BIZTONSÁGI PARADIGMÁK TÁVKÖZLÉSI HÁLÓZATOKAT MENEDZSELŐ RENDSZEREKBEN

Zömbik László
BME-TMIT, Ericsson Hungary

ÁTTEKINTÉS

- **Támadások a nagyvilágban**
- Kritikus infrastruktúrák és támadások
- Biztonsági célok Menedzsment rendszerekben
- Architektúrák

TÁMADÁSOK
CÉLOK

Támadások célja
- Rossz hír keltés
  - (pl. Deface - Arctalanítás)
- Tudás fitogtatás
  - (pl. szolgáltatás bénítás)
- Információ szabadság
- Pénzszerzés
- Terrorizmus
- Kémkedés
- Cyber hadviselés

BIZTONSÁGI SÉRÜLÉKENYSÉGEK

- Szoftverhibák, programmozási hibák
  - Buffer overflow
  - Nem megfelelő argumentum ellenőrzések, függvényhívások
  - Protokoll hibák: Undead attack, Teardrop, christmas
- Biztonsági Protokoll hibák
- Rendszer hibák
  - Elárasztással szemben védtelenség (smurf, SYN, ping,...)
  - Gyenge algoritmusok használata/engedélyezése
  - Komponensek nem biztonságos módon való összeépítése
- Felhasználás – az emberi tényező
  - Vírusok, malwarek
  - Phising, hiszékenység (social engineering)

AKTÍV HACKER CSOPORTOK

- Anonymous (2003-)
- Lulzsec (2011-)
- Cslsec (Cant stop Laughing on Security)
- TeaMp0isoN
- @itskahuma

TÁMADÁSOK
VILÁGSZERTE, 2011

- **March 17:** **RSA** SecureID data related Secure Token stolen **50-100M$**
- **April 20:** LulzSec **Sony** Playstation network **(4 billion$)** SQLi: **100 million user** personal information stolen
- **May 10:** **Citigroup** SQLi/XSS by LulzSec 200 000 user data stolen.Cost of the breach **22M$,** Hackers made **2.7M$**
- **June 1:** **Gmail** attacks from China against US Govt officials, Chinese political activist (Phising)
- **Jun 16:** **SEGA** 1.2M user name, emails, date of birth and passwords **77M$**
- **Jul 4:** **Fox News** Twitter account hack: **President** had been **killed**
- **Jul 8:** **Moody's** Portugeese hackers react defacing to the negative assessment
- **Aug 10,12:** Hong Kong **Stock Exchange**, when release sensitive results: **DDoS**
- **Sept 1:** **Kernel.org** server **rooted**

TÁMADÁSOK
VILÁGSZERTE, 2011

- **Sept 9:** **NBC News** twitter hacked, false tweets **plane** attack on **Ground Zero**
- **Sept 11:** Entire **Linux foundation** is down as a security breach again
- **Sept 26:** Inmotion Hosting Network is hacked by Tiger-M@te **700 000 sites** were defaced in one step
- **Oct 8:** German Chaos Computer Club reveals a "**state malware**" to record **skype** calls
- **Oct 12:** First **cloud** based attack on Raytheon, **US Defense** Contractor
- **Dec 1:** **Kapersky, NOD32** Defacement
- **Dec 4:** D3SMOND142 hacks **MySQL** with an **SQL injection**, db and user account
- **Dec 8:** **Lockheed Martin** is targeted with the **0-Day** vulnerability in Adobe Reader
- **Dec 8:** **Zaire Security** Firm BitDefender Defaced
- **Dec 15:** **Visa Europe** potential data securit breach affected payment processor servers

TÁMADÁSOK
VILÁGSZERTE, 2012

- **01.01-03.** South African **Postbank 6.7M$** is stolen
- **01.31, 02.12** **NASA** hacked, 6.7Gb data dumped, 122 passwords cost **26k$**
- **02.10.** Herxode found a vulnerability in the **Medal of Honour** forum, **asked 50$ for charity**.Admin rude reply, hacker dumped 3000 accounts **cost of breach 642 000$**
- **02.15** **NASDAQ** DDoS by L0NGwave99
- **03.11** Senior British **Military officers**, **Defense Ministry** officials tricked becoming **Facebook friends** with US Navy Admiral James Stravridis - **expose information**
- **03.13** AlienVault Detected several targeted attack against **Tibetan activist organizations** origin same Chinese group as launched 'Nitro' attacks against chemical and defense orgs.
- **03.14** **BBC** director declares **cyber attacks**, attempts to **jam satellite** feeds and **swamp London phone lines** with automated calls
- **03.25** **Militarysingles.com** **170 937 accounts** username, password, email on Pastebin
- **05.24** Hillary Clinton: **State Department** hacked **Yemeni** tribal websites replacing Al-Quaida propaganda
- **06.05** **Romney's** private email is hacked

TÁMADÁSOK
DÉLNYUGAT ÁZSIA 2011

2011.10.14 **Indian** hacker defaces Pakistan embassy in China
2011.10.15 **Pakistani** hacks **cyber cell**, Mumbai

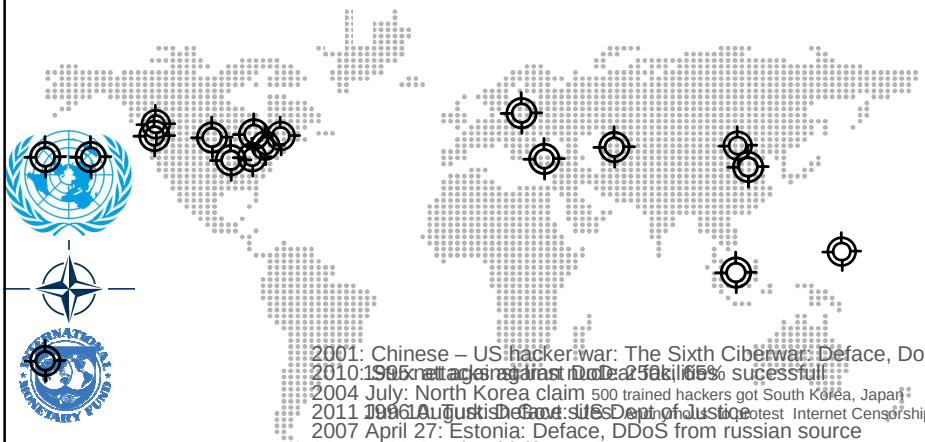
2011.11.27 **Hyderabad Alumni Association** hacked, 550+ user account leaked
2011.11.29 nearly 100 **Pakistan Govt site** targeted with malware Godzilla

2011.12.08 **Dawn.com** is deface and data leaked by India
2011.12.09 **Pakistani Cyber Army** defaces **India National Congress** and **Sonia Ghandi**

2011.12.20 Indishell hacks and Deface **800+ Pakistani sites**
2011.12.26 Destructivesec defaces twice in 10 hours bullshouse.com (**Indian Stock exchange**)

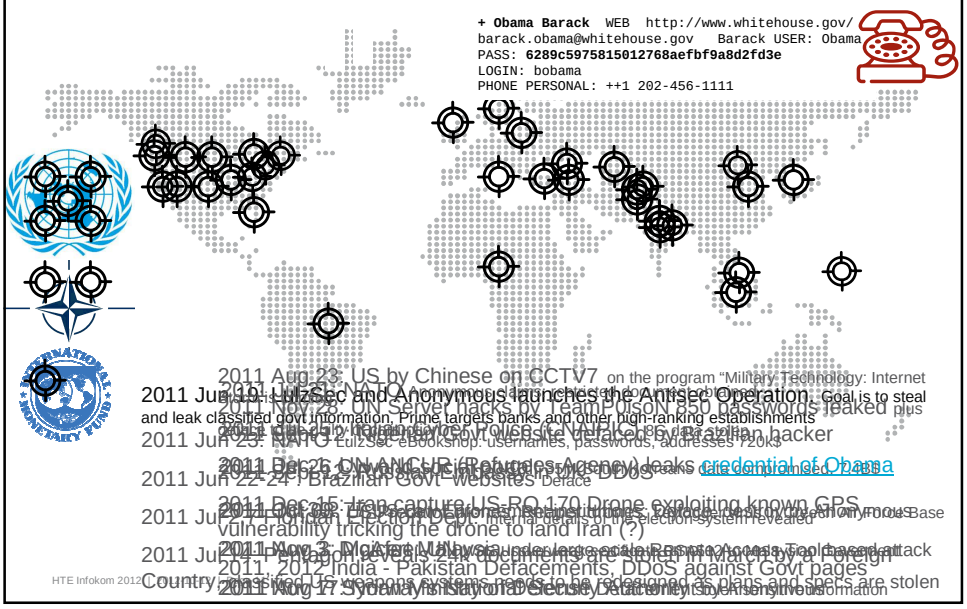
2012.01.04 30 **Pakistan Govt sites** defaced by Indishell
2012.01.06 @YamaTough:
The **source code of the Symantec** Endpoint Protection Enterprise Suite by hacking an **Indian Military Server**
Leaks out some information about: Indian Government is strong arming cell phone Manufactures to provide **back doors in their Handsets** (RIM, Nokia and Apple) information is allegedly stolen from Indian Embassy of Paris

TÁMADÁSOK
KORMÁNYZATI, KATONAI CÉLPONTOK -2011



2001: Chinese – US hacker war: The Sixth Ciberwar: Deface, DoS
2004 July: North Korea claim 500 trained hackers got South Korea, Japan
2007 April 27: Estonia: Deface, DDoS from russian source
as the response of the relocating of Bronze Soldier of Tallin

TÁMADÁSOK
KORMÁNYZATI, KATONAI CÉLPONTOK 2011



TÁMADÁSOK
KORMÁNYZATI, KATONAI CÉLPONTOK 2012

TÁMADÁSOK
HACKER VS HACKER

- **2011.08.09** **Syrian Electronic Army** hacked and Defaced **Anonplus** social network developed by Anonymous to retaliate the Deface of Syrian Ministry of Defense
- **2011.08.24** **TeaMp0isoN** deface **Cslsec**, which claim to be the new LulzSec
- **2011.10.04** **D33ds** hacks online **shop of Srblche** who sells access to websites, such as US Army, DoD, South Carolina National Guard
- **2012.01.15.** **DevilzSec** hacks and defaces several sites over the world, same day **M4tr1xCha0s Cyb3rSec** defaces DevilzSec Facebook page
- **2012.02.16** **TeamGreyHat** (TGH) Hacked by **3xp1r3** Cyber Army (Indian vs. Indian)
- **2012.02.05** **Devil's Café blog** is hacked, 4940 account is leaked online. Origin **unknown**
- **2012.02.09** India vs Pakistan: **Pakistani Hacker Group** defaces sites, which were **restored by Indian Hacker Godzilla Vulcanum**

ÁTTEKINTÉS

- Támadások a nagyvilágban
- **Kritikus infrastruktúrák és támadások**
- Biztonsági célok Menedzsment rendszerekben
- Architektúrák

KRITIKUS INFRASTRUKTÚRÁK

Azon rendszerek, melyek a társadalom működésének számára alapvetően fontosak

- Ivóvíz rendszerek (vízművek vezetékrendszerek),
- Elektromos hálózat
- Erőművek
- Logisztikai (és tömegközlekedési) rendszerek
- Kormányzati és igazgatási rendszerek
- Egészségügyi intézmények
- Pénzügyi rendszerek
- Távközlő hálózatok

TÁMADÁSOK KRITIKUS INFRASTRUKTÚRÁK ELLEN 1.

- Ivóvíz Rendszerek
  - 2011.11.17, Springfield, Ilinois: **water pump** turned on and off until burnt out. From September, Attack from Russia.
  - 2011.11.18 South Houston **water supply** hacked
  - 2011.12.13 FBI Deputy assistant director of Cyber division: hackers accessed **crucial water** and **power services** in three cities
- Elektromos hálózat
  - 2012.05.30 Anonymous: Indian Power company defaced
- Erőmű
  - 2010.03 Stuxnet
  - 2012.03.19 Atomic Data and Analysis Structure for Fusion in Europe is hacked
- Egészségügyi rendszerek
  - Tipikusan betörés és beteginformációk megszerzése
  - Szolgáltatás bénítás (webserver)

TÁMADÁSOK KRITIKUS INFRASTRUKTÚRÁK ELLEN 2.

- Pénzügyi rendszerek
  - IMF: Deface
  - Bankok
    - on line accountok, kártyaszámok
    - Pénzmozgás
  - Tőzsdék
    - DDoS

- Logisztika és tömegközlekedés
  - 2012.01. 23 **Nothwest Rail** “Hackers, possibly from abroad, attacked a Pacific Northwest railway company’s computer system, disrupting railway signals in December”

- Kormányzat
- Távközlő rendszerek

TÁMADÁSOK KRITIKUS INFRASTRUKTÚRÁK ELLEN 3.
TÁVKÖZLÉSI RENDSZEREK

- Előfizetői adatok, felhasználók adatforgalma
  - 2011.12.09 **Telstra**: ~1M user account details leaked, when the internal sever of customer service is openly accessible
  - 2011.12.14 **Telstra**: Phising attacks against users
  - 2011.06.26 **Mexico and Spain Telecommunication Network** : Software Vulnerability : Man In The Middle 110,000 User Credentials Stolen Email Addresses for Hotmail, AOL, Yahoo & Google Mail
  - 2011.02.08. (01.27) **KPN** mail server hacked 500+ user account details, including phone No, addresses

- Szolgáltatások elérhetősége
  - 2012.04.08 **USTelecom** DDoS by Anonymous
  - 2012.04.26 **UK2.net** a botnet DDoS attack from 10M IP addresses
  - 2012.04.16 **VoyagerMobile** DDoS

- Számlázás (számlázási információk, számlázás)

TÁMADÁSOK KRITIKUS INFRASTRUKTÚRÁK ELLEN 3.
TÁVKÖZLÉSI RENDSZEREK

- Transzport hálózat (hálózati elemek)
  - 2011.07 Femtocell hack lets intruders listen to calls
    - modified Sure Signal femtocell, a £50 device used to provide better mobile signals in homes, to eavesdrop on calls and text messages
  - 2012.06.22 New York - Dispatch Radio for Buses & Ground Vehicles (Police Cars, etc.)

```
RadioManufacturer=042,Motorola
RadioModel=042,MCS2000
Pwd: CleverDevices1
```

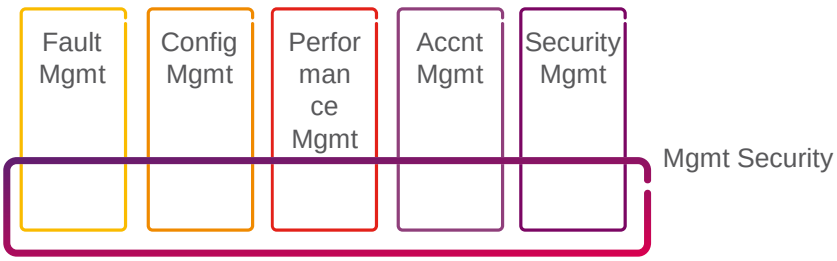
- Menedzsment infrastruktúra
  - 2012.06.27 **AT&T** #WikiBoatWednesday: https://voip.ipvoice.att.com/login.asp 6 admin account
  - 2012.01.14 US Telco server is hacked by TeamP0isoN, details of 80 administrators are leaked. Default passwords are used (112112)
  - Biztonsági és trust infrastruktúra - CA elleni támadások
    - **Comodo** (2011) **Diginotar** NL(2011) **Globalsign** (2011) **KPN** NL (2011)

ÁTTEKINTÉS

- Támadások a nagyvilágban
- Kritikus infrastruktúrák és támadások
- **Biztonsági célok Menedzsment rendszerekben**
- Architektúrák

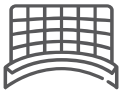
BIZTONSÁGI CÉLOK TÁVKÖZLÉSI MENEDZSMENT RENDSZEREKBEN

MENEDZSMENT RENDSZER
FCAPS MODELL



BIZTONSÁGI CÉLOK

- „Security Management”
  - Biztonsági szempontból eszközök menedzselése



- „Management security”
  - Menedzselt eszközök védelme
  - Menedzsment rendszerek védelme

BIZTONSÁGI CÉLOK
„SECURITY MANAGEMENT”

Security Mgmt

Szolgáltatások

- Trust és tanúsítvány menedzsment
- Biztonsági konfigurációs-menedzsment
- Központosított hitelesítés, authorizáció (hálózat, mgmt rendszer)
- Központosított naplózás, napló gyűjtés
- Biztonsági felügyelet
- Felhasználó (operátor) menedzsment
- Egyszeri beléptető rendszer (SSO - Single Sign On)

BIZTONSÁGI CÉLOK „MANAGEMENT SECURITY"

Mgmt Security

Módszerek a menedzselt és menedzsment rendszerek védelmére

- Határvédelem, zónák
  - Defense in Depth (többrétegű védelem) alapelv
  - Firewall, VLAN
- OS és alkalmazások felvértezése (hardening, striping)
- Vírusvédelem
- Nagy megbízhatóság HA (high availability)
  - Service Availability
- Kommunikáció védelme (titkosítás, integritás védelem)

ÁTTEKINTÉS

- Támadások a nagyvilágban
- Kritikus infrastruktúrák és támadások
- Biztonsági célok Menedzsment rendszerekben
- **Architektúrák**

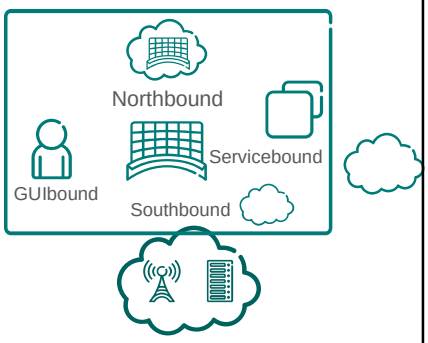
MENEDZSMENT RENDSZEREK BIZTONSÁGI ARCHITEKTÚRÁJA

MENEDZSMENT RENDSZEREK BIZTONSÁGI ARCHITEKTÚRÁJA

Management plane
(menedzsment réteg)

Control plane (vezérlő réteg)

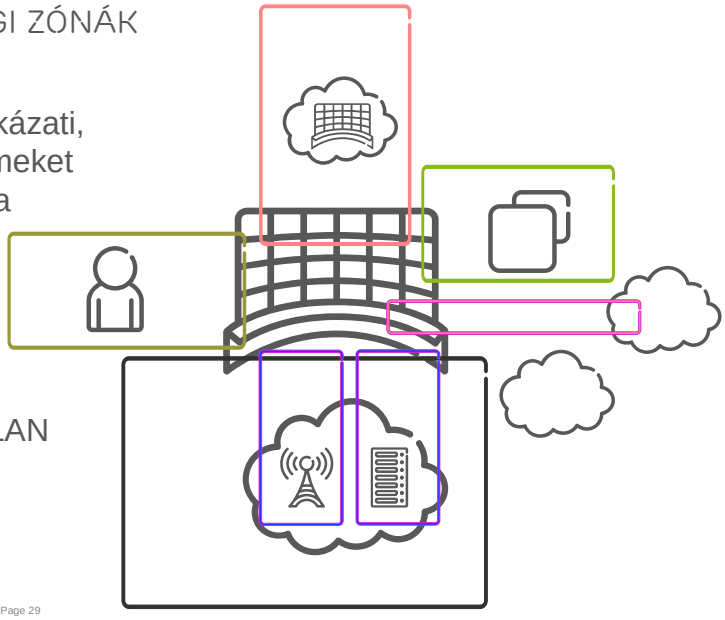
User plane (Felhasználói réteg)



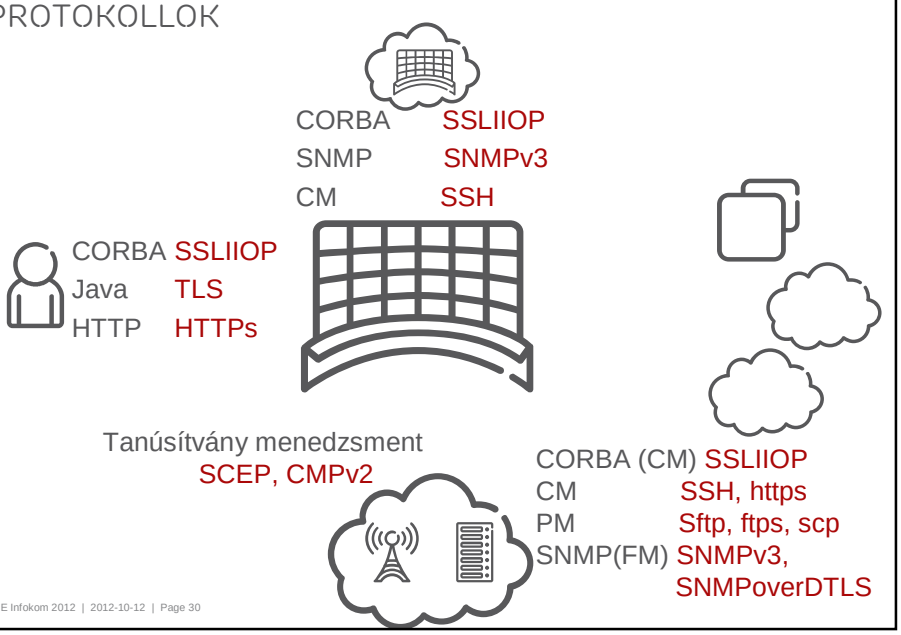
MENEDZSMENT RENDSZEREK
BIZTONSÁGI ZÓNÁK

Azonos kockázati, értékű elemeket egy zónába

Tűzfalak, VLAN

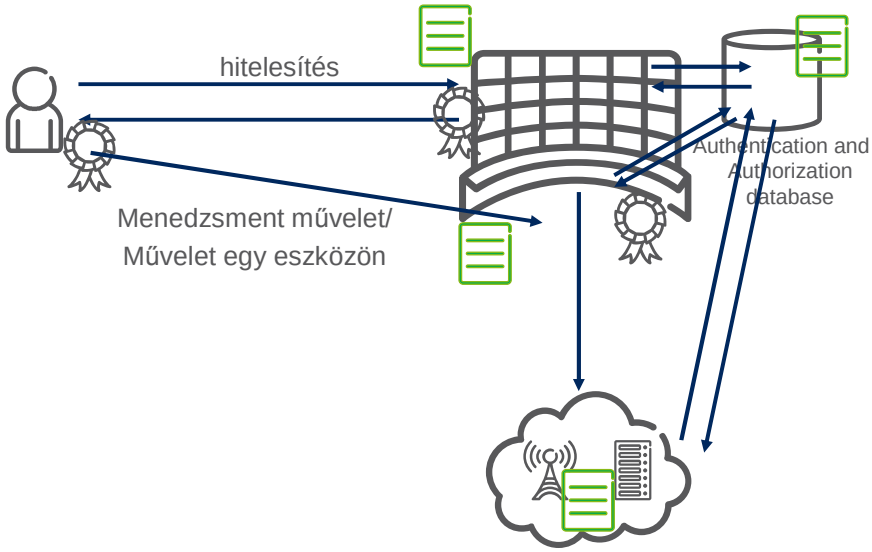


MENEDZSMENT RENDSZEREK
PROTOKOLLOK



MENEDZSMENT RENDSZEREK

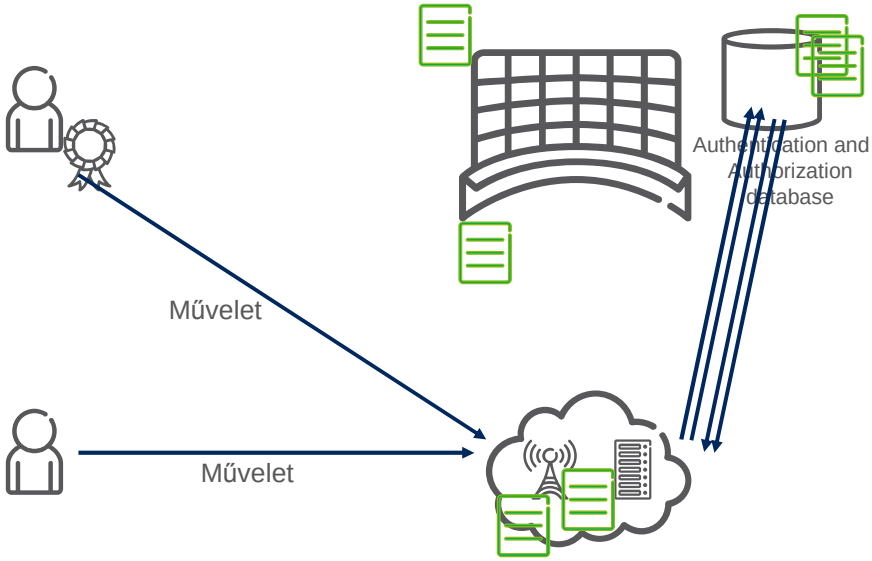
SSO, HITELESÍTÉS, JOGOSULTSÁG ELLENŐRZÉS, NAPLÓZÁS



HTE Infokom 2012 | 2012-10-12 | Page 31

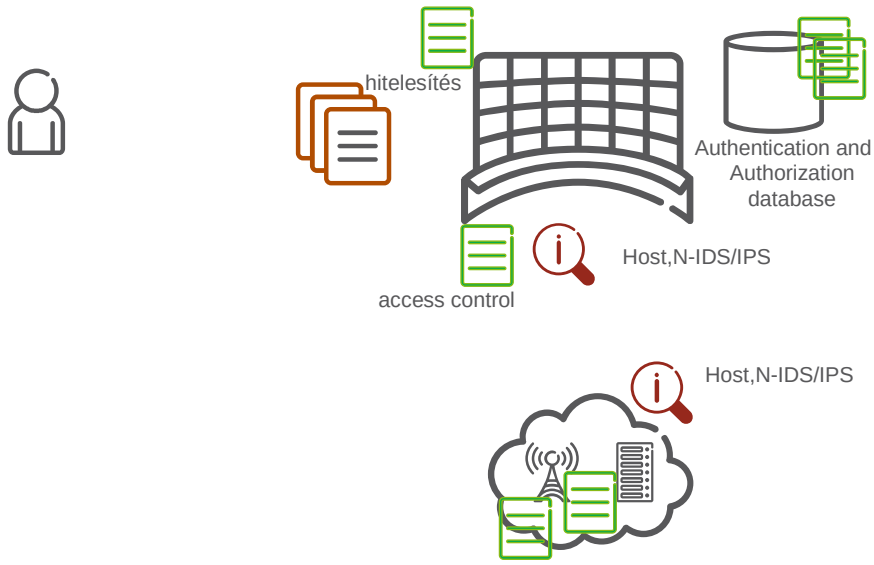
MENEDZSMENT RENDSZEREK

SSO, HITELESÍTÉS, JOGOSULTSÁG ELLENŐRZÉS, NAPLÓZÁS

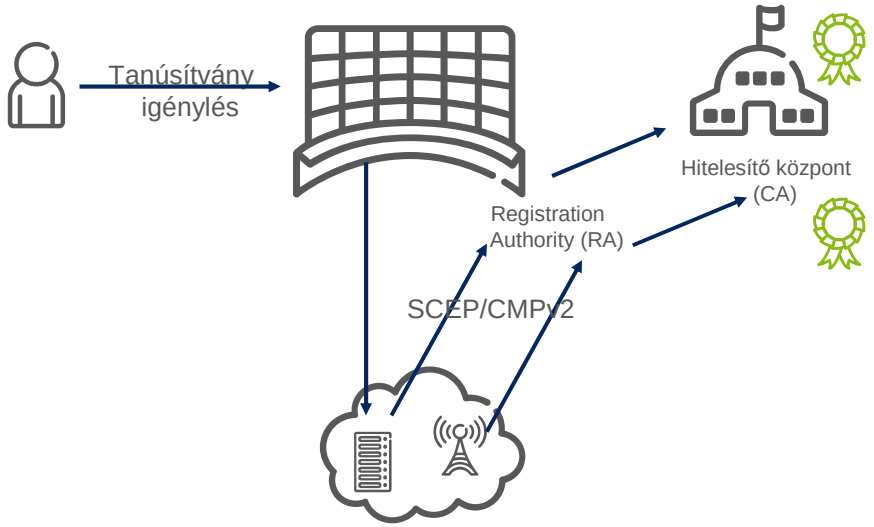


HTE Infokom 2012 | 2012-10-12 | Page 32

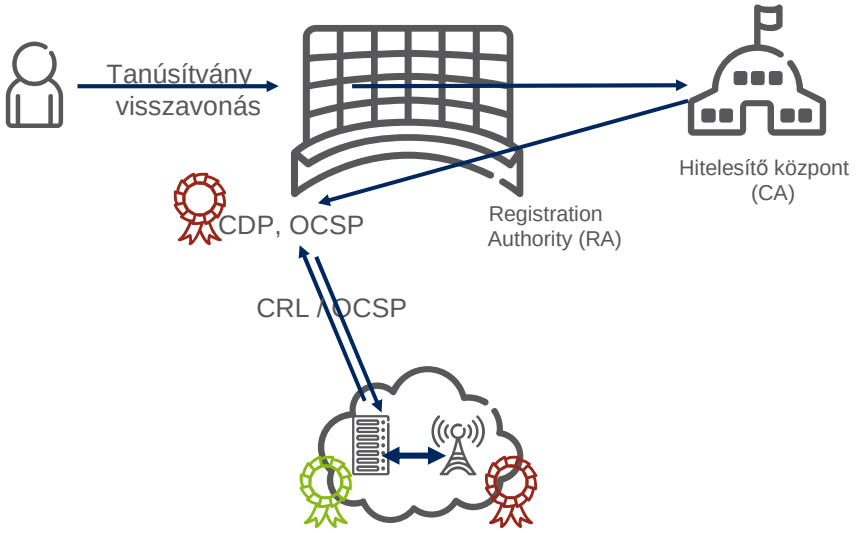
MENEDZSMENT RENDSZEREK
RENDSZER MONITOROZÁS



MENEDZSMENT RENDSZEREK
TANÚSÍTVÁNY LÉTREHOZÁSA



MENEDZSMENT RENDSZEREK
TANÚSÍTVÁNY ELLENŐRZÉSE

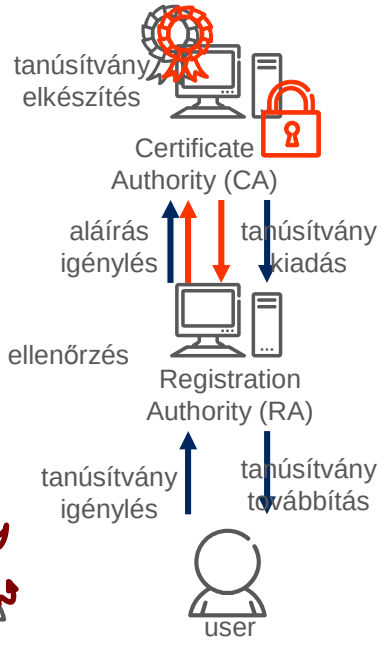


COMODO HACK

- 2011.03.15
  - Egy RA-nak egy jelszavát feltörték, új felhasználónevet készítettek

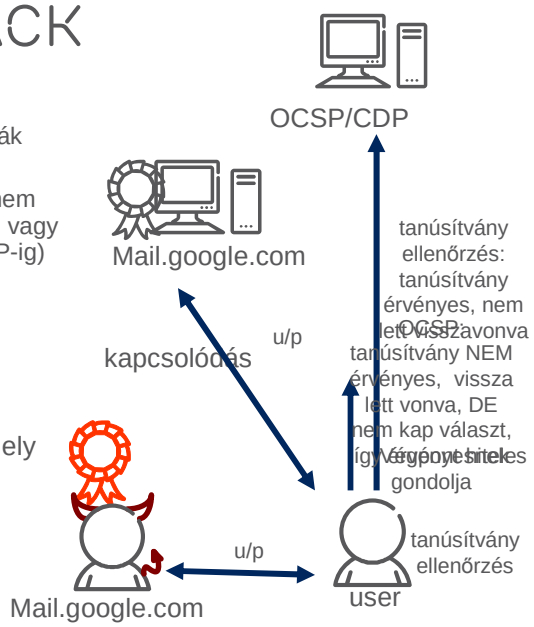
```
I hacked Comodo from InstantSSL.it, their
CEO's e-mail address mfpenco@mfpenco.com
Their Comodo username/password was:
user: gtadmin password: globaltrust
Their DB name was: globaltrust and instantsslcms
```

  - 9 tanúsíványt igényeltek
    - mail.google.com
    - www.google.com
    - login.yahoo.com (3 példányban)
    - login.skype.com
    - addons.mozilla.org
    - login.live.com
    - global trustee
  - A támadás iráni IP címről érkezett
    Pastebin Blog1 Blog2 Blog3 Blog4
    Comodo Fraud Incident



COMODO HACK

- 2011.03.15
  - A tanúsítványokat visszavonták
  - Visszavonás után az OCSP nem kapott kérést (nem haszálták, vagy a kérés nem jutott el az OCSP-ig)
- 2011.03.31
  - Ismételt támadás egy másik RA-hoz, sikertelenül
- Minden kliens sérülékeny, amely nem használ tanúsítvány ellenőrzést, ill. megbízik

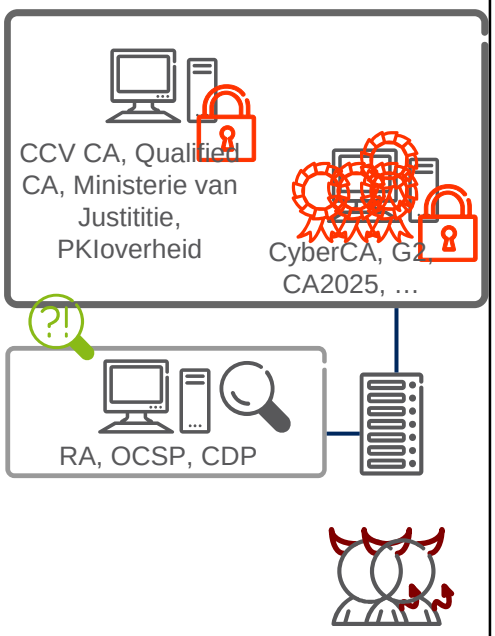


DIGINOTAR HACK

- Comodohacker (Janam Fadaye Rahbar) Pastebin Blog1, Blog2, Blog3
  „I will sacrify my soul for my leader”
- „Piet Hein Donner, minister of the interior, said in a press conference on Tuesday that the government will work as quickly as possible to replace all the DigiNotar SSL certificates in use. However, if the certificates are withdrawn immediately it will be damaging, he warned.”
- „The minister of internal affairs recommends people not to use the websites”
- „Tax administration would not be able to receive Money, unemployment and family benefits were not paid”
- „If the same CA are part of the main national Telco Operator, we can imagine what might have really happened and which risks the user have been exposed. ”
- Fox-IT: Operation Black Tulip 1.0

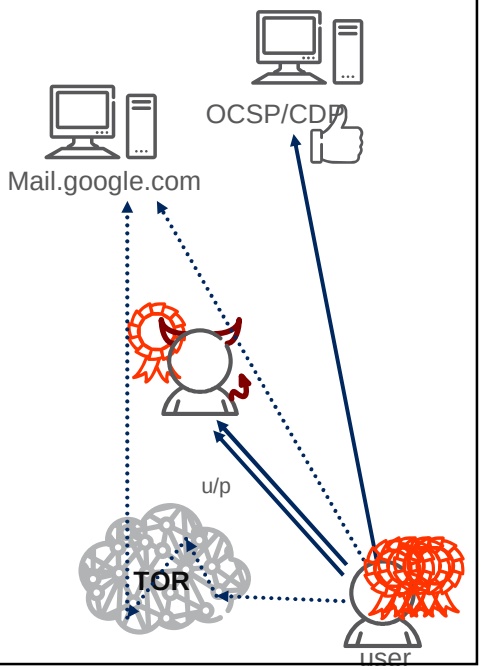
DIGINOTAR
A CA TÁMADÁSA

- 2009: F-secure
  - Diginotar web szervere kompromittálódott
- 2011.06.06.
  - Az első ismert felderítés
- 2011.06.17.
  - A DMZ-ben lévő szerverek elfoglalása
- 2011.06.19.
  - Betörés azonosítása a napi audit során
- 2011.07.02
  - Első kísérlet tanúsítvány készítésére
- 2011.07.10
  - Első sikeres tanúsítvány készítése
- 2011.07.19
  - *.google.com tanúsítványok készítése, mely a későbbi támadások alapja (128 tanúsítvány azonosítása és visszavonása aznap)
- 2011.07.20
  - Utolsó ismert tanúsítvány létrehozása (129 tanúsítvány azonosítása és visszavonása aznap)
- 2011.07.22
  - Utolsó ismert kimenő kommunikáció a támadók felé
  - Diginotar belső vizsgálatot indít, megbíz egy IT biztonsági céget
- 2011.07.27
  - IT biztonsági cég beszámolója, (75 tanúsítvány azonosítása és visszavonása)



DIGINOTAR
TANÚSÍTVÁNYOK FELHASZNÁLÁSA

- 2011.07.27.
  - Az első ismert felhasználása a hamis tanúsítványnak (ekkor még érvényes)
- 2011.08.04.
  - Nagy mennyiségű OCSP kérések Iránból ill. a TOR hálózatból
  - A tanúsítvány **érvényes**…
- 2011.08.27.
  - Hamis tanúsítvány felfedezése és bloggolása (iráni)
  - A tanúsítvány **érvényes**…
- 2011.08.29.
  - CERT-BUND (Német) felhívja a figyelmet a Govcert.nl (Holland Computer Safety for Govt Agencies)
  - Govcert Diginotar-nak jelez
  - Diginotar visszavonja a hamis tanúsítványt és beismeri a támadást



DIGINOTAR
EPILÓGUS

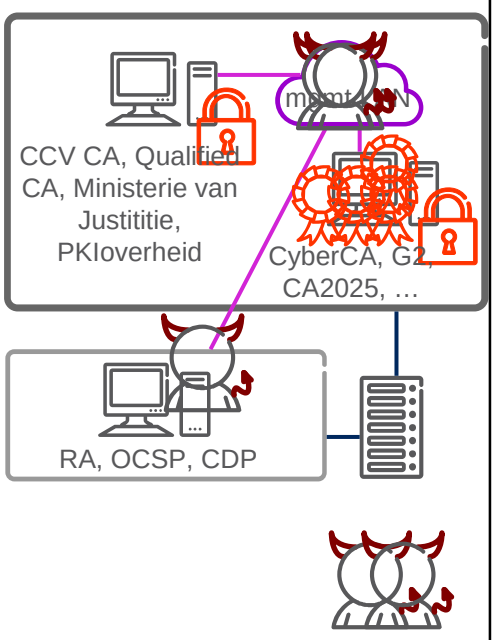
- 2011.08.31 Chrome update
- 2011.09.03 Mozilla, Chrome update
- 2011.09.04 Microsoft update
- 2011.09.06-07: comodohacker pastebin
- 2011.09.12. Holland elektronikus közszolgáltatást leállították mert még mindig a kompromittált CA tanúsítványt használták
- 300 000 IP cím, többnyire Iráni, amely nem iráni, az nagyrészt TOR
- 2011.09.09 Globalsign CA: külső web szerver feltörve (comodohacker)
- 2011.11.04 Diginotar users migrate to KPN,
  - DDoS programmok régóta fel lettek telepítve

- Hamis tanúsítványok (531)

- ```
  *.android.com
  *.aol.com
  *.globalsign.com
  *.google.com
  *.microsoft.com
  *.mossad.gov.il
  *.mozilla.org
  *.skype.com
  *.thawte.com
  *.torproject.org
  *.windowsupdate.com
  addons.mozilla.org
  DigiCert Root CA
  Equifax Root CA
  GlobalSign Root CA
  login.live.com
  login.yahoo.com
  Thawte Root CA
  twitter.com
  VeriSign Root CA
  www.cia.gov
  www.facebook.com
  www.google.com
  www.mossad.gov.il
  www.sis.gov.uk
  www.update.microsoft.com
  ```


DIGINOTAR
A FELTÉTELEZETT TÁMADÁS

- Felderítés
- DMZ-ben lévő szerverek elfoglalása
- Betörés menedzsment rendszeren keresztül
  - FoxIT: Operation Black Tulip 1.0 Sept5,2011
    „We have strong indications that the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the Management LAN.„
- Első kísérlet tanúsítvány készítésére
- tanúsítványok készítése, mely a későbbi támadások alapja
- Cain&Abel:
  - Windows based password recovery tool,
  - Hálózatmonitorozás, brute force támadás
- Konklúzió:
  - Több, mint egy hónapig érvényes volt a tanúsítvány
  - Ellenőrizni az érvényességét kell
  - Iráni támadók képesek voltak google accountokat feltörni, jelszavakat és levelezést megszerezni


  ```

ÖSSZEGZÉS

- Támadások száma növekszik
- Egyre motiváltabb, jobb képességű, nagyobb erőforrással rendelkező támadók
- Kritikus infrastruktúrák is áldozatul esnek
- Távközlés és azon belül Menedzsment rendszer is kritikus infrastruktúra
- Menedzsment rendszer Biztonsági szolgáltatásokat is nyújt
- Menedzsment rendszer értékeket kezel
- Alapvetően fontos a megfelelő védelem