

**1. crash course on securing web sites**  
**2. how is web site security practiced**  
**in internetland Holland**

*teus hagen* <[teus+ssl@theunis.org](mailto:teus+ssl@theunis.org)>

Competa/NLUUG  
Rijswijk, 21<sup>st</sup> of Sept 2011

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 2 to go

Hate mail to Teus Hagen <[noreply@theunis.org](mailto:noreply@theunis.org)> (not joking)

## content



- ◆ lessons to be learned from the physical key-lock world
- ◆ crash course on encryption, digital signatures and digital certificates
- ◆ internet land protection layers:
  - DNS, with DNSSEC the key to identify end points
  - SSL/TLS client and server security configuration
- ◆ SSL/TLS Assessments of Dutch web sites: status Nov 2010 – Sept 2011 one year later, and just after DigiNotar event of Aug 2011:
  - internet banks, governmental e-desks, academic e-desks,
  - e-commerce, health-care, security firms.
- ◆ found the web honeypot !!!
- ◆ three basic conclusions

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 5 to go

## Content

- development of locks in the real world
- encryption, hashing and certificates how they work  
the basic HowTo knowledge, example RSA
- DNSSEC status, statistics
- SSL/TLS what it is about
- amazing statistic figures,  
this does not make you make friends
- three items on the TO DO list  
of Neelie Kroes  
and **you too!**

## good books on security within IT



- ♦ *theory (math):*
  - Applied Cryptography, Bruce Schneier (2<sup>nd</sup> ed. 1996)
- ♦ *implementation (techi's):*
  - Cryptography Engineering, Ferguson, Schneier, Kohno (ed 2010)
  - Modsecurity Handbook, Ivan Ristić (rev 2010)
  - Apache Security (2009), Ivan Ristic
- ♦ *history and practice (managers):*
  - Security Engineering, Ross Anderson, (2<sup>nd</sup> ed. 2008)
- ♦ *non-technicians (you and me):*
  - Beyond Fear (thinking sensible), Bruce Schneier (2006)
  - Secret & Lies (with post 9/11 info), Bruce Schneier (2000)
  - Liars & Outliers, Bruce Schneier (Feb 2012)

theory book, 15 yrs old book, only if you know howto math?

crypto book is the howto,  
a recent book, many detailed algorithms

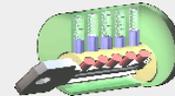
Ivan Ristic is the Apache security fellow,  
books can be ordered as ebooks

Ross Anderson is prof.  
First edition is freely downloadable but is old  
ed 1 has 600 pages, ed 2: 1000 pages....

how to live with fear,  
remain practical

## security in the physical world: keys and locks, authenticate and disclose

- ♦ yr 1778: double lever tumbling locks  
ca 10 bits strength
- ♦ yr 1844: cylinder / pin locks  
ca 20 bit strength
- ♦ yr 2000: physical locks getting digital  
ca 128 bit strength



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 7 to go

- 2-levers 4 blades 15 euro lock  
Chubb invented blocking of night lock,  
lock picking, 'runner key', 50 euro via web site order
- cylinder pins 4-6, some more sided, 35 euro lock  
Yale invention  
lock picking is like music, an art to tell a story  
  
bumping, Chaos conf. (Treffen) Berlin 2004  
95% of locks open easily
- Winkhaus 128 bit digital driven lock, 450 euro lock  
hacking: easy to do with magnet

### howto hack locks:

- brute force always the easy way,  
burglar way (Bulgarian Baco trick)  
social engineering a definite go (key below the carpet)  
have good survey done (open window, unlocked door).

- Stichting Kwaliteit Gevels certificate  
(keurmerk) with stars,  
so there is some form of accreditation

## hacking in the physical world

locks of cars are nowadays pretty good,

but.... there is now the

**Electronic Control Unit ECU**

which allows you

*to control your car*

*from a distance*

*so your car can be hacked*



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 8 to go

- locks of cars are better quality as locks of doors

- July 2010

Experimental Security Analyzes of a Modern Automobile

Karl Koscher on IEEE Symposium

it gives full remote access to the vehicle

speed 120 MPH, gear is in R (reverse),

message notice with title paper

- Black Hat July 2010:

showed how to make the ATM pay you dollars

hacked via the remote monitor function

- PIN: with thermal camera you can easily detect (80%) pin codes!

After 45 secs percentage drops heavily: UCSD (2011) Usenix paper

[http://www.usenix.org/events/woot11/tech/final\\_files/Mowery.pdf](http://www.usenix.org/events/woot11/tech/final_files/Mowery.pdf)

- remote control overlooked most of the time

## what can you learn from all this?

- ♦ protection arrangements **relate to emotional value** of the goods
- ♦ every security technique has **limited time of life**
- ♦ **all can be hacked**, usually via unexpected routes
- ♦ **security certification is the driving force**,  
but only with non-commercial interest
- ♦ **authentication is too complex**



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 9 to go

- locking can break emergency exit arrangements!
- evolution of internet is 100 times faster as physical world
- internet world is big, bigger, biggest  
and mostly anonymous, so w're all dogs
- are the precautions practical,  
can one maintain them?
- 1. IDENTIFY identify computers: client and server
- 2. AUTHENTICATE owner via certificates both ends
- 3. PROTECT COMMUNICATION privacy  
via encryption and integrity control:  
sender (hash function)

Nick Helm: "I needed a password with eight characters, so I picked 'Snow White and the Seven Dwarves'."

## encryption needs

- ♦ the encryption elements:
  - (pseudo) random numbers
  - primes (1024-4096 bits)
  - hash function (no collisions -> birth date paradox)
- ♦ number theory
  - project (1-1 function) number into finite space
  - calculations in finite space

## encryption technology

- ♦ the encryption elements:
  - (pseudo) random numbers
  - primes (1000-4000 bits)
  - least common multiples of prime minus 1
  - hash function (no collisions -> birth date theorem)
- ♦ number theory
  - project (1-1 function) number into finite space
  - calculations in finite space

## public and private encryption key

- ♦ pub key: **(n,e)**       $n = p \times q$  primes
- ♦ private key: **(p,q,t,d)**     $t = \text{gcd}(p-1, q-1)$
- ♦ choose **e** 'random' such that  $e \times d = 1 \pmod{t}$

## hash function

function to map number  $i$  to  $f(i)$  in N-space

N-space is big enough, say 256 bits

there is no  $f^{-1}$  function

no 1-1 function

***no collision is allowed***

Hash key is usually encrypted with private key,

So with published pub key you can check if content has been changed

To keep the private key secret and the strength of the encryption and the risk for collisions of the hash are the key factors of this technic

Disclosed access to the cert signing engine is the key element to protection

Diginotar event showed again that security measurements should be taken seriously

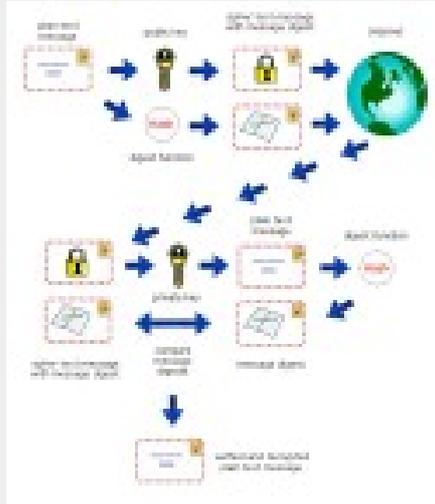
But also that access to the CA signing key should be protected well and reviewed, and reviewed well.

An encryption engine accessible only eg via serial channel and proprietary protocols is not enough:

Getting access to the management system is enough to get any cert signed by the CA.

# digital signature

*A. Lincoln*



## comments on encryption and hash functions

- ♦ hash functions used for signatures
  - MD5 (Ron Rivest) is broken
  - SHA-1 (Secure Hash Algorithm; NSA; banned from 1<sup>st</sup> of Jan 2011)
  - SHA-224, SHA-256, SHA-384 and SHA-512 (NIST)
- ♦ encryption functions to avoid
  - DH (Diffie-Hellman) 1976
    - has Man In The Middle (MITM) problem
  - RSA (Rivest, Shamir, Adleman) 1978 ( $n > 2048$  bits, 20 years)
    - small size problem eg with signatures
    - mathematical structure problem
    - with 2 signatures, compute sign. on message 3 as:  $s_3 = s_1 \cdot s_2 \pmod n$

hash function

no collision allowed, why?

MD5 is harmful.

a hack was expected and done.

SHA-1 2009 a collision was proofed,

so Jan 2011 no sha1 anymore

So fater one year now .... ni sha1 allowed

DH weaker as RSA

RSA still problem on low numbers

others ciphers:

AES, DSA, and ...

elleptic curve

## X.509 digital certificate

- ♦ public key of individual or server
- ♦ owner information
  - name, email or host name, owner 'details'
- ♦ digital signature of Certificate Authority (CA)
  - validates of **all information** on certificate (???)
- ♦ revocation information, start & expiration date
- ♦ allowed use of the certificate
  - login, code signing, EV, DV, etc.
- ♦ standard: X.509 (or e.g. another std PGP)

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 28 to go

X.509 have no public key service as PGP

X.509 is hierarchical structure via signatures

X.509 rely on one authority

maybe idea of web of trust via agents or users

X.509 info validation is doubtful due to

economics and culture difference

(law, trade, social culture)

how to get a trusted CA list?

e.g. Ubuntu validates Verisign?

what if a CA is becoming distrusted?

(no warning system)

PGP web of trust:

rely on many agents,

there is trust factor

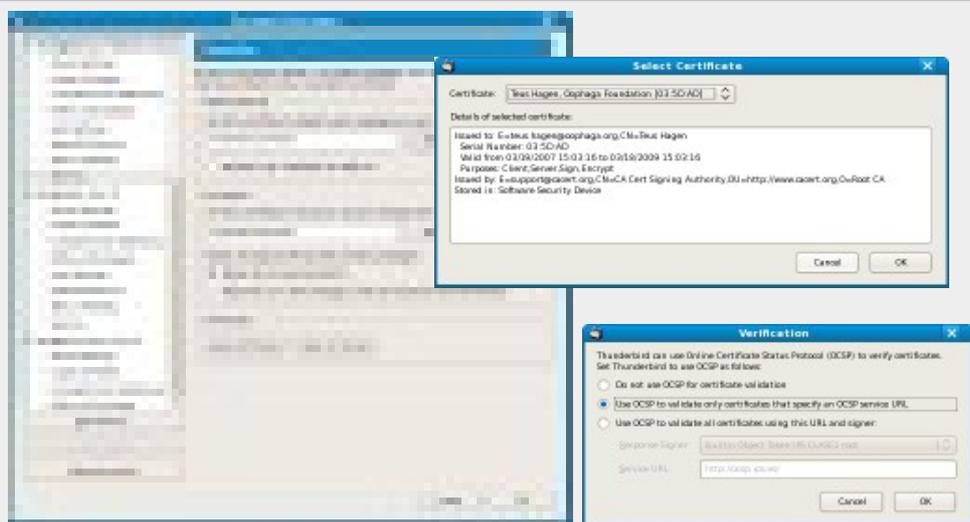
what about server cert fingerprint in DNS(SEC) record?

[www.startcom.com](http://www.startcom.com) provides free certs

CA not validating CA's info



# the How To Thunderbird Certificate Management



## X.509 certificate

### what to look for, do they make sense?

- ♦ Common Name (CN)
- ♦ owner, does it match what you think it should be
- ♦ domain and alt names (defined, no wild cards)  
do they match with DNSSEC data?
- ♦ DV (domain validated) or EV (owner extended validated)
- ♦ signature CA (trusted?, no MD5, and SHA-1 is deprecated one yr now)
- ♦ expiring within < 1-2 years and expired already?
- ♦ at least one revocation method/address, pref. OCSP
- ♦ private key well protected, and made by the owner!

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 31 to go

wild card e.g. : \*.shell.com (do not accept this!)  
server cert should have host name(s)

Common Name (CN) can be:

e.g. Teus Hagen, client cert email [teus@site.com](mailto:teus@site.com)  
or server cert [www.site.com](http://www.site.com)

Organisational Unit (OU) not needed.  
usually empty (cannot be validated)  
similar for country and address.

check own cert for capabilities:  
login, code signing, etc.  
the trick to collect a lot of money by the CA

Alt Names: 1 or 2, not 43!

X.509 certs are on the chip of ID  
(passport, driver license, etc.)

## what we learned so far

- ♦ the security practice with locks
  - ease of hacking,
  - dependency of policies
  - enforcement
  - validation and evaluation
- ♦ theory of security in digit land
- ♦ security tools in digit land
  - use them, configure them
  - server side **and** client side

## browser ↔ server: how to protect

### (1) URL : the host name

- DNS maps host name to IP address (cash poisoning)
- DNSSEC secures this, **but there is no evaluation!**

### (2) next get server document

- secured via HTTPS, the SSL/TLS protocol layer

AND do this also for:

protected email, terminal access, VPN, etc. etc.

ideally DNSSEC should cover this

However DNSSEC registrars do not review/validate info!

So only cache poisoning is avoided

signatures are proof to identity information

in practice we should use both,

and it is so more complicated

## 1<sup>st</sup> DNSSEC: is the IP address really you?

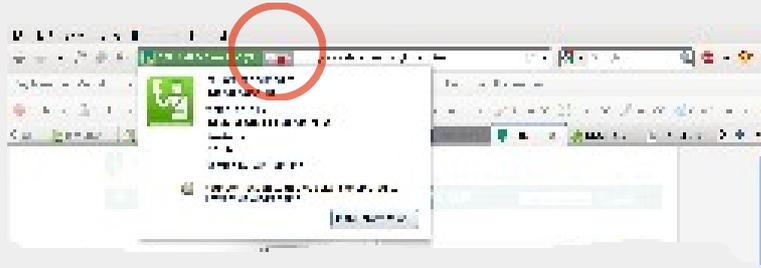
- ♦ July, 2010:
  - first firm step with signing the DNS Root;
- ♦ DNSSEC statistics October 2010:
  - 60% had software ready;
- ♦ DNSSEC test October 2010:
  - but world wide only 3% really uses it;
- ♦ one year later, Sept 2011 assessment of ~225 NL web sites:
  - only a very very few entries are secured by DNSSEC
  - CWI, RIPE, SIDN, CAcert, NLnet Labs,
  - none of the banks, gov's, etc. ...

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 34 to go

- DNSSEC relies on signatures
- registrars do not validate info up to today  
decisions to validate not yet started
- evaluation which ISP had the software ready:  
about 60%
- RIPE did made available a test:  
Also 60% (one year ago: now not much better)
- however  
what about the ADSL/routers at home.  
  
BSI study 36 home routers covering  
90% of the market,  
only 4 were ready!

## how end users surf: the host name in URL

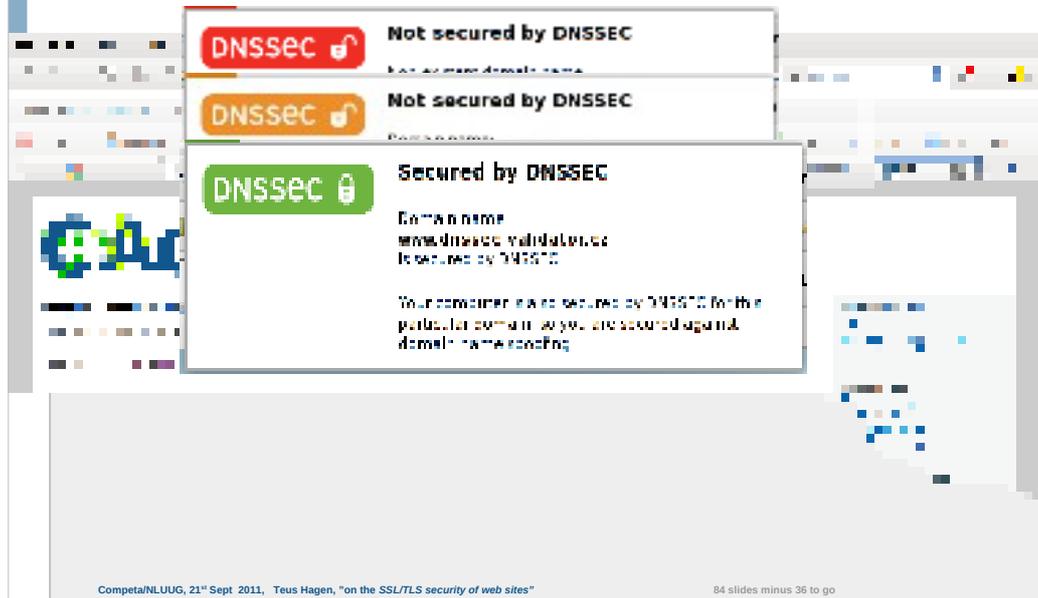


Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 35 to go

- does anyone know this?
  - what does the key with the stop signal means?
- who has that in their browser?
- it is an Firefox add-on, have a look for it: DNSSEC

## DNSSEC show IP - host name validation



- waiting for validating

- resolver can be adjusted via preference

## DNSSEC configuration status in more detail status three months after DNSSEC initiation

do main name	RRset secured	RRset insecure	DNSKEY/D/INSEC secured	DNSKEY/D/INSEC insecure	security algorithm	delegation secured	delegation insecure
csrc.nist.gov	2		12		RSASHA1 (4) RSASHA1-NSEC3-SHA1 (0) RSA/SHA256 (2)	2	1
www.icann.org	2		15		RSASHA1 (2) RSASHA1-NSEC3-SHA1 (0) RSA/SHA256 (2)	3	
www.isc.org	2		15		RSASHA1 (5) RSASHA1-NSEC3-SHA1 (4) RSA/SHA256 (2)	4	
www.abnamro.nl		1	3	4	RSASHA256 (0)		2
www.digid.nl		1	3	4	RSASHA256 (0)		2
www.sidn.nl		2	3	4	RSASHA256 (0)		2
www.nlnetlabs.nl		2	3	8	RSASHA1 (2) RSA/SHA256 (7)		2
www.nluug.nl		2	4	4	RSASHA256 (0)		4
www.surf.nl		2	3	7	RSASHA256 (0)		2
www.cacert.org	1		15		RSASHA1 (2) RSASHA1-NSEC3-SHA1 (7) RSA/SHA256 (2)	3	1
www.nunames.nu		1	2	1	RSASHA1 (2) RSA/SHA256 (2)	2	1

Oct 2010

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 37 to go

- Sandia DNS Visualization validation tool  
October 2010
- 6 cipher/hash suites used 4  
should be phased out: **MD5 now**  
and SHA-1
- ICANN and ISC of course,  
but notice the SHA1 use!
- Holland one year ago was far away.
- after some interactions  
CAcert play their own game:  
they use DNSSEC DLV trick  
via ISC consortium.
- it's still a long way to Tipperary

## DNSSEC configuration status in more detail

one year later ...

Sep 2011

domain name	RRset secured	RRset insecure	DNSKEY/DNSSEC secured	sec. alg	Delegation secured	Delegation insecure
espee.surfnet.nl	1	0	10	RSA/SHA256 (7)	2	1
mijn.vu.nl	2	2	6	RSA/SHA256 (4)	1	1
www.cwi.nl	2	0	8	RSA/SHA1 (2)	1	1
google.com	3	0	6	RSA/SHA256 (4)	1	1
www.twitter.com	3	0	6	RSA/SHA256 (4)	1	1
www.digid.nl	1	0	6	RSA/SHA256 (4)	1	1
www.diginotar.nl	1	0	6	RSA/SHA256 (4)	1	1
www.ov-chipkaart.nl	1	0	6	RSA/SHA256 (4)	1	1
www.ideal.nl	1	0	6	RSA/SHA256 (4)	1	1
www.triodos.nl	1	0	6	RSA/SHA256 (4)	1	1
cert.startcom.org	1	0	8	RSASHA1-NSEC3-SHA1 (4)	1	1
www.cacert.org	1	0	11	RSASHA1-NSEC3-SHA1 (7)	1	1
www.evss.nl	1	0	6	RSA/SHA256 (4)	1	1
www.pinkroccadecsp.nl	1	0	6	RSA/SHA256 (4)	1	1
drs.domain-registry.nl	1	0	6	RSA/SHA256 (4)	1	1
liportal.ripe.net	3	0	10	RSA/SHA1 (4)	1	1
www.perfectviewoverheid.nl	3	0	6	RSA/SHA256 (4)	1	1
www.ripe.net	2	0	10	RSA/SHA1 (4)	1	1
www.sidn.nl	2	0	8	RSA/SHA256 (6)	2	0
service.xs4all.nl	1	0	6	RSA/SHA256 (4)	1	1
webmail.xs4all.nl	1	0	6	RSA/SHA256 (4)	1	1
www.ziggo.nl	1	0	6	RSA/SHA256 (4)	1	1
www.internetshop.nl	1	0	6	RSA/SHA256 (4)	1	1
www.kwantum.com	1	0	6	RSA/SHA256 (4)	1	1
www.wehkamp.nl	1	0	6	RSA/SHA256 (4)	1	2
candidate.manpower.com	3	0	11	RSA/SHA256 (6)	2	4
www.nlnetlabs.nl	2	0	8	RSA/SHA256 (6)	2	0
www.alcoholdebaas.nl	1	0	6	RSA/SHA256 (4)	1	1
www.careweb.nl	1	0	6	RSA/SHA256 (4)	1	1
www.infoepd.nl	3	0	6	RSA/SHA256 (4)	1	1
www.zorgdraad.nl	1	0	6	RSA/SHA256 (4)	1	1
zorginnovatieplatform.nl	3	0	6	RSA/SHA256 (4)	1	1

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 38 to go

Situation after one year is not changed.

Only those added who are familiar with DNSSEC and involved in the operations.

In one year one added: CWI!

Notice that social network web sites are not ready for DNSSEC

## DNSSEC conclusions

♦ *it's still a too long way to Tipperary ...*

- ♦ but with some tricks we can shorten travel time
- ♦ *the end user should install more validation signals*
- ♦ DNSSEC is the first security step:  
secures network address and host/domain name

it steps silently over

the binding of the end user

to his end point on the network

public wifi's are not well secured? (MITM tactic)

home routers and modems are troublesome

but know your DHCP is not secured by your ISP

who is using IPV6? My experience: it is fast! Due to lack of use

maybe the VDSL2 introduction helps  
(new DSL modems streamered in today)

## make sure your software is up-to-date just taken from web server software statistics

160 web sites, 20 had no signature → 140 signatures:

- ♦ HTTP servers (mainly on “UNIX”-family OS):
  - 27% **Microsoft-ISS**: rel **5.0** (7%, 2000), 6.0 (79%, 2003) -**7.5** (13%, 2008)
  - 50% **Apache**: 1X **1.3** (2004, healthcare), 4 X **2.0** (2005, gov), majority 2.2.8 (2008), highest **2.2.20** (2011, NLnetLabs)
  - Apache mod\_ssl **2.0** (4), 2.2.3 (majority), **2.2.20** (highest in healthcare!)
- ♦ 10% **OpenSSL** (Apache) R 0.9.7 (2003) -0.9.8 (2005), **1.0.1** (2011)

**OpenSSL R0.9.8a is from Nov 2005!**

**PHP** 1X **4.4** (2008, finances), 5.2.X (majority), **5.3.8** (2011)

unique example signature of **www.ideal.nl** (checked Sept 2011):

**Apache/2.0.55 (Ubuntu); PHP/4.4.2-1build1 mod\_ssl/2.0.55 OpenSSL/0.9.8a**



release dates via Google search on “XXX relnr”, and ditributors announcements sites  
Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, “on the SSL/TLS security of web sites”

84 slides minus 40 to go

Server software seems not much updated today!  
sloppyness everywhere...., is security taken seriously?

The big honeypot is [www.ideal.nl](http://www.ideal.nl) (honeypot is web security pitfall)

However the site might not do any fin. transactions, but you never know

And: it does not add to trust feeling of customers at all

Is this site really running software dated from 2005?

Lucky the OpenSSL release was before the Debian OpenSSL event in May 2008

Slogan iDeal: based on internet banking, same security measurements ...

Keep your name high....

## make sure your web server is up to date!

my situation Sep 2011: FC12, FC15, Ubuntu 11.4

- ♦ OpenSSH: 1.3a5.8p1 in 2008 FC7 4.5p1
- ♦ OpenSSL: 10.0.0b & e in 2008 FC7 0.9.8b
- ♦ Apache 2.2.15 & 17 in 2008 FC7 2.2.8
- ♦ Apache mod\_ssl 2.2.15 & 17
- ♦ PHP 5.3.6 in 2008 FC7 5.2.6
- ♦ Perl 5.12.4 in 2008 FC7 5.8.8

May 2008: Debian OpenSSL 0.9.8c vulnerability

Overview of up to date (6 months delay) of web site server software

one system I have running with FC7 2008 latest update just for reference

Time costs? : 15 minutes per week for 5 machines, mostly automated

Do not show that security is taken not seriously (iDeal case)

Do not hide mistakes

## 2. SSL/TLS protocol layer:

identify and authorize: client ... and ... server sides

### 2.1 first identify / authenticate:

use the X.509 certificate

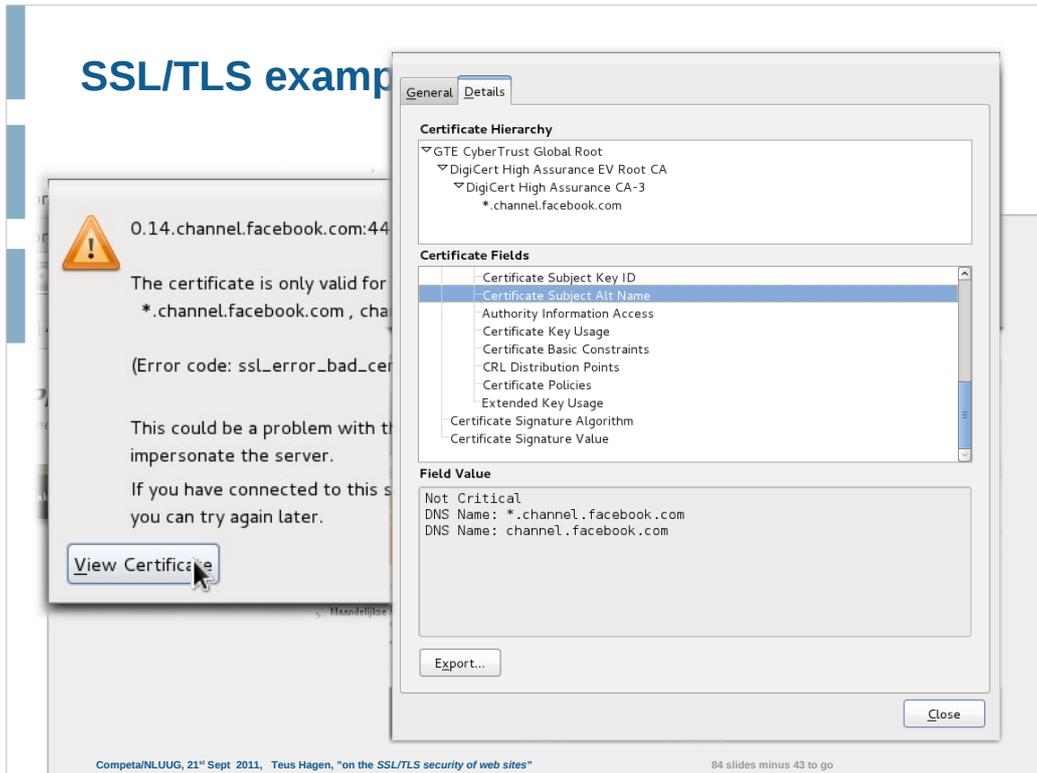
- match *validated* host/domain name <-> IP address
- match *owner* (CN)...
- info validated by the Certificate Authority (CA) (really?)
- check trust of the CA
- check: revocation, signature algorithm, ...

2.2

Cometa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 42 to go

- support needed from DNS
  - to know who you say you are,
  - and you are talking to
- is this the domain name
  - you wanted to talk to?
- host names, domain names
  - do not say much
  - if they are not on the certificate
  - or are wild cards
- sloppiness needs proper identification
  - from owner
- BUT user should identify himself
  - also properly: individual certificates:
- Web ID, OpenID
- be aware of your traceability
- browser fingerprinting can easily be used



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 43 to go

Privacy is not a security champ

Facebook is A rated, takes security serious?

Add a friend and you get a facebook channel

But that channel carries a certificate of wrong domain

So your browser says: he friend there is an error and try again later

EVERYBODY does not view the certificate, do you?

Well let us see what is wrong

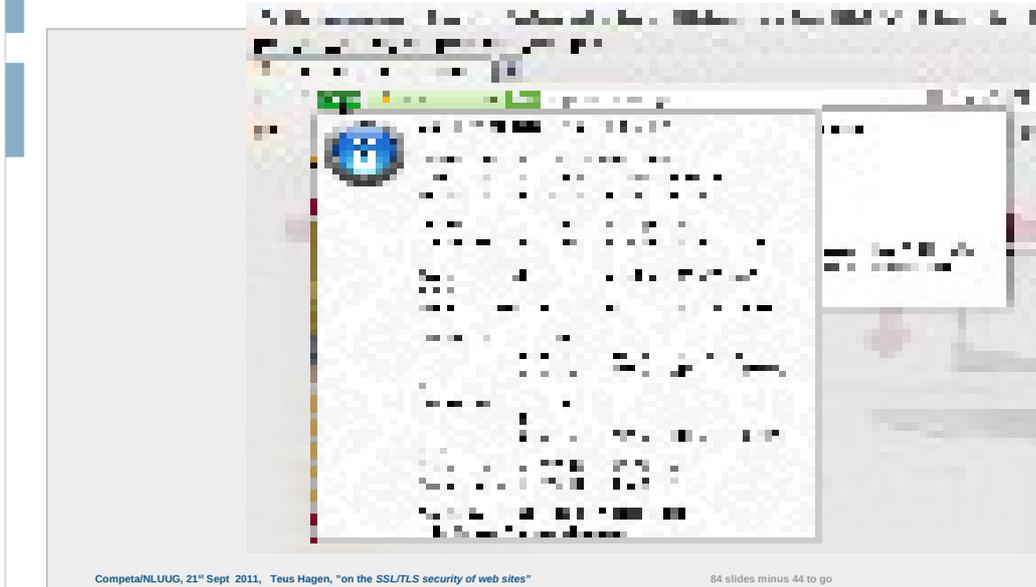
The server may or may not be part of facebook

The certificate is not validated at all.... (EV cert in this case)

Depending on reasoning for adding the friend you are trusted or not

## browser show: Certificate Authority (CA)

<https://www.verisign.com>



- **who you are, you say you are**

- **Verisign:**

EV certificate,

owner known

self signed! All CA's do this, why not cross signing?

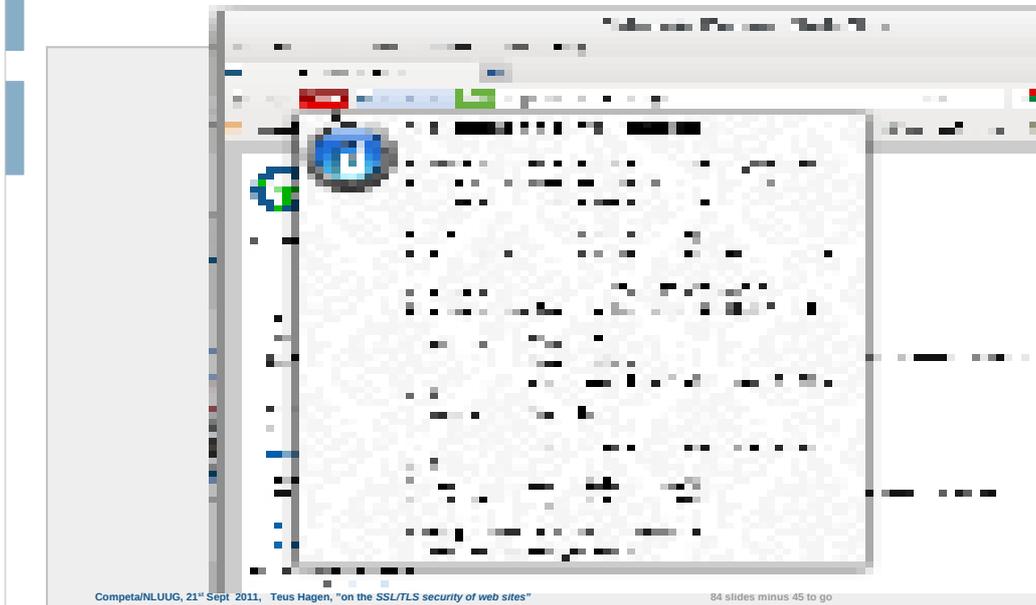
- **EV certificates are sometimes on sale:**

ca 100 euro per year, so expect not much

validation doubtful

## browser show: Certificate Authority (CA)

<https://www.cacert.org>



- **who you are, you say you are**

- **CAcert:**

added on CA accepted list, so blue,  
owner unknown

- **Venray.nl:**

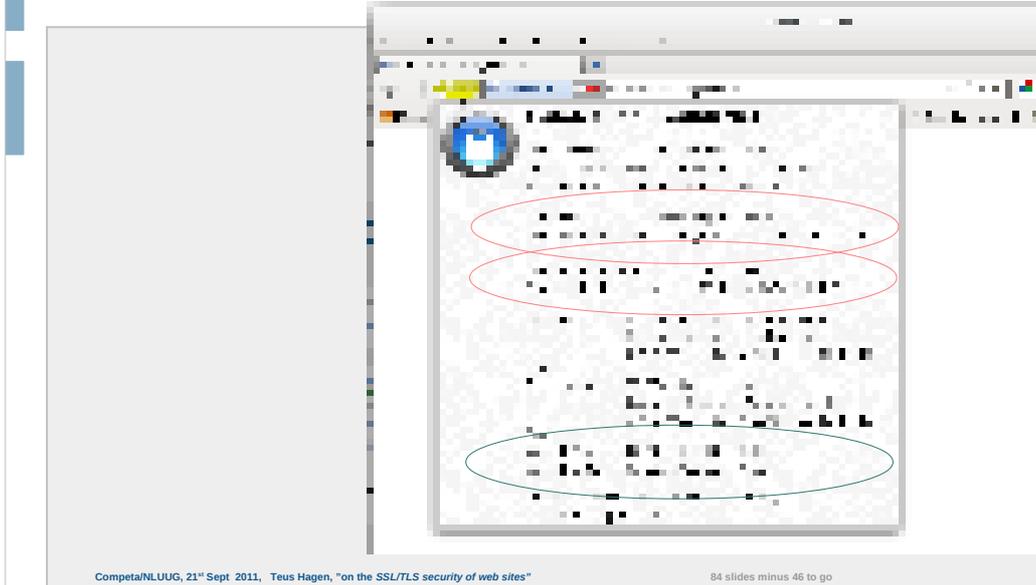
local government e-desk,  
owner unknown,  
no EV certificate,  
not trusted

- **ICANN:**

accredited  
owner unknown  
no EV certificate

## browser show: Certificate Authority (CA)

<https://www.diginotar.nl>



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

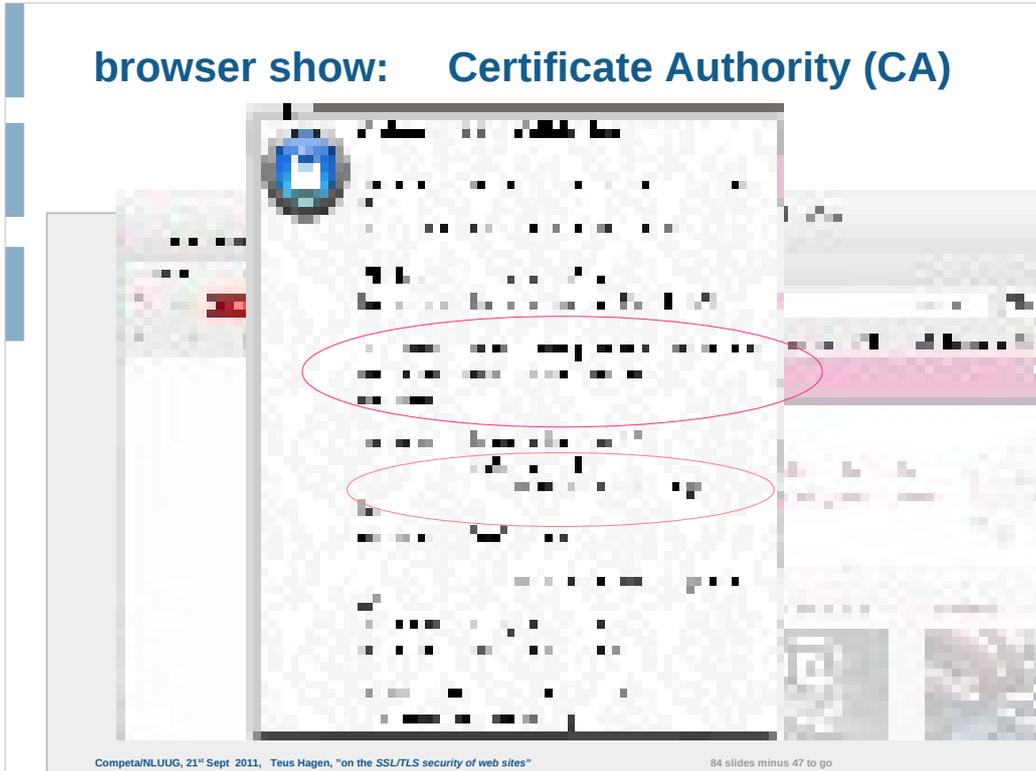
84 slides minus 46 to go

**Now an easy one: diginotar**

**See blank page**

**Certificate is brand new not from Staat der Nederlanden**

## browser show: Certificate Authority (CA)



Honey pot [www.ideal.nl](http://www.ideal.nl)

Servicing web site trade financial actions for dutch banks

A show how reliable one can be

***“Say what you do,  
do what you say,  
and ... proof it.”***

**David Ross**

- ♦ accreditation of CA' s *is sloppy*
- ♦ certificate applications (configurations):  
*not assessed, no check!*
- ♦ names on certificates *are hopeless*

**conclusion: *certificates give false sense of trust***

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 48 to go

- in commercial hands

- should Ubuntu require  
audit for Verisign?

- David Ross criteria

- most CA's are based in the US  
and operate from there

far away is a jurisdiction problem

there is a market culture problem:

bought an EV cert:

need entry phone book

or lawyer/bank director

for name validation?

Chambre de Commerce (trade)

KvK Nld is most advanced in EU

do not expect much is done

for your 100 euro

## the DigiNotar Sept 2011 show case

### just an example, just one of many

- ♦ CA accreditation and chain accreditation was sloppy
- ♦ lacking was (unacceptable):
  - review of configuration and
  - measurements to secure signing key was lacking
- ♦ unacceptable: broken key, political power to delay revocation of signing key
- ♦ what to do with all CA signed signatures on notary central archive?
- ♦ Nov 2010 presentation showed:
  - hacking could be expected, only question when and
  - how intelligent applied
- ♦ wrong mindset: Internet (and so impact) is thought local, but is world wide

## after the DigiNotar:

### lessons taken, ... probably not?

- ♦ CA accreditation in hands of independent bodies:
  - certify and controlling body for CA's
- ♦ certificates for individuals
- ♦ more as one CA who signs certificates (PGP dream)
- ♦ review and control: measurements enforcement
- ♦ who can take action here
  - PCI/IFIPS 140-2 compliant
  - US: there are (unenforced) security measurements bodies
  - EU: Neelie to do list?
    - (banks do it silently and disclosed from public?)

## 2<sup>nd</sup> SSL/TLS protocol layer: choose encryption

### 2.1 identification / authentication: X.509 certificate

- match host/domain name <-> IP address
- match owner
- Checked by Certificate Authority (CA)

### 2.2 negotiate and establish cipher suite:

- **encryption** algorithm (hide) **and**
- **hashing** function (validate)



this needs **a well defined configuration** on **BOTH end points**

- hashing function MD5 is harmful
  - already more as a year now
  - how many persons needed for birthday collision?
  - 50% chance of collision
- SHA1 only till end of 2010, that is one year ago...
  - statement of Bruce Schneier
- insecure ciphers
- insecure renegotiation (MITM possibility)
- too many self invented algorithms
  - are still around

## SSL/TLS configuration on both end points

- ♦ end-user end: Firefox
- ♦ server side configuration, the internet security policy
  - e-banking: PCI DSS-2
  - e-commerce FIPS 140-2
- tools: check and assess it!  
openssl, sslscan, ssllsnif, ... [www.ssllabs.com](http://www.ssllabs.com)



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 53 to go

### - PCI DSS -2 sloppy requirements:

Payment Card Industry Data Security Standard  
only strong ciphers  
for banks, initiated credit card companies  
easy to implement

### - FIPS 140-2:

especially for e-commerce  
**Federal Information Processing Standard**  
much more detail  
MD5 is out, SHA1 is just still in  
but nobody implements them....

- there is still (one year later) no certifying/marketing (waarborg) body  
in Holland who checks/assesses

- paper has full details and suggestions

- it is so easy to get things  
on an acceptable level

reminder: you can arrange:  
null-MD5, the lock shows "locked".

- use: Apache Security and Modsecurity Handbook, Ivan Ristic publ Feisty Duck

## SSL/TLS configuration what to look for



- ♦ X.509 cert OK? Name matches with DNSsec server name?
- ♦ no MD5, and SHA-1 is deprecated one year ago
- ♦ minimal 1024 bits
- ♦ no SSL V2 usage at all
- ♦ no (insecure) renegotiation
- ♦ SSL Labs ratings  $\geq 85\%$
- ♦ ephemeral DH support
- ♦ no MITM (man in the middle) possibility
- ♦ adjust browser configuration for acceptable cipher level
- ♦ not any of weak or insecure encryption/cipher

Ephemeral DH:

also when data is recorded and saved

no used encryption key recovery is possible

## SSL/TLS assessment



of ca 225 Dutch web sites

### categories / branches:

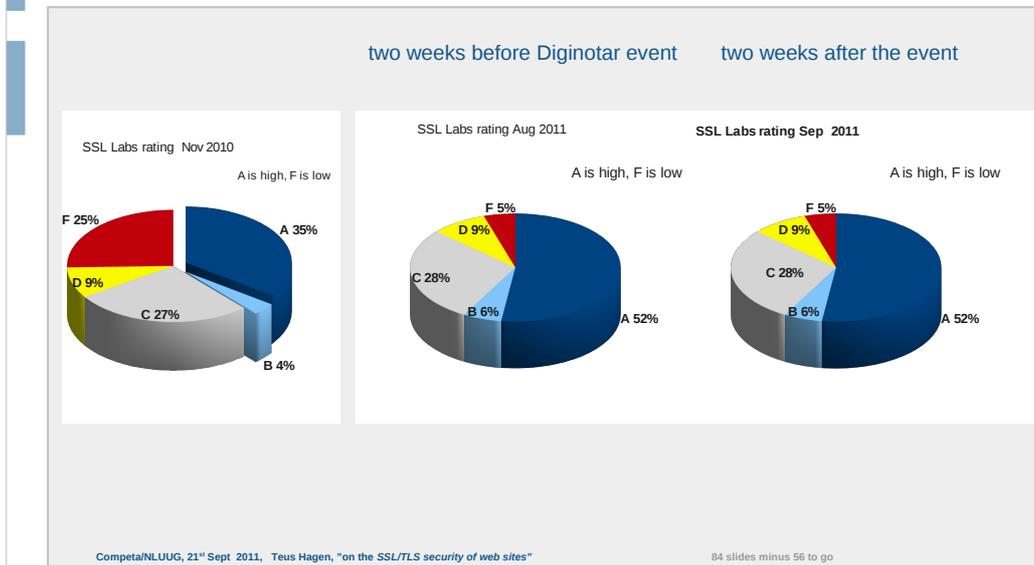
- ♦ ~95% of on-line banking sites (37)
- ♦ governmental e-desks: central, regional, local (42)
- ♦ e-commerce web trade: trade, services (53)
- ♦ health care e-desks, chat (41)
- ♦ academic e-desks: academics, colleges (25)
- ♦ internet security consultancy and services (20)

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 55 to go

- values are not statistical solid  
(not random selection and check)
- all assessments figures from SSL Labs (Qualys)
- how: convert HTML SSL Labs data into spreadsheet data/formula
- tried to send all assessment values to web site manager:  
end of July and 31 October 2010, Feb 2011, Aug 2011 and Sep 2011  
Diginotar event showed no diff in last two assessments  
  
the feedback/response was minor, eg  
email from "postmaster" that  
"user postmaster did not exists"  
"you will get an answer within 24-48 hours, ticket number NNN"  
Volksuniversiteit: antenna.nl answer: indeed no cert, you can order one with us...  
anyhow those who are personally known to me reacted  
Digid and ING improved due to tweakers.net noise in Nov 2010  
RIPE, VU, CAcert reacted and improved also in Aug 2011
- but nevertheless some did update the config, much improved after one year  
healthcare: thanks to blogs health care  
this shows that it can be done easily  
NLnetLabs and CAcert went so on top DNSSEC AND SSL configs

## general picture of the SSL Labs assessments November 2010, and one year later



average ratings

blue color: >80%

- cipher strength
- key exchange
- protocols offered
- server cert is the CA trusted?
- expired cert
- insecure cipher use
- renegotiation (MITM?)

Cross Site Request Forgery – CSRF  
use only encrypted cookie as parameter

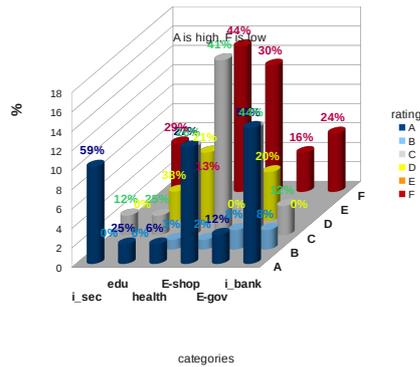
- insecure session resumption

## the figures of all categories in more detail November 2010, and 3 months later ...

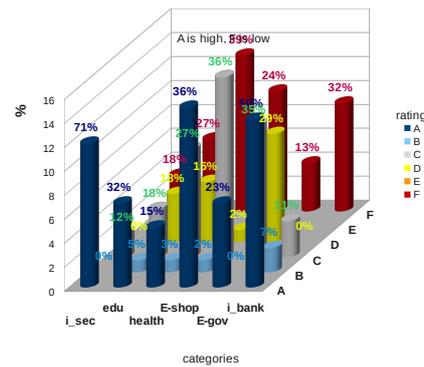
statistics of 2010, November

2011, February

SSL Labs ratings per category Nov 2010



SSL Labs ratings per category



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

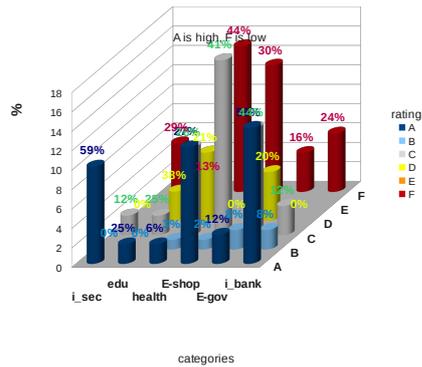
84 slides minus 57 to go

- per category
- banks, I-sec differ from rest
- health-care worst
- education worry some
- e-commerce trouble, a mess,  
no technical certification/marketing,  
However geared for trade

## the figures of all categories in more detail November 2010, and one year later ...

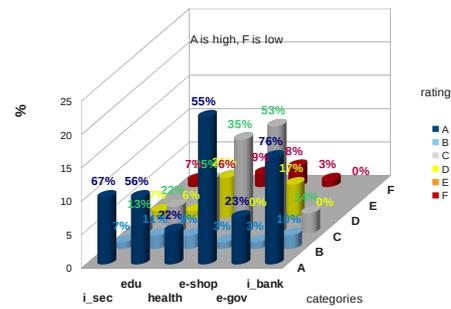
statistics of 2010, 31<sup>st</sup> October

SSL Labs ratings per category Nov 2010



2011, September

SSL Labs ratings per category Sep 2011



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 58 to go

- per category
- banks, I-sec differ from rest
- health-care worst
- education worry some
- e-commerce trouble, a mess,  
no technical certification/marketing,  
However geared for trade

## all categories in much more detail (Oct 2010)

category	av. rating	CA trusted	protocol	key exchange	cipher	MITM?	TLS 1.0	SSL 3.0	SSL 2.0+	SSL 2.0	session resumption	insecure renegot.	PCI compliant	FIPS ready	# weak cyphs	# insec cyphs
i_sec	79%	81%	80%	74%	83%	53%	100%	88%	88%	19%	75%	13%	69%	0%	19%	6%
healthcare	59%	59%	63%	49%	64%	18%	100%	100%	100%	73%	88%	42%	9%	0%	73%	3%
edu	59%	88%	63%	53%	63%	33%	100%	100%	100%	75%	100%	38%	25%	0%	75%	0%
e-shop	69%	76%	73%	57%	71%	42%	100%	100%	100%	36%	83%	21%	31%	0%	60%	5%
e-gov	58%	88%	63%	47%	63%	37%	100%	100%	100%	71%	92%	21%	25%	0%	75%	4%
i_bank	77%	75%	76%	76%	80%	44%	100%	100%	100%	26%	87%	22%	65%	0%	17%	0%
all categories	69%	76%	72%	62%	73%	35%	100%	99%	99%	46%	100%	26%	40%	0%	51%	4%

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 59 to go

- average rating, all should be >80%
- CA trusted, all >80%
- protocols:
  - protocol rating
  - key exchange rating
  - cipher rating
- protocols
  - SSL2 should be out, zero
- PCI DSS 2 / FIPS 140-2
  - Payment Card Industry Data Security Standard
  - Federal Information Processing Standard
- no weak cipher strength
  - >128 bits, > 10 minutes computer power

## all categories in much more detail (Sep 2011)

category	av. rating	CA trusted	protocol	key exchange	cipher	M/R/TW?	cert type	cert chain	TLS 1.1	TLS 1.0	SSL 3.0	SSL 2.0+	SSL 2.0	session resumption	insecure renegot.	PCI compliant	FIPS ready	# weak cyphs	# insec cyphs
i_sec	79%	88%	78%	69%	83%	20%	30%	6%	0%	100%	88%	88%	31%	100%	13%	63%	6%	19%	0%
healthcare	63%	95%	67%	56%	68%	7%	22%	28%	0%	100%	100%	100%	61%	100%	26%	26%	0%	65%	4%
edu	70%	100%	70%	64%	76%	16%	12%	38%	0%	100%	100%	100%	56%	100%	33%	44%	0%	39%	6%
e_shop	72%	97%	76%	66%	76%	25%	35%	9%	0%	100%	100%	100%	42%	100%	26%	42%	0%	42%	3%
e-gov	58%	82%	66%	48%	61%	25%	17%	41%	0%	100%	100%	100%	68%	100%	16%	19%	0%	74%	0%
i_bank	79%	100%	78%	77%	83%	17%	52%	14%	0%	100%	100%	100%	25%	100%	35%	75%	0%	15%	0%
Sep 2011	71%	95%	74%	64%	74%	19%	24%	10%	0%	100%	99%	99%	46%	100%	24%	46%	1%	43%	2%

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

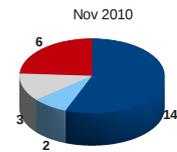
84 slides minus 62 to go

- average rating, all should be >80%
- CA trusted, all >80%
- protocols:
  - protocol rating
  - key exchange rating
  - cipher rating
- protocols
  - SSL2 should be out, zero
- PCI DSS 2 / FIPS 140-2
  - Payment Card Industry Data Security Standard
  - Federal Information Processing Standard
- no weak cipher strength
  - >128 bits, > 10 minutes computer power

## internet banking (38 sites assessed)

much better in one year

but smaller once not there!



♦ 24% MITM warning, 72% PCI compliant

♦ **ING:** mijn.postbank.nl, mijnpostbank.nl, mijn.ing.nl, mijn.ing.nl, www.ing.nl  
ok, maar 😞 **DNB and DHB:** \*.dnb.nl, \*.dhbbank.nl

😞 **FBA:** expired certificate (11<sup>th</sup> May), no EV

😞 **DNB, BoS, Argenta en Triodos** (40-bits!) :  
CA chain issues

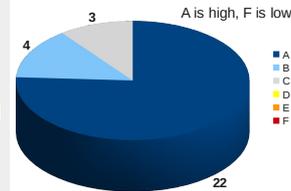
😞 **Direct Bank en Vermogensbeheer On Line:** DV cert

😞 **AT Bank (B rate), Ideal, DHB, Triodos, Vermogensbeheer On Line, LeasePlan:**  
SSL2.0 supported YES :-)

😞 **Ideal:** C rate, 40-bits, no PCI compliance, allow 10 weak ciphers, no secure renegotiation, no EV/DV certificate, Ubuntu release too old, server SW too old, but ... MITM OK.

**X 39% (was 79%) allow insecure renegotiation (MITM)**

SSL Labs rating internet banking Sept 2011



Cometa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 64 to go

-One year ago:

ING

[www.ing.nl](http://www.ing.nl), [mijn.ing.nl](http://mijn.ing.nl), [mijn.postbank.nl](http://mijn.postbank.nl)

redirect without notice

expired certificate

- NIBC

redirect naar [sparen.nibcdirect.nl](http://sparen.nibcdirect.nl) without notice

gap of 6 weeks from expired and

low level SSL/TLS arrangement

- Fortis, FBA (much improved lately) and Staalbankiers

expired certificate, no EV certificate, allow 40 bits

- Ideal

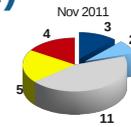
only at C level, no EV/DV certificate

- SNS bank

connection failure, broke communication

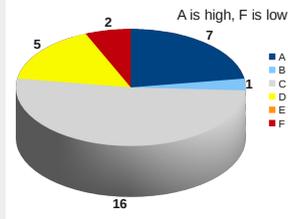
## government e-desks (42 sites assessed)

### high lights



- ☹️ 21% CA chain issues and/or too long
- ☹️ only 10% has EV certificate
- ☹️ police (public office, locals):  
exp. (~6 m) cert, 40-bits, support weak cyphers

SSL Labs rating government e-desks Sep 2011



- ☹️ balie Delft: exp. cert, F rating, SSL2.0
- ☹️ IND D rate, allow 40-bits, SSL2.0 supported, long chain
- ☹️ **overheid.nl en politie.nl**: champs on weak cyphers support
- ☹️ local gov: low rates.  
Venray, Horst ad Maas, Kerkrade, Peel en Maas, Gennepe, prov Limburg: many self made CA are replaced by no CA now.

Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 66 to go

-One year ago:

Venray, Horst ad Maas

self signed cert Cavernray

Horst was initially self signed

now Pink Rocado/Getronics week after complain

local gov use all probably

local host provider and web service provider

anecdote: provider was right on corner, "who do you think you are!"

- DigiD

Was F rate, after publication now OK,

And now use Getronics/Staat (10 Sept issued)

Chain length still 4!

Getronics (KPN PKI bedrijf) voorwaarden(art 6.1) staat:

De Vertrouwende Partij is verplicht om per geval zelfstandig te beoordelen of het gerechtvaardigd is om op een PKI-overheid Certificaat te vertrouwen

- police

Police Rotterdam (no domain name, no DV/EV cert),

Politie onderzoeken (OM) (use 6 ms expired cert)

Rotterdam: two web sites: secured and unsecured web site

only 52% average, 40 bit, insecure ciphers (with 10-12 on top)

21% PCI compliant:

tax, local Eemmond, government, DigiD, Diginotar, land registry

## e-commerce / web shops (44 sites)

### high lights



#### providers:



only Tele2 has A rating;

have (DV) CA cert:

only Xs4all, UPC (lowest 44% rating), BrabantNet

25% have CA chain issues or chain too long

13 of 38 with **host/domain name** on cert use **wild card** :-)

have EV CA cert: Wehkamp, Coolblue, Kwantum

Pixmania (no security at all)

expired cert only one: Ttec (Feb 2011) with lowest SSL Labs rating



35% **validated CA certs**: only 3% uses Ext. V, 9% Domain V, 38% no rating ie no SSL.

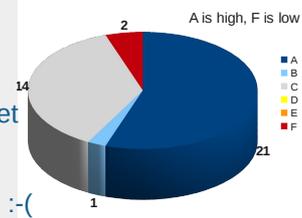


42% support 40-bits, 42% support SSL2.0



best (rating 88%, no issues): Wehkamp, Kwantum

SSL Labs rating web shops Sep 2011



- None is FIPS 140 compliant,  
13 (23%) PCI compliant
- 35% use validated cert, only 8% EV cert

- 41% SSL2.0 supported

TTEC: lowest rating, expired cert

10% has chain issues or too long (providers 25%)

## web shop certification / marking



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 69 to go

Data from one year ago:

- 16 web shop certification organisations
- 2 have applied for certification to Council of Accreditation (ConsuWijzer)
- only Thuiswinkel reacted in 2010 but did not know what SSL/TLS is about however Google showed discussions in 2007 to do: techn. Assessments
- ICTRecht in some way the only honest one?: advise/help to adjust to all legal aspects
- all web sites searched for techn security policies/requirements none had them approached all of them to ask for correctness of omissions

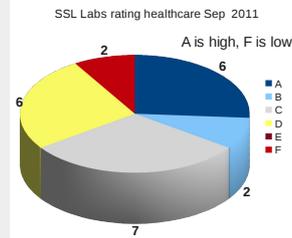
## healthcare (41 sites assessed)

Physicians, hospitals, GGD, EPD, health support, specialists, internet (urgent) help and chat services



much improved in one year!

- ♦ 63% use SSL, 56% use CA cert
- ♦ 22% validated cert,  
only chat Sens Oor uses EV cert.
- ♦ 65% bad configuration: weak cyphers, SSL2.0
- ♦ survival Kid XL has 5 much different hostnames
- ♦ expired CA cert: Grip op je Dip, chat Welzijns Groep
- ♦ champ: chat Sens Oor, but CA chain too long: 6



Competa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 71 to go

- Slideshow much better status now) One year ago:

- Hard to find SSL/TLS protected web sites.

- 50% still use old fashioned login/password without any protection

- Health care is the category to show how bad it can be made some extra push done and it helped

- only a very few with A grading (with EV cert), most had no hostname/domain name on cert

Improved: chat, digipolis, physician site, hulpmix

Most chat have now DV/EV cert

50% no name on cert

25% improved due to publications

- self manufactured certificates easy to find

- looking at RR host name record one sees a lot of good willing help sites

- conclusion: money is better protected as privacy

## academic e-desks (25 web sites)

### high lights



☹️ **CA chain issues:** 38%, 56% SSL2.0 support,

- ♦ **CWI:** use wild card, CA chain issue + too long

☹️ **TUE, TUD, VU, Nijmegen**

40 bits, Terena CA

☹️ only 12% have **DV CA cert**, none EV CA cert.

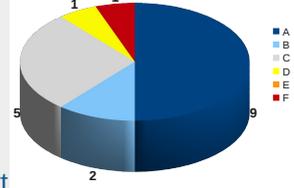
😊 best is **webmail.hva.nl** and **intra.hva.nl**: DV CA cert

CA chain, PCI compliant, webmail: no secure renegotiation support (MITM)

- ♦ 72% use **Terena** as CA cert provider

SSL Labs rating academic Aug 2011

A is high, F is low



-Slide status now, One year ago:

- Universiteit van Amsterdam:

employee site, A 84%,

128 bits, no SSL 2

- CWI: A 88%,

wild card, no SSL2

- all others had 40 bits,

Terena has high market share in edu land.

- uni's: highest D 48%,

TUE 45 alt names

- high tech:

InHolland one of the two site not secured,

NOVI no name on certificate

Fontys Venlo: own brewn, one expired, one no name on cert, rating too low

## internet security aware companies (18 sites)

### high lights



#### ♦ Certificate Authorities and providers (CA's)

**CAcert** (no accredited.), high rating, good DNSSEC config



**evssl:**

unknown cert type (Diginotar), lowest rating 48%,  
40-bits and weak cyphers

#### ♦ registries

SIDN (2 different sites), wildcard and no EV: RIPE and SIDN

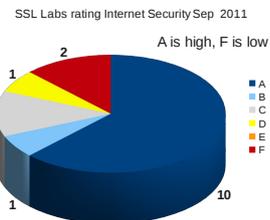
#### ♦ weak cyphers supported: 19%

lirportal Ripe, EV SSL, Tunix (highest weak cyphers)

#### ♦ Pink Roccade: only one with CA chain issues



best: **cert Startcom**: 93% rating, PCI and FIPS 140 ready!,  
but low key exchange rate



Cometa/NLUUG, 21<sup>st</sup> Sept 2011, Teus Hagen, "on the SSL/TLS security of web sites"

84 slides minus 76 to go

Slide status now, one year ago it was:

- mentioned

CA StartCom: provider, CA, highest score ever seen:

A 93%,

But still have insecure renegotiation

- SIDN:

two sites: WWW is weak but improved now, registry is OK

- NLNet Labs, CAcert:

got to F 91%, they clearly know ho

- either EV (30%) or not known, none with DV cert

70% support ephemeral DH (forwad encryption)

- Tunix: only 52% rate, due to use insecure ciphers

red color:

CAcert, Perfect Overheid, Quovadis Global, Nlnet Labs, 2Reclame, Nul77

Protocol issues with Quovadis Global, Nul77

gray color (C): Pink Roccade, Tunix

## comments on SSL/TLS configurations of Dutch web sites



- ♦ much is improved in one year! Well done, but still loose ends
- ♦ only ~0.4% is FIPS 140 ready
  - it ain't hard, OpenSSL certification for 30K US\$ only
- ♦ end-user:
  - Is still unable to require acceptable security level
  - browser lock only says: "maybe" secured to something
  - CA coloring only says "maybe" accredited CA at some point in time
  - lesson learned from Diginotar event: revocation is doubted
- ♦ once you have HTTPS, support SSL also on HTTP port
- ♦ have a look at the other applications: email-server, vpn, ssh, chat, etc.
- ♦ accreditation of CA's is doubtful, there is lack of reviewing and certification
- ♦ good **SSL/TLS configurations** is still far away

# Neelie: three basic things to do

my to-do list for Neelie Kroes



## 1. DNSSEC:

*host identification and validation*

not much progress in one year

## 2. X.509 CERT: *owner identification / validation*

lack of independent certified CA's procedure/review for end user and service provider

## 3. HTTP: **SSL/TLS cipher suites policy**

security policies defined, checked and maintained

configurations fixed, checked and maintained

validated -> certification procedures?

***ASSESS all work done in a open and public way***

Chock effects are the only tool to improve things...

Lucky enough: internet land is full of earth quakes

## Ross Anderson 2008

### phrase from his book

“We worried about crooks hacking bank smartcards, and put in lots of back-end protection for early electronic purses; the attack came on pay-TV smartcards instead, while the bank fraud folks concentrated on mag-stripe fall-back and on phishing.”