2011-11-24, Kõltsu

Usaldusteenuste roll Euroopas

Anto Veldre, CERT-EE

Tisklaimer

sertifitseerimine?

Dumas, “Kolm musketäri”:

“Selle paberi ettenäitaja toimis minu loal ja Prantsusmaa huvides..."

X.509

http://en.wikipedia.org/wiki/X.509

- Specification: Complexity and lack of quality
- Architectural flaws
- Problems of Commercial Certificate Authorities
- Implementation issues
- Exploits

Wikipedia: Problems of Commercial Certificate Authorities

* Flawed business model: The subject, not the relying party, purchases certificates. The RA will usually go for the cheapest offer; quality is not being paid for in the competing market.

* CAs deny almost all warranties to the user.

* Expiration date: Should be used to limit the time the key strength is deemed sufficient. Abused by CAs to charge the client an extension fee. Places unnecessary burden on user with key roll-over.

* Client certificates have zero protection value against dedicated attackers.

* In browsers, the security is that of the weakest CA. There are very weak CAs.

* "Users use an undefined certification request protocol to obtain a certificate which is published in an unclear location in a nonexistent directory with no real means to revoke it."

Wikipedia: HTTPS

The trust inherent in HTTPS is based on major certificate authorities that come preinstalled in browser software (this is equivalent to saying "I trust certificate authority (e.g. VeriSign/Microsoft/etc.) to tell me whom I should trust"). Therefore an HTTPS connection to a website can be trusted if **and only** if all of the following are true:

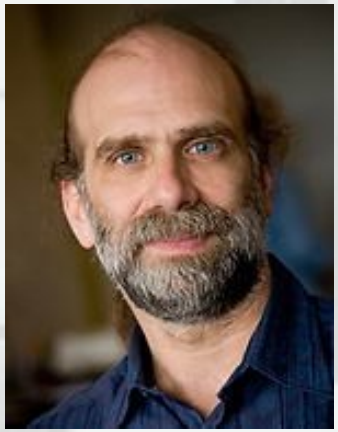
1. The user trusts that their browser software correctly implements HTTPS with correctly pre-installed certificate authorities.
2. The user trusts the certificate authority to vouch only for legitimate websites without misleading names.
3. The website provides a valid certificate, which means it was signed by a trusted authority.
4. The certificate correctly identifies the website (e.g., when the browser visits "https://example.com", the received certificate is properly for "Example Inc." and not some other entity).
5. Either the intervening hops on the Internet are trustworthy, or the user trusts that the protocol's encryption layer (TLS/SSL) is sufficiently secure against eavesdroppers.

Tähtsusetu sündmus

2010-04-12 Bruce Schneier

http://www.schneier.com/blog/archives/2010/04/man-in-the-midd_2.html

Packet Forensics LI-5B



Kõrvalepõige: Tuneesia jõulud

2011-01-24 – Tuneesia valitsus vs FaceBook

http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/

Bushehr: seest siiruviiruline...

Kes? Kus?

1909 – 9. mai 1979

Richelieu?
ei.
Realtek.

Tappa Buckinghami hertsogit?
ei.
“Draiverite” install
“turvalisse” OS'i.

Hsinchu Science Park, Taiwan

StuxNet

2010-09-26 - Rikkis pesumasina juhtum

- Realtek'i sertifikaat
- MS10-046, MS10-061, MS10-073, MS08-67
- magic_code = 19790509 -> 09. mai 1979

http://securitywatch.pcmag.com/hacking/283870-certificate-used-to-code-sign-malware-was-expired

http://threatpost.com/en_us/blogs/verisign-revokes-certificate-used-sign-stuxnet-malware-071710

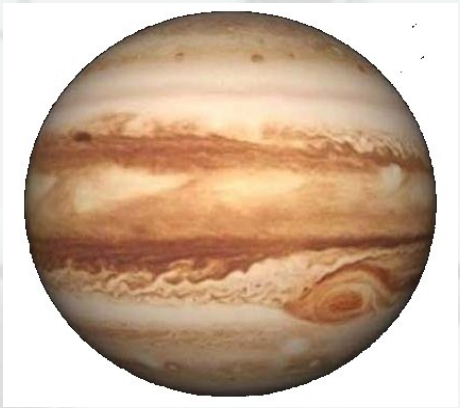
http://www.infosecurity-us.com/view/15331/ny-times-stuxnet-was-a-usisraeli-effort-to-disrupt-irans-nuclear-program/

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&pagewanted=all

Quod licet Jovi ...

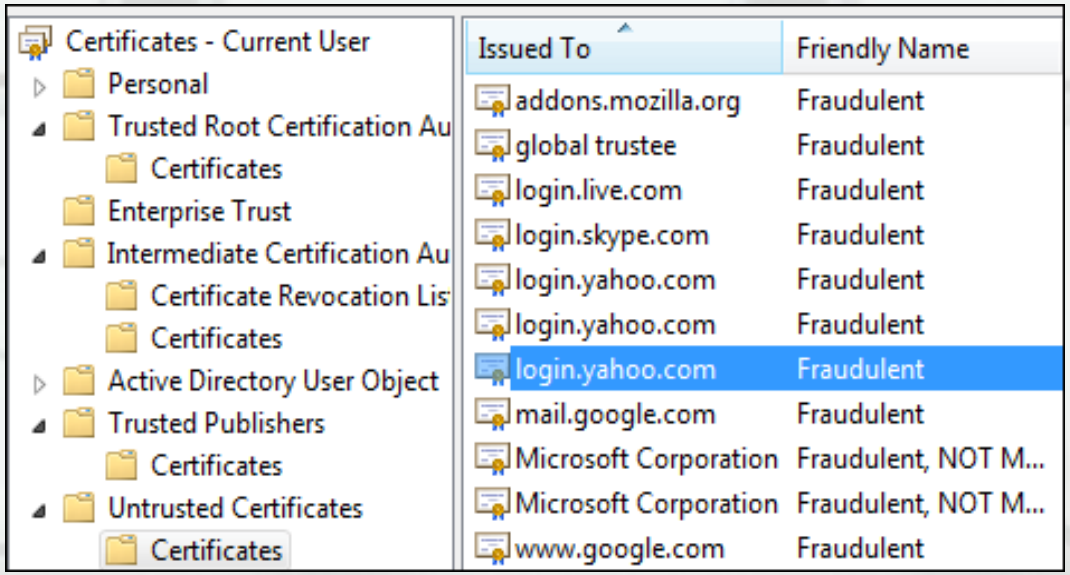
Packet Forensics LI-5B

=?



Comodo

2011-03-24 Microsoft CRL:



- "Global Trustee"

http://nakedsecurity.sophos.com/2011/03/24/fraudulent-certificates-issued-by-comodo-is-it-time-to-rethink-who-we-trust/

https://www.infosecisland.com/blogview/12679-Comodo-Fingers-Iranian-Hackers-in-Digital-Certificate-Heist.html

http://www.net-security.org/secworld.php?id=10788

Pilt © F-Secure blogist

2011-07-10

Autasustatute nimekiri

2011-09-04

"2011-07-10 21:36:31","9d69f4c1849361c63933f08de899b145","DigiNotar Extended Validation CA","unknown","unknown","*.azadegi.com","CN=twitter.com,SN=PK000229200018,OU=DN: CN=*.azadegi.com,TITLE=Shoghale Ahmagh Farari,SN=PK000229200017,OU=Israeli Lizard,L=Mazar sharif,O=Sage Pasokhteye Mozdur,C=IL,L=Mazar sharif,O=Sage Pasokhteye Mozdur,C=IL"

Pärsia -> inglise sõnastik

- Sahebeh Donya => Possessor of the World e.g. God.
- Sarbazeh Gomnam => Unknown Soldier
- Elme Bikaran => Science/Knowledge of the idle/unemployed
- Daneshmande Bi nazir => Peerless Scientist
- RamzShekaneBozorg => Great Cryptanalyst
- Toro Ham Mishkanam => I will breakTOR too
- Hameye Ramzaro Mishkanam => Will break all cyphers

DigiNotar

..com

..org

*.10million.org

*.android.com

...

*.comodo.com

*.digicert.com

*.globalsign.com

*.google.com

...

www.mossad.gov.il

www.sis.gov.uk

www.update.microsoft.com

Comodo Root CA

CyberTrust Root CA

DigiCert Root CA

DigiCert Root CA

Equifax Root CA

Equifax Root CA

GlobalSign Root CA

Thawte Root CA

VeriSign Root CA

Must tulp

http://www.youtube.com/watch?v=wZsWoSxxwVY

~600 võlts-sertifikaati tunnistatud kehtetuks

DigiNotar: kohustusliku kirjanduse loetelu

http://blog.trendmicro.com/diginotar-iranians-the-real-target/

https://blog.torproject.org/blog/diginotar-damage-disclosure

http://www.securelist.com/en/blog/208193111/Why_Diginotar_may_turn_out_more_important_than_Stuxnet

http://www.telegraph.co.uk/technology/news/8411252/Iranian-hacker-claims-revenge-for-Stuxnet.html

http://isc.sans.edu/diary.html?storyid=11512&rss

http://www.pcpro.co.uk/news/security/369703/iranian-hacker-claims-access-to-four-more-cas

http://www.f-secure.com/weblog/archives/00002231.html

http://uscyberlabs.com/blog/2011/09/16/diginotar-ssl-hack-diagram/

DigiNotari õppetunnid

* Viivitus kehtetukstunnistamisega, sest
  - riigiportaalide sertifikaadid
  - riigiametite serverite sertifikaadid
  - tuli süüa oma esialgseid sõnu sissemurdmise kohta
* "a driver signed with a certificate during its validity period will never expire. That the signing certificate is now expired is irrelevant because the rootkit was signed when the certificate was valid."
  http://nakedsecurity.sophos.com/2010/07/20/certified-uncertainty/
* Üldine usalduskriis

http://www.businesscomputingworld.co.uk/the-diginotar-hack-compromises-the-security-of-millions-of-internet-users/

* arutelu "seadusliku vahendusründe" lubatavast ulatusest

Jaht jätkub

2011-06-21 **StartSSL**. .il

Eddy Nigg, StartCom'i CTO & COO ütles:

privaat võti **EI ASUNUD** Internetiga ühendatud arvutis, häkkerid sellele ligipääsu ei saanud ega ühtegi sertifikaati ei genereerinud.

http://www.theregister.co.uk/2011/06/21/startssl_security_breach/

JMicron

2011-07-17 – Stuxneti senitundmatu versioon

Sertifikaat - JMicron Technology Corp, **Hsinchu Science Park, Taiwan**.

http://blog.eset.com/2010/07/19/win32stuxnet-signed-binaries

Edasised arengud

2011-09-02 GlobalSign peatas ajutiselt tegevuse

http://www.theregister.co.uk/2011/09/12/globalsign_security_breach/

2011-11-06 KPN peatas ajutiselt sertifikaatide genereerimise seoses **sissemurdmisega** serveritesse

http://www.h-online.com/security/news/item/Certificate-issuing-stopped-at-KPN-after-server-break-in-discovered-1372339.html

2011-11-14 **anjungnet.mardi.gov.my** (Malaisia Põllumajanduse uurimise Instituut) RSA-512 cert

http://www.theregister.co.uk/2011/11/14/stolen_certificate_discovered/

http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/

ja sellega seonduv viirus

http://www.computerworlduk.com/news/security/3318371/virus-cloaked-with-security-certificate-found-by-f-secure/

RSA512 tegurdatav?

2011-11-10 Microsoft Security Advisory (2641690),

- 22 sertifikaati DigiCert Sdn. Bhd, .my

http://technet.microsoft.com/en-us/security/advisory/2641690

2011-11-21 – RSA-512 sertifikaadid hoopiski tegurdatud, mitte varastatud ega genereeritud?

http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/

Praktiliselt kõigi nende sertifikaatide puhul on leitud neid ärakasutav viirus:

* skillsforge.londonmet.ac.uk (Cybertrust)
* agreement.syniverse.com (GlobalSign Inc)
* www.esupplychain.com.tw (TAIWAN-CA.COM Inc.)
* ahi.anthem.com (Anthem Inc) .....

Hiljutine uudis

2011-11-12 Sejil-2 rakett plahvatas stardieelsel testil

http://www.theblaze.com/stories/report-iran-revolutionary-guard-commander-killed-in-explosion-was-testing-intercontinental-missile/

36 ohvitseri surnud

Stuxnet süüdi ?

http://www.debka.com/article/21496/

Kohustuslik kirjandus

Man in the Middle

http://files.cloudprivacy.net/ssl-mitm.pdf või http://files.cloudprivacy.net/ssl-mitm.pdf

SSL is broken? - kas ja kuipalju täpselt?

http://cryptome.org/0005/ssl-broken.htm

Access: An Access Policy Brief ...

https://s3.amazonaws.com/access.3cdn.net/e6130dacde804482e7_xvm6iigk1.pdf

US versus Euroopa

* Võtmeküsimuseks on **usaldus** riigi ja valitsuse vastu

STORK - https://www.eid-stork.eu/

USA mudel:

- “McDonaldsi kliendikaardiga autendin FaceBook'is”

Euroopa mudel:

- usaldust ja identiteete jagab riik

Apple: SIM kaart või mitte-SIM-kaart või SIM-mittekaart?

http://www.ft.com/cms/s/0/db917464-f344-11df-a4fa-00144feab49a.html#axzz1eQWp6YP8

http://www.zdnet.com/blog/btl/apples-master-sim-card-plan-brilliant-abroad-us-may-not-fly/41002

Kes keda?

OS (vahel ka brauseri tootja) on alati paremal positsioonil kui arvutikasutaja või 3-nda osapoole tarkvara.

Rutkowska printsiip:

http://theinvisiblethings.blogspot.com/2011/04/why-us-password-revolution-wont-work.html

..the operating system can impersonate the user at will! This is because the operating system fully controls the keyboard, the mouse, and the screen.

APT

Advanced Persistent Threat

http://www.arvutikaitse.ee/apt-jouliselt-ebamaarane-kuber-oht/

Muus osas aga ...

Eesti on endiselt ID-lahenduste esirinnas,

igapäevane elu läheb edasi,

poes on endiselt leiba ja piima,

Sertifitseerimiskeskus vunkab kenasti,

privaatvõtmeid hoitakse kindlas kohas

ja ID-kaart on jätkuvalt turvaline.

a.D. 2011

Tähh!

Küsida võib kõike!

materjal: xyz.ee /2011-11-24-sk/