IT biztonság

2018/2019 tanév

Tartalomjegyzék

A kriptográfiai sérülékenységek („ethical hacking”)

A kriptográfia alkalmazásához (fejlesztéshez , üzemeltetéshez) alaposabb tudásra van szükség. Ehhez érdemes mások hibáit is megvizsgálni, hogy tanulni lehessen belőlük.

Ethical hacking

```
BLOWFISH (BSD):
                    $2a$07$kiuhgfslerd...........6k0kSI76CqJ/RWGnSp9MWRDF91gJZfw
                    //John the Ripper
                    //pl. salt="kiuhgfslerd...........", password="mypassword"

MD5 (Apache, BSD):
                    $apr1$zzzzzzzz$rxLW/SrarDA49keyZN1Y..
                    //openssl passwd -apr1 -salt string -in input_file.txt
                    //pl. salt="zzzzzzzz", password="abcd1234"

MD5 (BSD):
                    $1$zzzzzzzz$jWwdEbSnqF.oBvMFCGNHg/
                    //John the Ripper
                    //openssl passwd -1 -salt string -in input_file.txt
                    //pl. salt="zzzzzzzz", password="abcd1234"

DES (Unix):
                    zzG5YscX99Vvs
                    //John the Ripper
                    //openssl passwd -crypt -salt string -in input_file.txt
                    //pl. salt="zz", password="abcd1234"

MD5 (raw):
                    e19d5cd5af0378da05f63f891c7467af
                    //openssl dgst -md5 -hex input_file.txt
                    //pl. password="abcd1234"

MD4 (raw):
                    15c8a6dc3061129d08757ab5f2991689
                    //openssl dgst -md4 -hex input_file.txt
                    //pl. password="abcd1234"

MySQL pre-v4.1:
                    335f5a824b3ba309
                    //old_password('abcd1234')
                    //pl. password="abcd1234"

MySQL:
                    *4ad47e08dae2bd4f0977eed5d23dc901359df617
                    //password('abcd1234')
                    //pl. password="abcd1234"

NTLM:
                    b3ec3e03e2a202cbd54fd104b8504fef
                    //John the Ripper
                    //pl. password="abcd1234"
```

Jelszavak tárolása, megfejtése

az MD5 előtt alapértelmezettként DES algoritmust használtak, az OpenBSD pedig képes Blowfish algoritmussal kódolva is tárolni a jelszavakat

a John the Ripper „dictionary attack” és „brute force” támadás esetén is figyelembe veszi a „salt” értékeket és kezeli a Blowfish algoritmust is

a GI John (GRID Implemented John elosztott jelszótörés)

a Ravan (AndLabs HTML5 GRID jelszótörés)

Ethical hacking

```
BLOWFISH (BSD)

   without NUL
   59 bytes = $2$ + 2 bytes + $ + 22 bytes + 31 bytes
   salt     = $2$ + 2 bytes + $ + 22 bytes
   cost     = 2 bytes (between 04 and 12)
    2 bytes = 2^cost number of rounds
   22 bytes = base64(128 bits = 16 bytes salt)
   31 bytes = base64(184 bits = 23 bytes data)

   with NUL
   60 bytes = $2a$ + 2 bytes + $ + 22 bytes + 31 bytes
   salt     = $2a$ + 2 bytes + $ + 22 bytes
   cost     = 2 bytes (between 04 and 12)
    2 bytes = 2^cost number of rounds
   22 bytes = base64(128 bits = 16 bytes salt)
   31 bytes = base64(184 bits = 23 bytes data)

MD5 (Apache, BSD)

   Apache variant of the BSD algorithm (OpenSSL)

   37 bytes = $apr1$ + 8 bytes + $ + 22 bytes
   salt     = $apr1$ + 8 bytes + $
    8 bytes = base64( 48 bits =  6 bytes salt)
   22 bytes = base64(128 bits = 16 bytes data)

MD5 (BSD)

   MD5 based BSD password algorithm (OpenSSL)

   34 bytes = $1$ + 8 bytes + $ + 22 bytes
   salt     = $1$ + 8 bytes + $
    8 bytes = base64( 48 bits =  6 bytes salt)
   22 bytes = base64(128 bits = 16 bytes data)
```

```
DES (Unix)

   standard Unix password algorithm

   13 bytes =  2 bytes + 11 bytes
   salt     =  2 bytes
   11 bytes = base64( 64 bits =  8 bytes data)


MD5 (raw)

   32 bytes = hex(128 bits = 16 bytes)

MD4 (raw)

   32 bytes = hex(128 bits = 16 bytes)

MySQL

   MySQL vX.X < v4.1
   16 bytes = hex( 64 bits =  8 bytes)

   MySQL v4.1
   41 bytes = * + 40 bytes
   40 bytes = hex(160 bits = 20 bytes)

NTLM

   14 bytes = UpperCasePassword(password) + N bytes of 0
   14 bytes = 7 bytes (DES#1) + 7 bytes (DES#2)
   cipher#1 = DES#1("KGS!@#$%")
   cipher#2 = DES#2("KGS!@#$%")
   16 bytes = cipher#1 + cipher#2
   32 bytes = hex(128 bits = 16 bytes)
```

Ethical hacking

Jelszavak törése

a John the Ripper segítségével szótár („dictionary”, „wordlist”) alapján

jól kell megválasztani a szógyűjteményt (magyar, angol?)

```
C:\WINDOWS\system32\cmd.exe

F:\John>john-mmx.exe -wordlist=hungarian.dic -format=MD5 passwd_MD5.txt
Loaded 26 password hashes with 26 different salts (FreeBSD MD5 [32/32])
guesses: 0  time: 0:00:01:40 100%  c/s: 4635  trying:

F:\John>john-mmx.exe -wordlist=english.dic -format=MD5 passwd_MD5.txt
Loaded 26 password hashes with 26 different salts (FreeBSD MD5 [32/32])
code             (user2)
devil            (user3)
evil             (user4)
funny            (user5)
gogo             (user6)
honey            (user7)
java             (user9)
king             (user10)
lover            (user11)
metal            (user12)
noop             (user13)
ogre             (user14)
peace            (user15)
quit             (user16)
runner           (user17)
satan            (user18)
teen             (user19)
unique           (user20)
valid            (user21)
wow              (user22)
yummy            (user24)
guesses: 21  time: 0:00:15:48 100%  c/s: 4560  trying: zythum

F:\John>_
```

```
C:\WINDOWS\system32\cmd.exe

F:\John>john-mmx.exe -wordlist=hungarian.dic -format=DES passwd_DES.txt
Loaded 26 password hashes with 26 different salts (Traditional DES [64/64 BS MMX
])
guesses: 0  time: 0:00:00:00 100%  c/s: 559340  trying: zsolt 8

F:\John>john-mmx.exe -wordlist=english.dic -format=DES passwd_DES.txt
Loaded 26 password hashes with 26 different salts (Traditional DES [64/64 BS MMX
])
code             (user2)
devil            (user3)
evil             (user4)
funny            (user5)
gogo             (user6)
honey            (user7)
java             (user9)
king             (user10)
lover            (user11)
metal            (user12)
noop             (user13)
ogre             (user14)
peace            (user15)
quit             (user16)
runner           (user17)
satan            (user18)
teen             (user19)
unique           (user20)
valid            (user21)
wow              (user22)
yummy            (user24)
guesses: 21  time: 0:00:00:05 100%  c/s: 570022  trying: zymosthe - zythum
```

a 26 jelszó lenyomatból 21 volt törhető szótár alapján

DES: 00:05 [min:sec]
MD5: 15:48 [min:sec]

Rainbow table („salt” ellen nem jó)

Ethical hacking

```
C:\WINDOWS\system32\cmd.exe

F:\John>john-mmx.exe -incremental=all -format=DES passwd_DES.txt
Loaded 26 password hashes with 26 different salts (Traditional DES [64/64 BS MMX
])
metal            (user12)
teen             (user19)
abcd             (user0)
peace            (user15)
wow              (user22)
xyz              (user23)
code             (user2)
guesses: 7  time: 0:00:00:30  c/s: 275933  trying: muccol - m1sa98
Session aborted

F:\John>john-mmx.exe -incremental=all -format=MD5 passwd_MD5.txt
Loaded 26 password hashes with 26 different salts (FreeBSD MD5 [32/32])
metal            (user12)
guesses: 1  time: 0:00:00:30  c/s: 3975  trying: moodlan
Session aborted

F:\John>
```

```
# Incremental modes
[Incremental:All]
File = $JOHN/all.chr
MinLen = 0
MaxLen = 8
CharCount = 95

[Incremental:Alpha]
File = $JOHN/alpha.chr
MinLen = 1
MaxLen = 8
CharCount = 26

[Incremental:Digits]
File = $JOHN/digits.chr
MinLen = 1
MaxLen = 8
CharCount = 10

[Incremental:Alnum]
File = $JOHN/alnum.chr
MinLen = 1
MaxLen = 8
CharCount = 36

[Incremental:LanMan]
File = $JOHN/lanman.chr
MinLen = 0
MaxLen = 7
CharCount = 69
```

Jelszavak törése

a John the Ripper segítségével „brute-force” alapján

2009-07-08: IGHASHGPU (Ivan Golubev)

- **ATI Radeon HD4850: 955 M/s MD5, 305 M/s SHA-1**
- **nVidia GeForce GTX 260 192SP: 533 M/s MD5, 166 M/s SHA-1**
- **ATI Radeon 5970: Oracle DES/SHA-1 jelszó (csak kisbetűk – 26)**

8 karakter:	**DES – 10 óra**	**SHA-1 – 4,6 perc**
10 karakter:	**DES – 283 nap**	**SHA-1 – 2 nap**

Ethical hacking

ATI Radeon HD 69XX series (VLIW4)

GPU Name	SP/ALU count	Clock rate	Peak perf. with integers	Single MD5 speed	Single SHA1 speed	MS Office 2007 speed	WinZip/AES speed	WPA speed	SL3 unlock time	Price	SHA1 perf. per $
Radeon HD 6930	1280	750	960.00	3887M	1000M	19048	475715	58115	9d 11h	$180	**5.56**
Radeon HD 6950	1408	800	1126.40	4560M	1173M	22349	558172	68188	8d 1h	$245	4.79
Radeon HD 6970	1536	880	1351.68	5472M	1408M	26819	669806	81825	6d 17h	$360	3.91
Radeon HD 6990	3072	830	2549.76	10323M	2656M	50590	1263498	154352	3d 13h	$700	3.79

AMD Radeon HD GCN series

GPU Name	SP/ALU count	Clock rate	Peak perf. with integers	Single MD5 speed	Single SHA1 speed	MS Office 2007 speed	WinZip/AES speed	WPA speed	SL3 unlock time	Price	SHA1 perf. per $
Radeon R9 290	2560	947	2424.32	9815M	2525M	48102	1201338	146759	3d 17h	$399	**6.33**
Radeon R9 290X	2816	1000	2816.00	11401M	2933M	55873	1395430	170469	3d 5h	$549	5.34
Radeon R9 295X2	5632	1018	5733.38	23212M	5972M	113757	2841095	347075	1d 14h	$1499	3.98

nVidia GeForce G80-2XX series (SM 1.0-1.3)

GPU Name	SP/ALU count	Clock rate	Peak perf. with integers	Single MD5 speed	Single SHA1 speed	MS Office 2007 speed	WinZip/AES speed	WPA speed	SL3 unlock time	Price	SHA1 perf. per $
Tesla S1070 400	960	1296	1244.16	3027M	915M	17425	435195	53165	12d 15h	$8000	0.11
Tesla S1070 500	960	1440	1382.40	3364M	1016M	19361	483550	59072	11d 9h	$9000	0.11

nVidia GF100 series (SM 2.0/Fermi)

GPU Name	SP/ALU count	Clock rate	Peak perf. with integers	Single MD5 speed	Single SHA1 speed	MS Office 2007 speed	WinZip/AES speed	WPA speed	SL3 unlock time	Price	SHA1 perf. per $
GeForce GTX590	1024	1215	1244.16	3363M	1054M	20083	501581	61274	10d 23h	$699	1.51
Tesla S2050	1792	1150	2060.80	5570M	1746M	33266	830808	101494	6d 15h	$14000	0.12

Ivan Golubev

- **http://www.golubev.com/gpuest.htm (from archive)**

Ethical hacking

Software eszközök:
kismet, aircrack-ng, NetStumbler

Hardware eszközök:
driver típusától függ

promiscuous mode:
nemcsak a keretek (frame), hanem a teljes csomag feldolgozásra kerül, azaz a címzett MAC címétől függetlenül minden forgalmat lát vezetékes és vezetéknélküli hálózatoknál is az eszköz, de csak ha csatlakozott (pl. adott SSID-hoz tartozó összes forgalom)

monitor mode (RFMON):
csatlakozás (association) nélkül is lát mindent

Driver	802.11	Bus interface	WEP	WPA	WPA2	Monitor mode
acx1xx	802.11b, 802.11g	PCI, Mini PCI, PC card, USB	Yes	No	No	Yes
adm8211	?	PCI	?	?	?	?
ath5k	802.11a, 802.11b, 802.11g	PCI, Mini PCI, PC card	Yes	Yes	Yes	Yes
ath9k	802.11a, 802.11b, 802.11g, 802.11n	PCI, Mini PCI, AHB	Yes	Yes	Yes	Yes
b43	802.11b, 802.11g	PCI, Mini PCI, ?	Yes	Yes	Yes	Yes
bcm43xx	802.11b, 802.11g	PCI, Mini PCI, PC card, Cardbus	Yes	Yes	Yes	Yes
hostap	802.11b	PCI, Mini PCI, PC card	Yes	Yes[45]	Yes[45]	Yes
ipw2100	802.11b	Mini PCI	Yes	Yes	?	Yes
ipw2200	802.11a, 802.11b, 802.11g	Mini PCI	Yes	Yes	Yes	Yes
ipw2200-ap	802.11b, 802.11g	Mini PCI	?	?	?	Yes
ipw3945	802.11a, 802.11b, 802.11g	Mini PCI, PCI Express Mini Card	Yes	Yes	Yes	Yes
islsm	?	PCI, USB	No	No	No	?
iwlwifi	802.11a, 802.11b, 802.11g	Mini PCI, PCI Express Mini Card	Yes	Yes	Yes	Yes
libertas	802.11b, 802.11g	USB, CF	?	?	?	?
MadWifi	802.11a, 802.11b, 802.11g	PCI, Mini PCI, PC card	Yes	Yes	Yes	Yes
orinoco	802.11b	Mini PCI, PC card	Yes	Yes[46]	No	Yes
p54	802.11b, 802.11g	Mini PCI, Cardbus, USB	Yes	Yes	Yes	Yes
prism54	802.11b, 802.11g	PCI	Yes	No	?	Yes
rt2x00	802.11b, 802.11g	PCI, Mini PCI, USB	Yes	Yes [47]	?	Yes
rtl8180	802.11a, 802.11b, 802.11g	PCI, Mini PCI, PC card	?	?	?	?
rtl-wifi	802.11a, 802.11b, 802.11g	PCI, Mini PCI, PC card	Yes	Yes	?	?
zd1201	802.11b	USB	Yes	No[48]	No[48]	Yes
zd1211	802.11a, 802.11b, 802.11g	USB	Yes	Yes	Yes	Yes
zd1211rw	802.11b, 802.11g	USB	Yes	Yes	Yes	Yes

Ethical hacking

```
root@ubuntu: /home/ubuntu/aircrack-ptw-1.0.0
File  Edit  View  Terminal  Tabs  Help
root@ubuntu:/home/ubuntu/aircrack-ptw-1.0.0# ./aircrack-ptw crack-01.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw
/
allocating a new table
bssid = 00:30:4F:3F:D5:EB  keyindex=0
stats for bssid 00:30:4F:3F:D5:EB  keyindex=0 packets=531765
Found key with len 13: 6E 61 67 79 6F 6E 75 67 79 65 73 21 21
root@ubuntu:/home/ubuntu/aircrack-ptw-1.0.0#
```

Jelszavak törése

WEP-kulcs törése:

- **aireplay**
  (kezdeti forgalom generálásához „deauthentication”)
  (felhasználó által elküldött „ARP request” csomagok visszajátszása)
- **airodump**
  (IV-k – „initialization vector” – gyűjtése, tárolása),
- **aircrack**
  (40/104 bites RC4 kulcs kitalálása + 24 bit IV)

Ethical hacking

Történet

- 2008-11-08: Martin Beck, Erik Tews (12-15 perc)
- 2009-08-27: Toshihiro Ohigashi, Masakatu Morii (1-4 perc)

WPA TKIP

- WEP továbbfejlesztése
- RC4 szimmetrikus algoritmus
- Michael algoritmusos Message Integrity Check (MIC) a CRC32 helyett
- TKIP Sequence Counter (TSC) számláló a visszajátszásos támadások ellen
- IV is ellenőrzésre kerül, nemcsak a ellenőrző-összeg

Támadás

- WEP ellen használt „chopchop” átírása
- MIC kulcs megfejtése kis csomagnál (pl. ARP)
- ha „nyílt szöveg – rejtjelezett szöveg” ismert, RC4 keystream is ismert
- ARP üzenetek kiküldése a kommunikáló feleknek (man-in-the-middle)

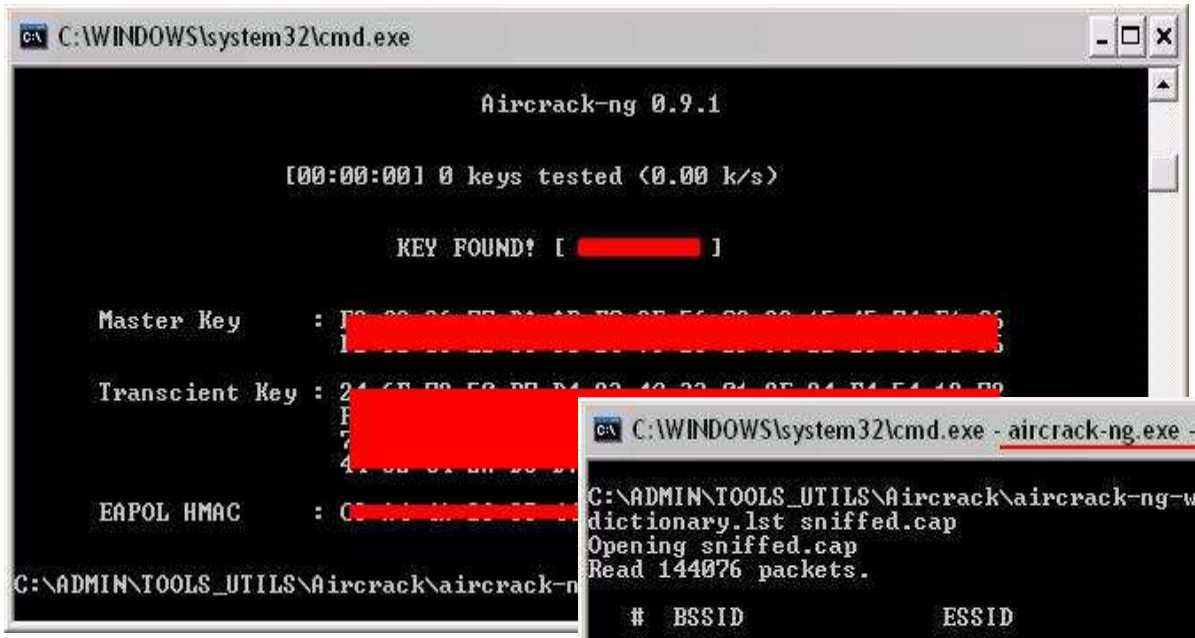
Megoldás

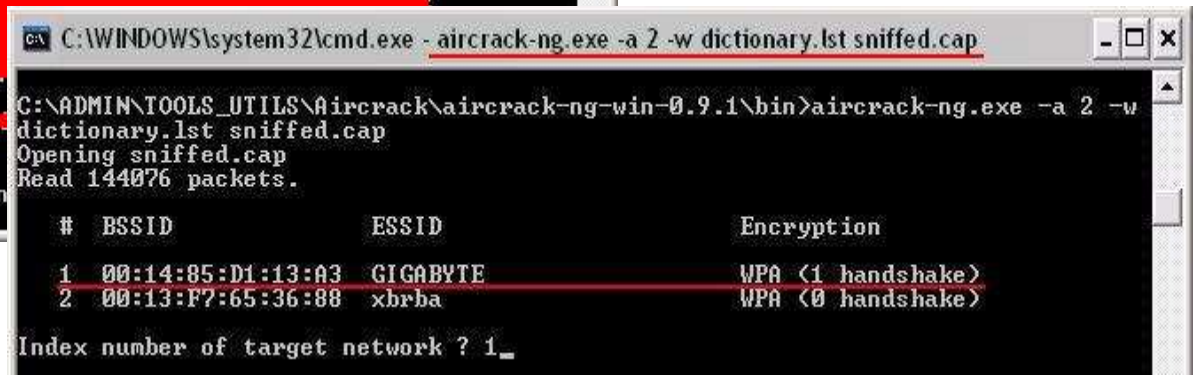
- A gyakoribb TKIP kulcsfrissítés sem elegendő, mindenképpen CCMP (AES az IETF RFC 3610 alapján) használata ajánlott!

Alkalmazás

- tkiptun-ng (forrás: http://www.aircrack-ng.org)

Ethical hacking



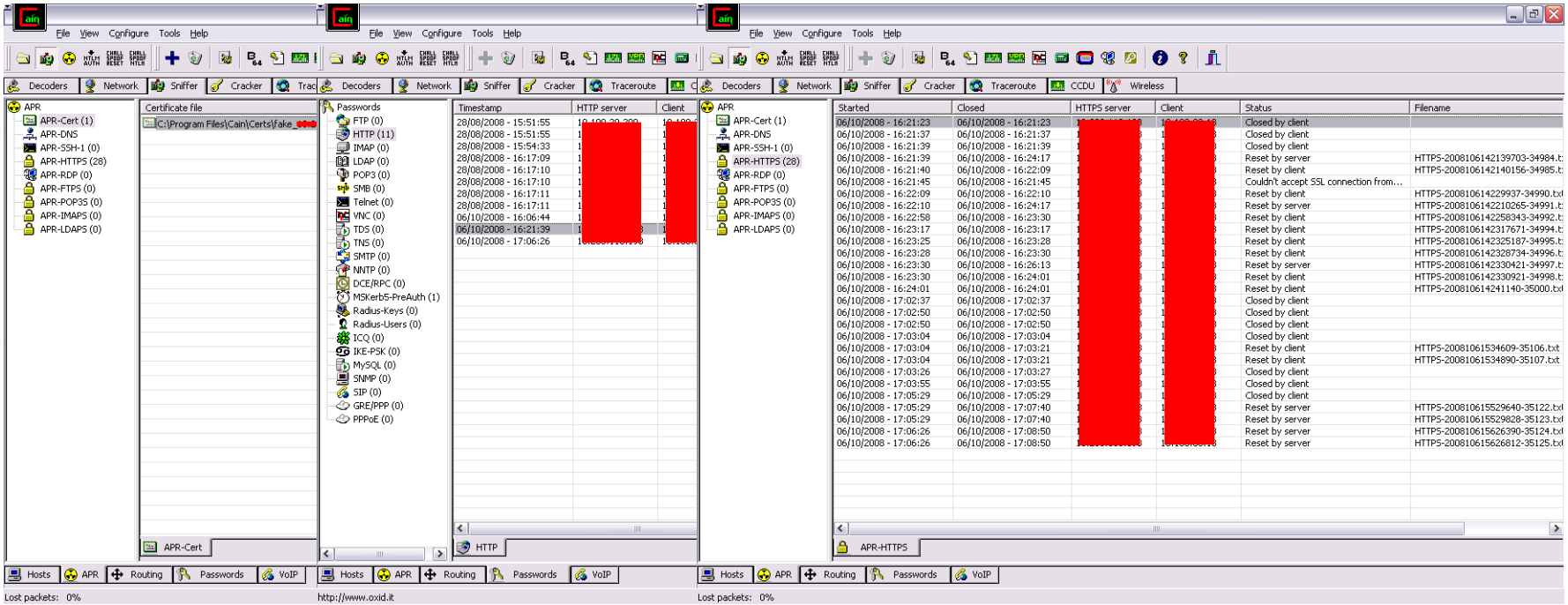


Jelszavak törése

WPA2-kulcs törése:

- **aireplay**
  - **(„ARP request” csomagok),**
- **airodump**
  - **(legalább 1 „handshake”),**
- **aircrack**
  - **(csak szótár alapján)**

Ethical hacking



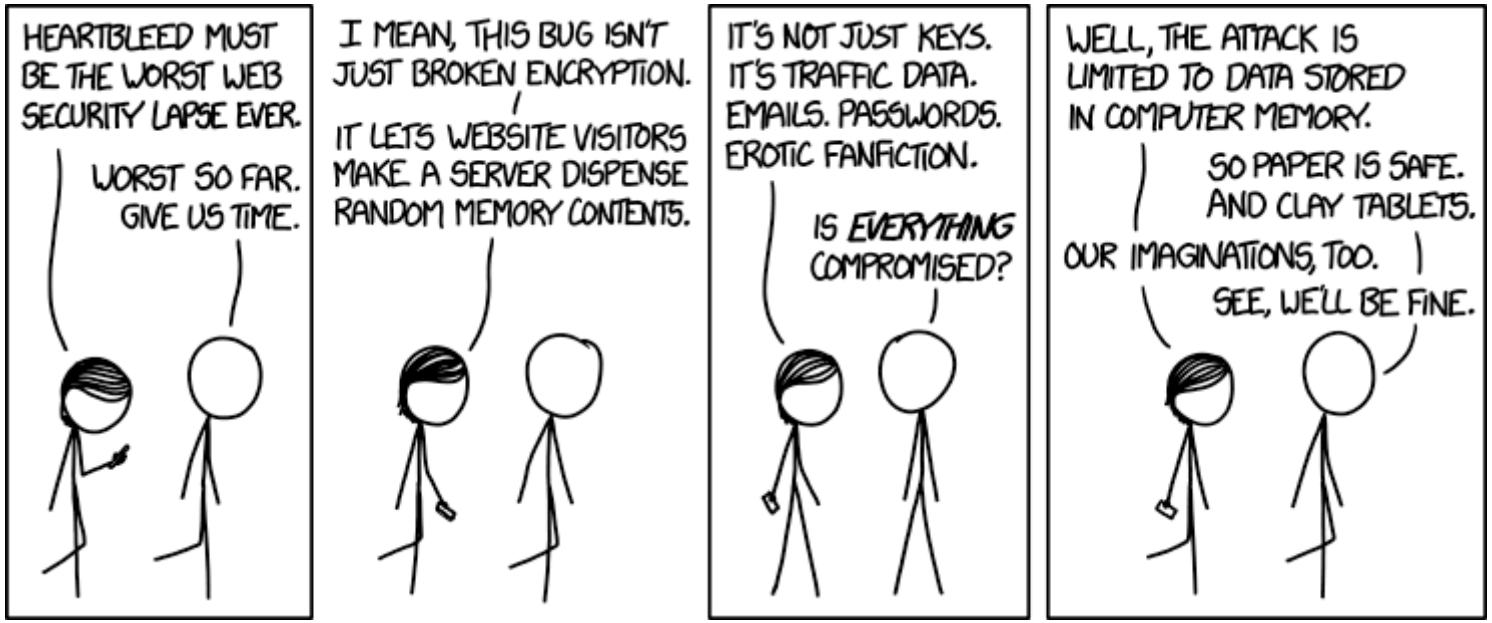
Jelszavak megszerzése - Cain&Abel (Windows), ettercap (Linux)

- **Man-in-the-Middle támadás HTTP/HTTPS(SSL/TLS)/SSH kapcsolatoknál is**
  - **sniffer aktiválása**
  - **alhálózaton host-ok felderítése**
  - **ARP poisoning elindítása**
  - **elcsípett csomagok elemzése**
- **kizárólag megbízható SSL/TLS szerver tanúsítványt szabad elfogadni**
- **ARP poisoning nélkül SSL/TLS: Fiddler2, chrome://net-internals**

Ethical hacking

kódvizsgálat és OpenSSL

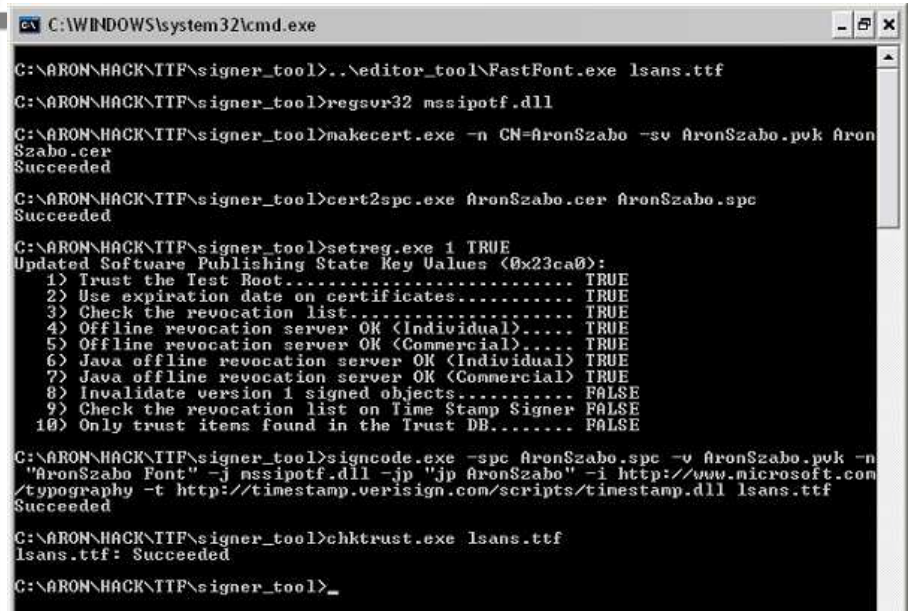
- OpenSSL: 2012-03-14 – 2014-04-07 (1.0.1 – 1.0.1g)
- IETF RFC 6520 Heartbeat Extension of TLS: OpenSSL bug (memory leak)
- a Heartbeat Extension engedélyezve van?
- a titkos kulcsot HSM tárolja a memória helyett?

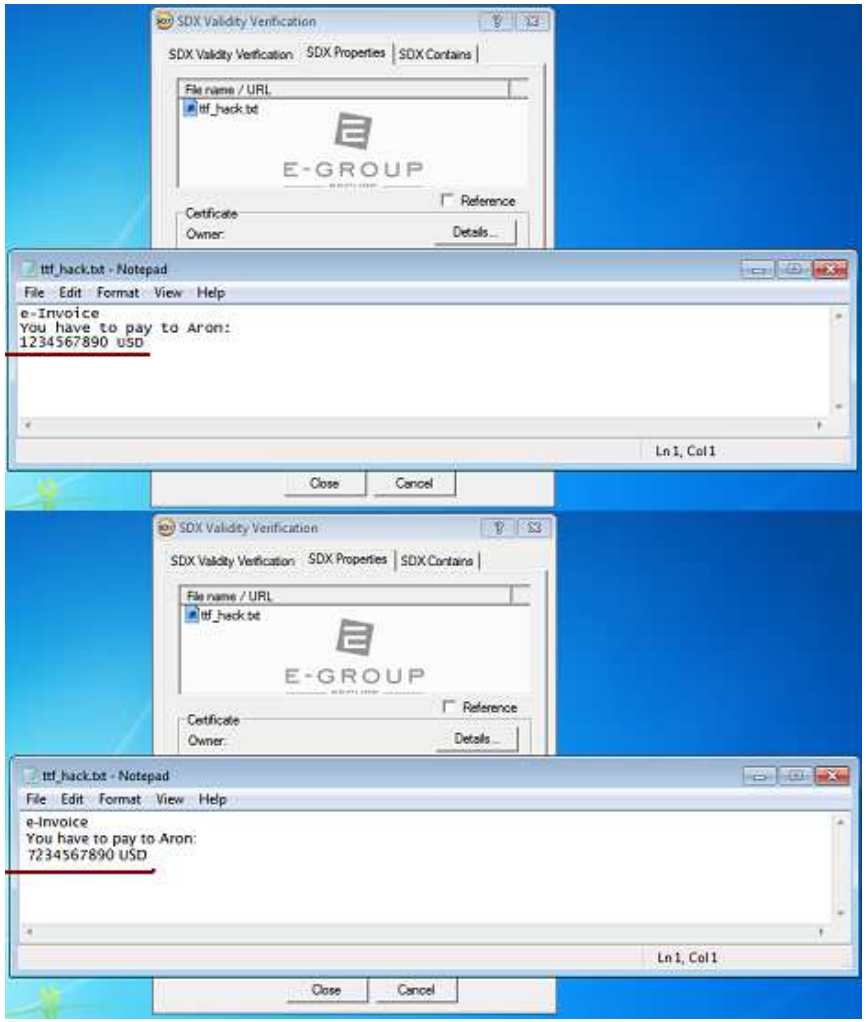


Ethical hacking

2011-04-01: **Windows betűkészletek**

A .ttf állományokon levő elektronikus aláírás ellenőrzése a Windows operációs rendszereken felületes: aláírásnak kell rajta lennie, de alapértelmezettként megbízhat tetszőleges aláíró tanúsítványban.



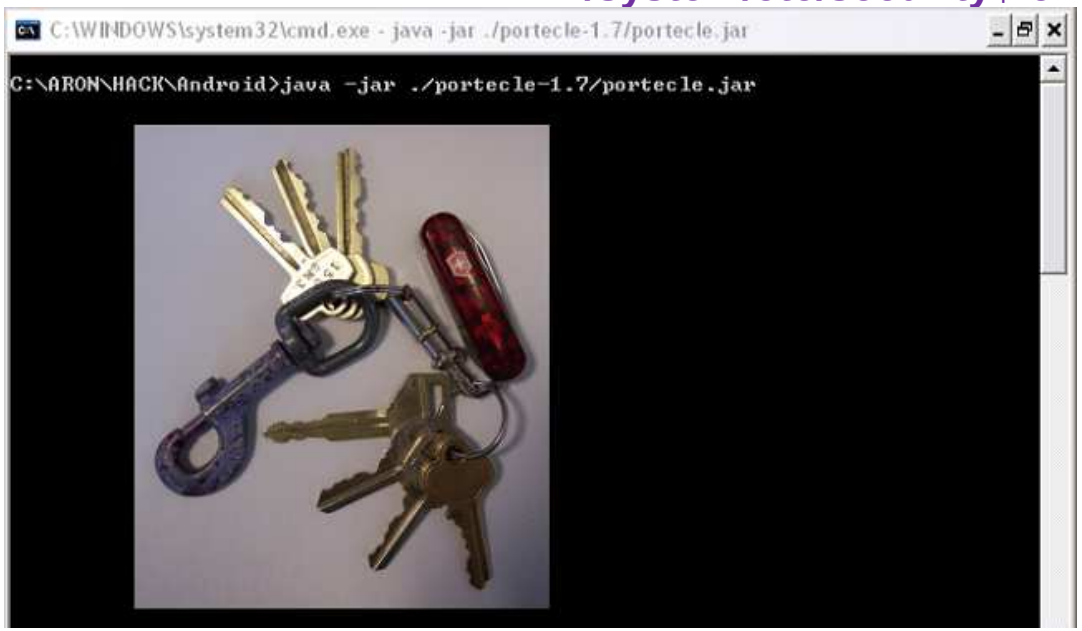


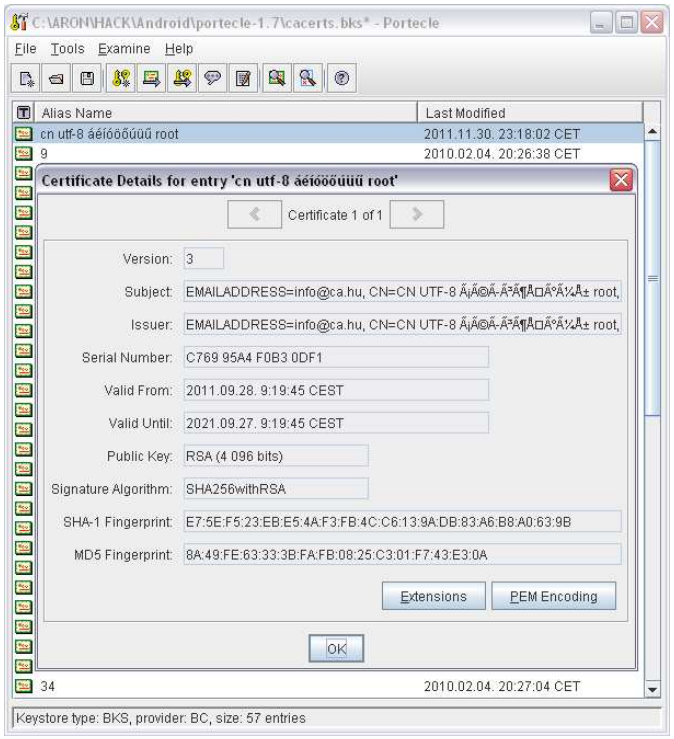
Ethical hacking

Az okostelefonoknál is fontos a tanúsítványtár elsősorban az SSL/TLS csatornák kezelése miatt (de néhol a code signer szabályok is ebből táplálkoznak).

Android root jogosultság: SuperOneClick
cacerts.bks szerkesztése: Portecle
cacerts.bks visszaírása: SSHDroid + WinSCP => console

/system/etc/security$ mount –w –o remount /dev/stl12 /system
/system/etc/security$ chmod 755 cacerts.bks





Ethical hacking

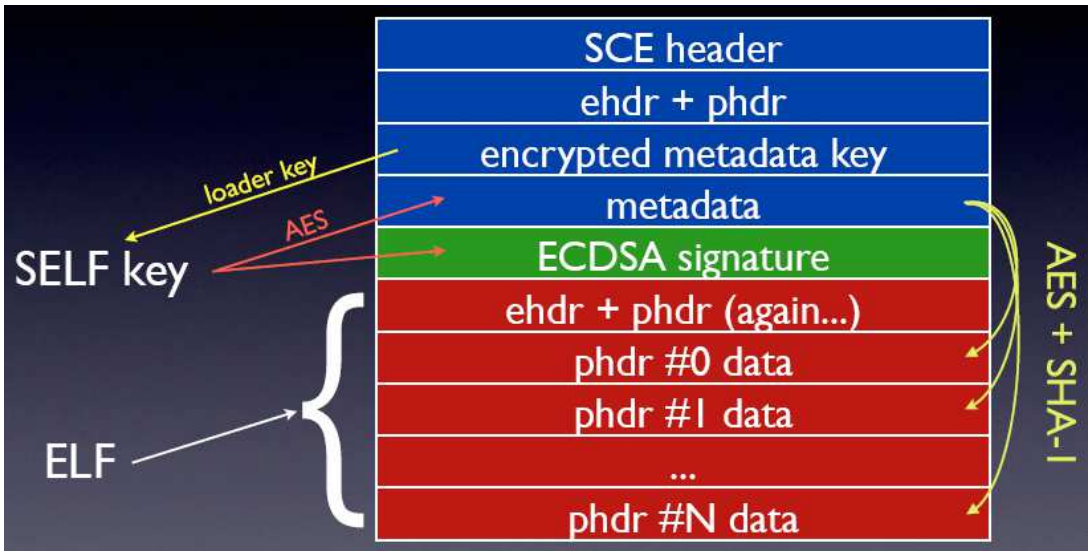
2010-12-29: **fail0verflow (27. Chaos Communication Conference)**

saját ECDSA implementáció kriptográfiai tudás nélkül: a titkos kulcs két komponense közül az egyik (random number) be volt égetve

=> két különböző aláírásból meghatározható a titkos kulcs másik értéke is

=> bárki tud aláírt alkalmazásokat futtatni Sony PlayStation3 eszközön

http://www.youtube.com/watch?v=4loZGYqaZ7I




```
public parameters:
p, a, b, G, N: elliptic curve parameters
Q: public key
e: hash of data
R,S: signature

private parameters:
m: random number
k: private key

R1 = m1G
S1 = (e1 + kR1) / (m1)

R2 = m2G
S2 = (e2 + kR2) / (m2)

R1 = R2
m1 = m2
S1 <> S2

(S1 - S2) = (e1 - e2) / (m)
(m) = (e1 - e2) / (S1 - S2)
(k) = (mS1 - e1) / (R) = (mS2 - e2) / (R)

    |
    v

(k) = (e1S2 - e2S1) / ((S1 - S2) (R))
```

Ethical hacking

2011-03-18: RSA Inc. – RSA SecurID

célzottan kiküldött e-mailek, csatolmányban Excel-tábla, benne 0-day Flash exploit megnyitáskor telepítette a Poison Ivy (Remote Administration Tool) alkalmazást

=> Az RSA SecurID titkos kulcs „seed”-ek kikerültek

=> illetéktelen behatolások a Lockheed Martin cégnél is

```
HOTP: An HMAC-Based One-Time Password Algorithm
http://www.ietf.org/rfc/rfc4226.txt

        HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

TOTP: Time-Based One-Time Password Algorithm
http://www.ietf.org/rfc/rfc6238.txt

        TOTP(K,T) = Truncate(HMAC-SHA-1(K,T))
        TOTP(K,T) = Truncate(HMAC-SHA-256(K,T))
        TOTP(K,T) = Truncate(HMAC-SHA-512(K,T))
```