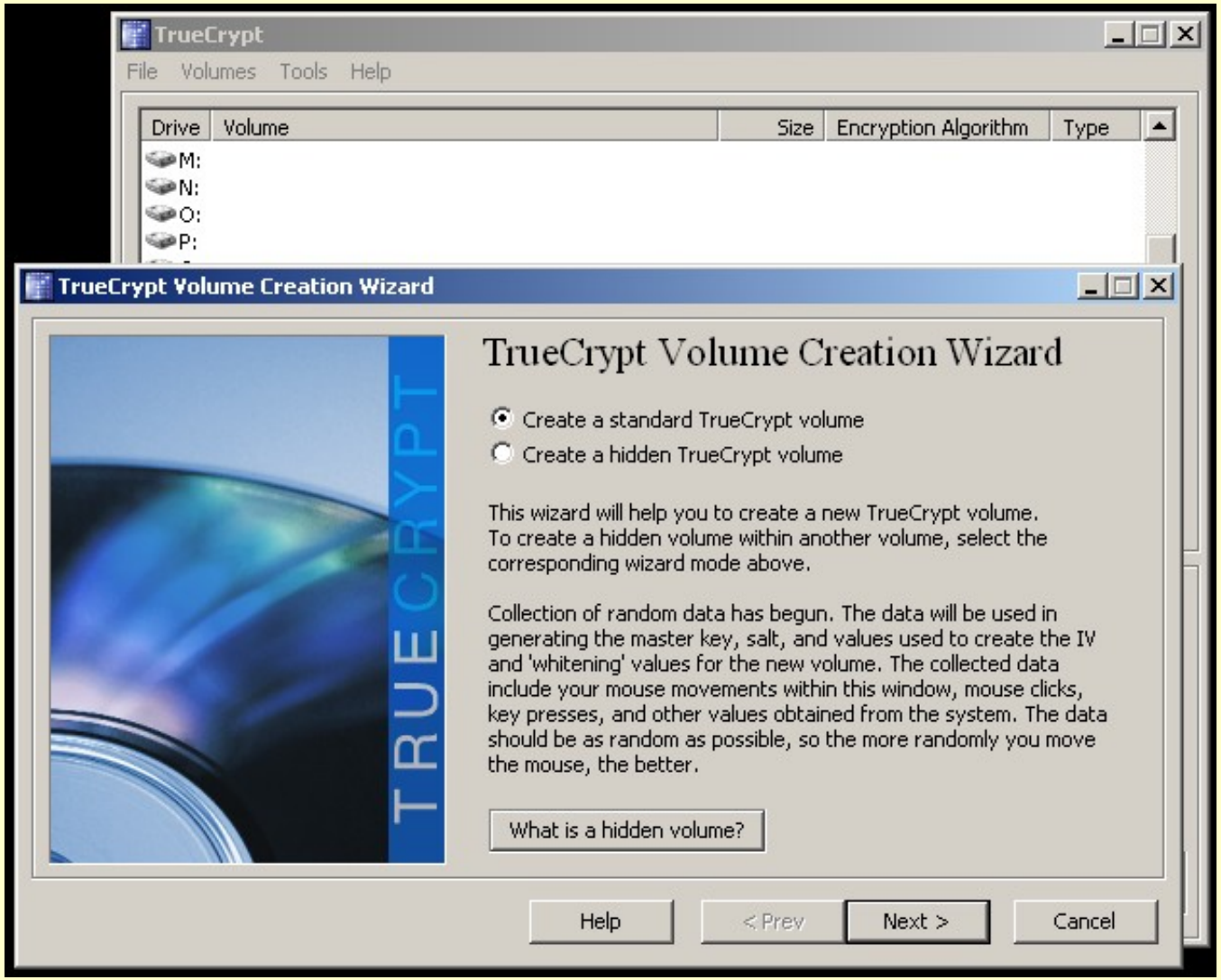


Šifriranje elektronske pošte v odprtokodnem odjemalcu elektronske pošte *Mozilla Thunderbird* z dodatkom *Enigmail*.

Šifriranje nosilcev podatkov

- Predpriprava nosilcev podatkov za šifriranje (varno uničevanje podatkov).
  - DBAN
  - dd
- Šifriranje z geslom in šifriranje z datoteko s ključem.
- Šifriranje začasnih pomnilnikov (temp, cache, swap)

Šifriranje nosilcev podatkov



Šifrirni program *TrueCrypt* v okolju Windows.

General guidelines for security* :-)

1. Do not assume anything (*Ne predpostavljaj ničesar*).
2. Trust no-one, nothing (*Nikomur, ničemur ne zaupaj*).
3. Nothing is secure (*Nič ni varno*).
4. Security is a trade-off with usability (*Večja varnost pomeni manjšo udobnost*).
5. Paranoia is your friend (*Paranoja je tvoja prijateljica*).

* **Splošne varnostne smernice**, iz priročnika orodja *Advanced Intrusion Detection Environment*, "The Aide manual" <http://www.cs.tut.fi/%7Erammer/aide/manual.html>.