

# **Varnost skozi transparentnost ali varnost skozi skrivanje?**

**Matej Kovačič**

**Fakulteta za družbene vede, Univerza v Ljubljani**

9. slovenski dnevi varstvoslovja, Bled 5. in 6. junij 2008

**(CC) 2008**

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Čufarjeva ulica 17, 1000 Ljubljana.

# 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 večih 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.

# Kerckhoffsov zakon...

- Kerckhoffsov zakon tako pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa.
- Kerckhoffsov zakon zavrača načelo, da je mogoče varnost zagotoviti s skrivanjem (t. i. *'security through obscurity'*).
- Kerckhoffsov 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.”*.

# 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

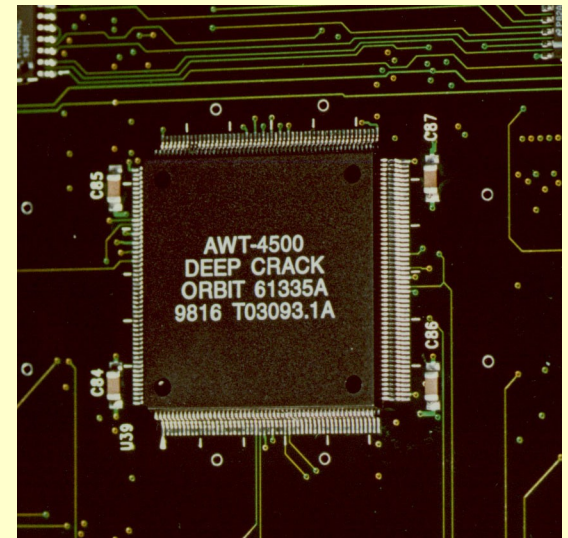
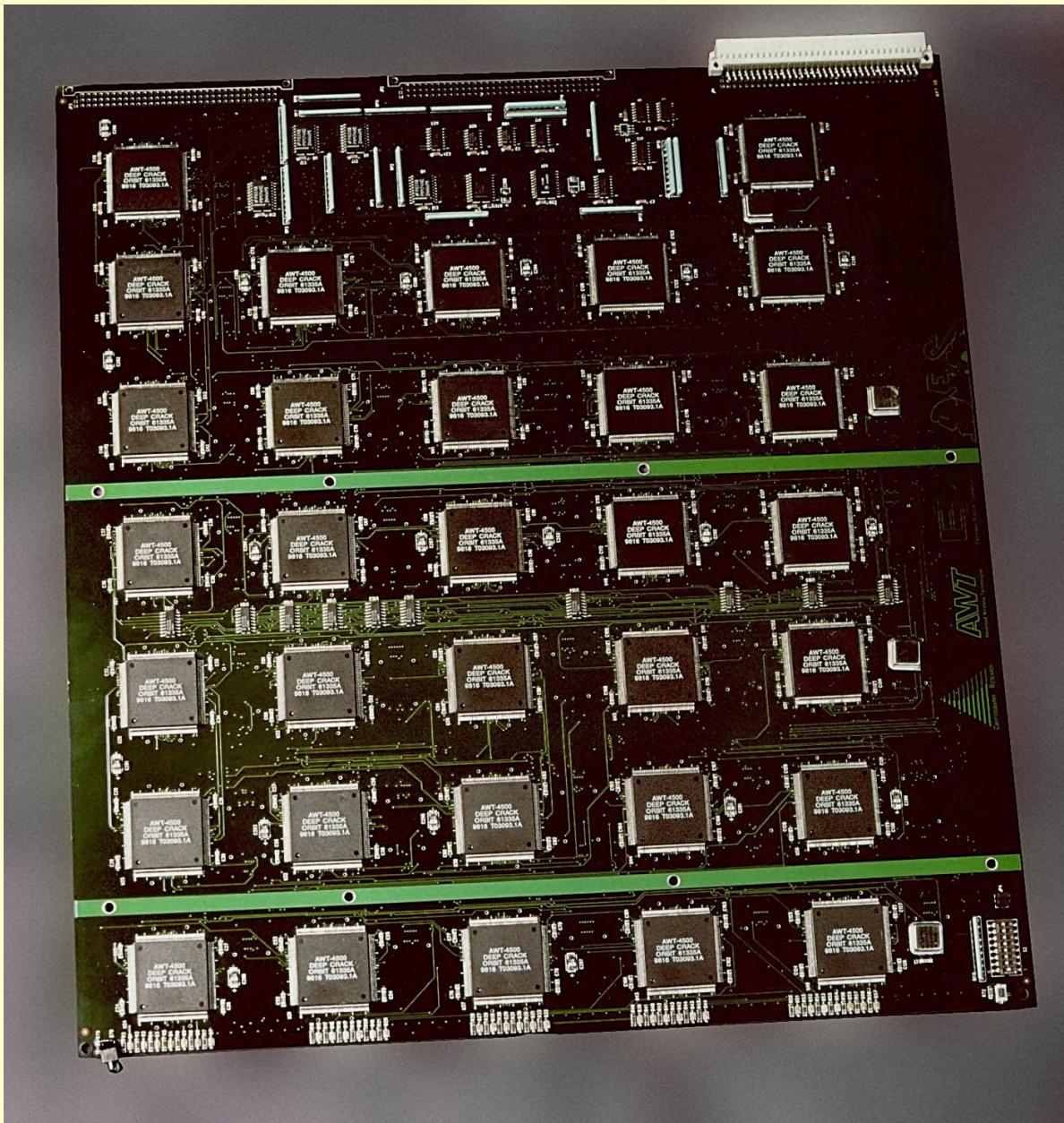
- Revizija NSA ugotovila, da v algoritmu ni nobenih statističnih ali matematičnih slabosti, januarja 1977 je algoritem postal *Data Encryption Standard*.
- Pred tem je bil algoritem deležen številnih kritik. Hellman in Diffie sta izračunala, da bi bilo mogoče s posebnim računalnikom za 20 milijonov USD 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 kriptanalize, ki sta jo poimenovala diferencialna kriptanaliza (ang. *differential cryptanalysis*).

# Primer Data Encryption Standard

- Civilna različica DES naj bi bila prirejena tako, da je bila učinkovitost do tedaj neznanega napada z diferencialno kriptanalizo povečana.
- 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

# Primer 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.

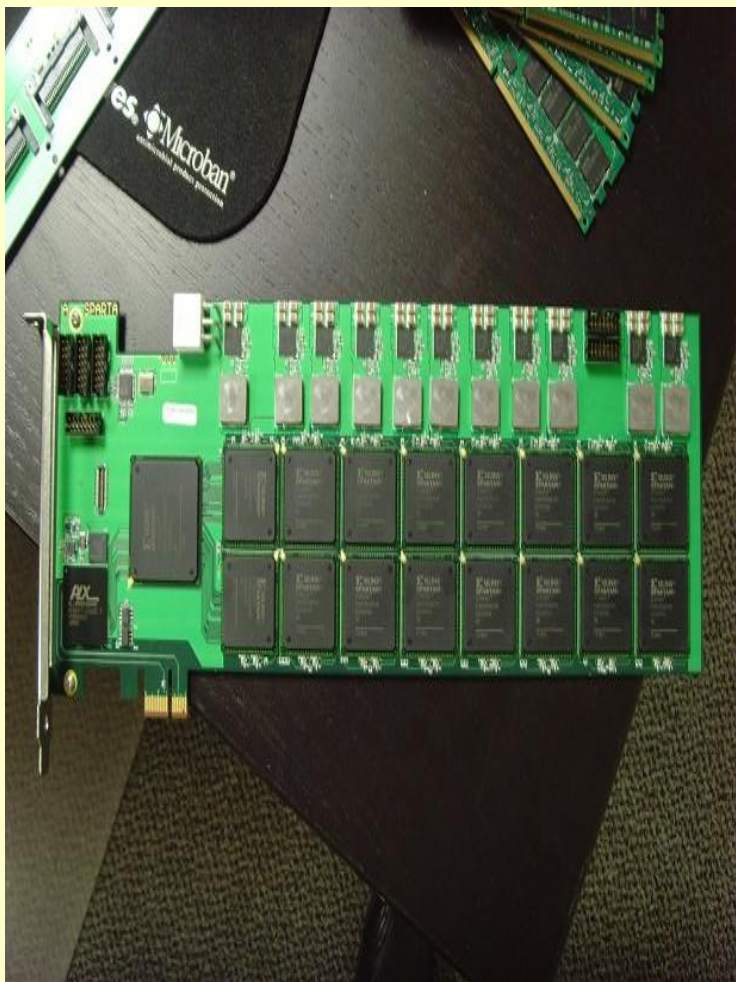
# Primer GSM telefonije

- 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 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, ki so jo poimenovali COPACOBANA.

# GSM Cracking Project



FPGA (Field-programmable gate array) in The A5 Buster

# Primer 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.
- Hulton in Muller trdita, da bo njuna naprava za 1000 USD omogočala dešifriranje signala v 30 minutah, naprava za 100.000 USD pa dešifriranje v 30 sekundah.
- Danes GSM uporablja več kot 2 milijardi uporabnikov, slabo zasnovano infrastrukturo pa bo izredno težko v kratkem času nadgraditi v varnejšo.

# Pomen transparentnosti

- Vprašanje odprtosti in transparentnosti ni zgolj vprašanje svobode, pač pa tudi vprašanje varnosti in zaupanja.
- Šibka varnostna zasnova se čez nekaj časa lahko vrne kot bumerang.
- *But there's an old saying inside the NSA: "Attacks always get better; they never get worse." --Bruce Schneier*