Public Key Infrastructures

Ralph Holz

Network Architectures and Services
Technische Universität München

November 2014

Part 2: Recent results – or: the sorry state of X.509

How This Got Our Interest (1)

PKI weaknesses in 2008

- Early December 2008:
  - 'Error' in Comodo CA: no identity check
  - Reported by Eddy Nigg of StartSSL (a CA)
  - A regional sub-seller just took the credit card number and gave you a certificate
  - No real reaction by Mozilla
- Late December 2008: whitehat hacks StartSSL CA
  - Technical report: simple flaw in Web front-end
  - Certificate for `mozilla.com` issued
  - Caught by 2nd line of defence:
    human checks for high-value domains

How This Got Our Interest (1)

PKI weaknesses in 2008

- Early December 2008:
  - ‘Error’ in Comodo CA: no identity check
  - Reported by Eddy Nigg of StartSSL (a CA)
  - A regional sub-seller just took the credit card number and gave you a certificate
  - No real reaction by Mozilla
- Late December 2008: whitehat hacks StartSSL CA
  - Technical report: simple flaw in Web front-end
  - Certificate for `mozilla.com` issued
  - Caught by 2nd line of defence:
    human checks for high-value domains

How This Got Our Interest (1)

PKI weaknesses in 2008

- Early December 2008:
  - ‘Error’ in Comodo CA: no identity check
  - Reported by Eddy Nigg of StartSSL (a CA)
  - A regional sub-seller just took the credit card number and gave you a certificate
  - No real reaction by Mozilla
- Late December 2008: whitehat hacks StartSSL CA
  - Technical report: simple flaw in Web front-end
  - Certificate for `mozilla.com` issued
  - Caught by 2nd line of defence:
    human checks for high-value domains

How This Got Our Interest (2)

PKI weaknesses in 2009

- February 2009
  - New ‘easy’ attack on MD5 (‘MD5 considered harmful today’)
  - Demonstrated by issuing valid but fake CA certificate
  - ‘Fast’ reaction by vendors: MD5 to be disabled for signatures by 2012
- Spring 2009
  - J. Nightingale of Mozilla writes crawler to traverse HTTPs sites
  - Goal: determine number of MD5-signed certificates (11%)
  - This piece of software was made public, it’s our starting point

How This Got Our Interest (2)

PKI weaknesses in 2009

- February 2009
  - New ‘easy’ attack on MD5 (‘MD5 considered harmful today’)
  - Demonstrated by issuing valid but fake CA certificate
  - ‘Fast’ reaction by vendors: MD5 to be disabled for signatures by 2012
- Spring 2009
  - J. Nightingale of Mozilla writes crawler to traverse HTTPs sites
  - Goal: determine number of MD5-signed certificates (11%)
  - This piece of software was made public, it’s our starting point

How This Got Our Interest (2)

PKI weaknesses in 2009

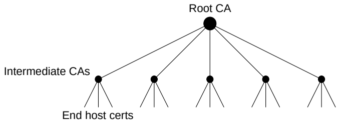
- February 2009
  - New ‘easy’ attack on MD5 (‘MD5 considered harmful today’)
  - Demonstrated by issuing valid but fake CA certificate
  - ‘Fast’ reaction by vendors: MD5 to be disabled for signatures by 2012
- Spring 2009
  - J. Nightingale of Mozilla writes crawler to traverse HTTPs sites
  - Goal: determine number of MD5-signed certificates (11%)
  - This piece of software was made public, it’s our starting point

How This Got Our Interest (3)

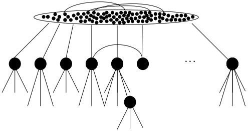
State of Mozilla Root Store

- Mozilla 2009: “Does anyone know who owns this root cert?”
- It turned out there were root certs that no-one could remember
- No-one could remember when they were accepted, or on which grounds

Ideal PKI



Involuntary ‘Bridge CA’ – Root Store



Kurt Seifried vs. RapidSSL

How to hijack a Web mailer in 3 easy steps

- Step 1: register e-mail address: `ssladministrator@portugalmail.pt`
- Step 2: ask RapidSSL for certificate for portugalmail.pt, giving this address as your contact
- Step 3: Watch ‘Domain Validation by e-mail probe’ fail

Kurt succeeded. It cost him $<$ 100 USD.

Main failure here:

- Web mailers and CAs have not agreed on ‘protected’ addresses
- This issue is now in Mozilla’s ‘Problematic practices’

How This Got Our Interest (4)

In 2011, the foundations of X.509 were rocked.

- March 2011: Comodo CA hacked (a sub-seller, again)
  - Attacker claims to come from Iran
  - ≈ 10 certificates for high-value domains issued
  - Browser reaction: blacklisting of those certificates *in code*
  - Neither CRLs nor OCSP trusted enough to work for victims
- July 2011: DigiNotar CA hacked
  - Attacker claims to be the same one as in March
  - 531 fake certificates, high-value domains
  - E.g., Google, Facebook, Mozilla, CIA, Mossad, Skype
  - Some hints pointed at Man-in-the-middle attack in Iran
  - The Netherlands' PKI was operated by DigiNotar...
  - For the first time, a Root CA is removed from a browser for being compromised

How This Got Our Interest (4)

In 2011, the foundations of X.509 were rocked.

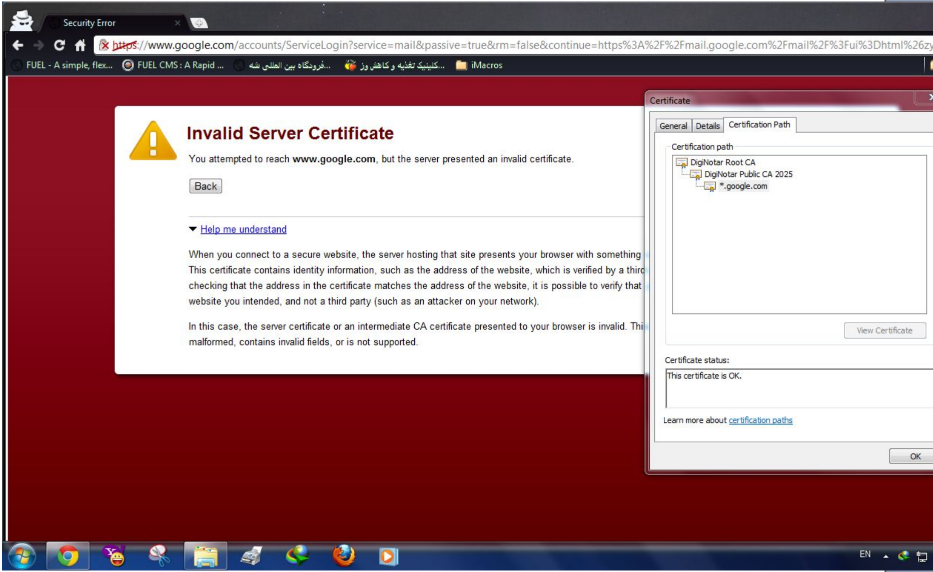
- March 2011: Comodo CA hacked (a sub-seller, again)
  - Attacker claims to come from Iran
  - $\approx$ 10 certificates for high-value domains issued
  - Browser reaction: blacklisting of those certificates *in code*
  - Neither CRLs nor OCSP trusted enough to work for victims
- July 2011: DigiNotar CA hacked
  - Attacker claims to be the same one as in March
  - 531 fake certificates, high-value domains
  - E.g., Google, Facebook, Mozilla, CIA, Mossad, Skype
  - Some hints pointed at Man-in-the-middle attack in Iran
  - The Netherlands' PKI was operated by DigiNotar...
  - For the first time, a Root CA is removed from a browser for being compromised

How This Got Our Interest (4)

In 2011, the foundations of X.509 were rocked.

- March 2011: Comodo CA hacked (a sub-seller, again)
  - Attacker claims to come from Iran
  - $\approx$ 10 certificates for high-value domains issued
  - Browser reaction: blacklisting of those certificates *in code*
  - Neither CRLs nor OCSP trusted enough to work for victims
- July 2011: DigiNotar CA hacked
  - Attacker claims to be the same one as in March
  - 531 fake certificates, high-value domains
  - E.g., Google, Facebook, Mozilla, CIA, Mossad, Skype
  - Some hints pointed at Man-in-the-middle attack in Iran
  - The Netherlands' PKI was operated by DigiNotar...
  - For the first time, a Root CA is removed from a browser for being compromised

DigiNotar vs. Iran?



Security Error
~~https~~://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy
FUEL - A simple, flex...
FUEL CMS : A Rapid ...
...فروشگاه بین المللی شه
...کلینیک تغذیه و کاهش وز
iMacros

Invalid Server Certificate

You attempted to reach **www.google.com**, but the server presented an invalid certificate.

When you connect to a secure website, the server hosting that site presents your browser with something This certificate contains identity information, such as the address of the website, which is verified by a third checking that the address in the certificate matches the address of the website, it is possible to verify that website you intended, and not a third party (such as an attacker on your network).

In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. Thi malformed, contains invalid fields, or is not supported.

- DigiNotar Root CA
  - DigiNotar Public CA 2025
    - *.google.com

Certificate status:

This certificate is OK.

Learn more about certification paths

Can We Assess the Quality of this PKI?

A good PKI should

- ... allow HTTPs on all WWW hosts
- ... contain only valid certificates
- ... offer good cryptographic security
  - Long keys, only strong hash algorithms, ...
- ... have a sensible setup
  - Short validity periods (1 year)
  - Short certificate chains (but use intermediate certificates)
  - Number of issuers should be reasonable (weakest link!)

Acquiring Our Data Sets

Active scans to measure *deployed* PKI

- Scan hosts on Alexa Top 1 million Web sites
- Nov 2009 – Apr 2011: scanned 8 times from Germany
- March 2011: scans from 8 hosts around the globe

Passive monitoring to measure *user-encountered* PKI

- Munich Research Network, monitored all SSL/TLS traffic
- Two 2-week runs in Sep 2010 and Apr 2011

EFF scan of IPv4 space in 2010

- Scan of 2-3 months, no *domain* information

In the meantime...

EFF scan presented at 27C3

- Focuses on CA certification structure
- Scan of IP addresses:
  does not allow to check match of host names
- No temporal distribution
- EFF project: SSL Observatory

Ivan Ristic of Qualys presents similar scan

- Smaller data basis
- Data set not published as raw data
- No temporal distribution
- Could not include it in our analysis

Our Data Sets

Active Scans — Passive Monitoring — EFF IPv4 scan

Location	*Time (run)*	*Type*	*Certificates*
Tuebingen, DE	November 2009	Active scan	833,661
Tuebingen, DE	December 2009	Active scan	819,488
Tuebingen, DE	January 2010	Active scan	816,517
Tuebingen, DE	April 2010	Active scan	816,605
Munich, DE	September 2010	Active scan	829,232
Munich, DE	November 2010	Active scan	827,366
Munich, DE	April 2011	Active scan	829,707
Munich, DE	April 2011	Active scan with SNI	826,098
Shanghai, CN	April 2011	Active scan	798,976
Beijing, CN	April 2011	Active scan	797,046
Melbourne, AU	April 2011	Active scan	833,571
İzmir, TR	April 2011	Active scan	825,555
São Paulo, BR	April 2011	Active scan	833,246
Moscow, RU	April 2011	Active scan	830,765
Santa Barbara, US	April 2011	Active scan	834,173
Boston, US	April 2011	Active scan	834,054
Munich, DE	September 2010	Passive monitoring	183,208
Munich, DE	April 2011	Passive monitoring	989,040
EFF servers	March–June 2010	Active IPv4 scan	11,349,678

25 million certificates to evaluate.

Our Data Sets

Active Scans — Passive Monitoring — EFF IPv4 scan

Location	*Time (run)*	*Type*	*Certificates*
Tuebingen, DE	November 2009	Active scan	833,661
Tuebingen, DE	December 2009	Active scan	819,488
Tuebingen, DE	January 2010	Active scan	816,517
Tuebingen, DE	April 2010	Active scan	816,605
Munich, DE	September 2010	Active scan	829,232
Munich, DE	November 2010	Active scan	827,366
Munich, DE	April 2011	Active scan	829,707
Munich, DE	April 2011	Active scan with SNI	826,098
Shanghai, CN	April 2011	Active scan	798,976
Beijing, CN	April 2011	Active scan	797,046
Melbourne, AU	April 2011	Active scan	833,571
İzmir, TR	April 2011	Active scan	825,555
São Paulo, BR	April 2011	Active scan	833,246
Moscow, RU	April 2011	Active scan	830,765
Santa Barbara, US	April 2011	Active scan	834,173
Boston, US	April 2011	Active scan	834,054
Munich, DE	September 2010	Passive monitoring	183,208
Munich, DE	April 2011	Passive monitoring	989,040
EFF servers	March–June 2010	Active IPv4 scan	11,349,678

25 million certificates to evaluate.

Our Data Sets

Active Scans — Passive Monitoring — EFF IPv4 scan

Location	*Time (run)*	*Type*	*Certificates*
Tuebingen, DE	November 2009	Active scan	833,661
Tuebingen, DE	December 2009	Active scan	819,488
Tuebingen, DE	January 2010	Active scan	816,517
Tuebingen, DE	April 2010	Active scan	816,605
Munich, DE	September 2010	Active scan	829,232
Munich, DE	November 2010	Active scan	827,366
Munich, DE	April 2011	Active scan	829,707
Munich, DE	April 2011	Active scan with SNI	826,098
Shanghai, CN	April 2011	Active scan	798,976
Beijing, CN	April 2011	Active scan	797,046
Melbourne, AU	April 2011	Active scan	833,571
İzmir, TR	April 2011	Active scan	825,555
São Paulo, BR	April 2011	Active scan	833,246
Moscow, RU	April 2011	Active scan	830,765
Santa Barbara, US	April 2011	Active scan	834,173
Boston, US	April 2011	Active scan	834,054
Munich, DE	September 2010	Passive monitoring	183,208
Munich, DE	April 2011	Passive monitoring	989,040
EFF servers	March–June 2010	Active IPv4 scan	11,349,678

25 million certificates to evaluate.

Our Data Sets

Active Scans — Passive Monitoring — EFF IPv4 scan

Location	*Time (run)*	*Type*	*Certificates*
Tuebingen, DE	November 2009	Active scan	833,661
Tuebingen, DE	December 2009	Active scan	819,488
Tuebingen, DE	January 2010	Active scan	816,517
Tuebingen, DE	April 2010	Active scan	816,605
Munich, DE	September 2010	Active scan	829,232
Munich, DE	November 2010	Active scan	827,366
Munich, DE	April 2011	Active scan	829,707
Munich, DE	April 2011	Active scan with SNI	826,098
Shanghai, CN	April 2011	Active scan	798,976
Beijing, CN	April 2011	Active scan	797,046
Melbourne, AU	April 2011	Active scan	833,571
İzmir, TR	April 2011	Active scan	825,555
São Paulo, BR	April 2011	Active scan	833,246
Moscow, RU	April 2011	Active scan	830,765
Santa Barbara, US	April 2011	Active scan	834,173
Boston, US	April 2011	Active scan	834,054
Munich, DE	September 2010	Passive monitoring	183,208
Munich, DE	April 2011	Passive monitoring	989,040
EFF servers	March–June 2010	Active IPv4 scan	11,349,678

25 million certificates to evaluate.

Our Data Sets

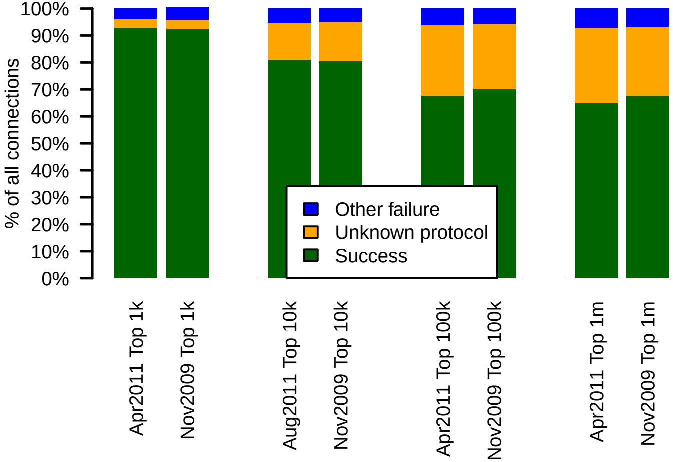
Active Scans — Passive Monitoring — EFF IPv4 scan

Location	*Time (run)*	*Type*	*Certificates*
Tuebingen, DE	November 2009	Active scan	833,661
Tuebingen, DE	December 2009	Active scan	819,488
Tuebingen, DE	January 2010	Active scan	816,517
Tuebingen, DE	April 2010	Active scan	816,605
Munich, DE	September 2010	Active scan	829,232
Munich, DE	November 2010	Active scan	827,366
Munich, DE	April 2011	Active scan	829,707
Munich, DE	April 2011	Active scan with SNI	826,098
Shanghai, CN	April 2011	Active scan	798,976
Beijing, CN	April 2011	Active scan	797,046
Melbourne, AU	April 2011	Active scan	833,571
İzmir, TR	April 2011	Active scan	825,555
São Paulo, BR	April 2011	Active scan	833,246
Moscow, RU	April 2011	Active scan	830,765
Santa Barbara, US	April 2011	Active scan	834,173
Boston, US	April 2011	Active scan	834,054
Munich, DE	September 2010	Passive monitoring	183,208
Munich, DE	April 2011	Passive monitoring	989,040
EFF servers	March–June 2010	Active IPv4 scan	11,349,678

25 million certificates to evaluate.

Errors in TLS Connection Setup

Scans from Germany, Nov 2009 and Apr 2011

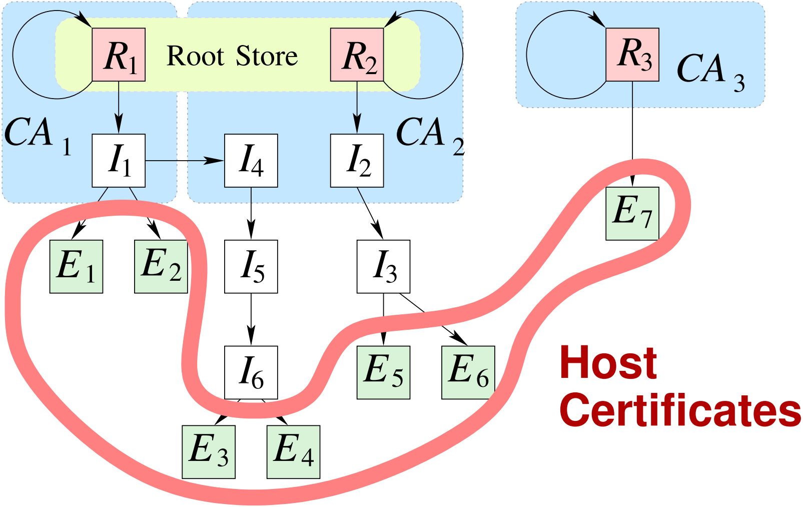


Errors in TLS Connection Setup

`UNKNOWN PROTOCOL`

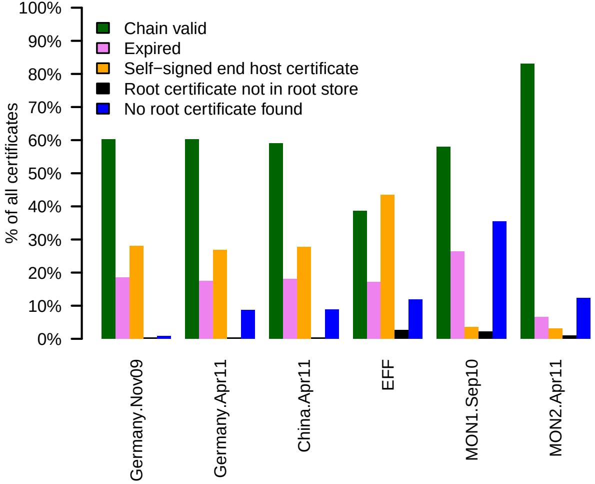
- Rescanned those hosts and manual sampling
- Always plain HTTP...
- ... and always an `index.html` with HTML 2 ...
- Hypothesis: old servers, old configurations
- More likely to happen in the lower ranks

Validity of End-Hosts Certificates



Validation of Certificate Chains

Just check chains, not host names



Correct Domain Name in Certificate

Now also check host names

- Look in Common Name (CN) and Subject Alternative Name (SAN)
- Munich, April 2011, only valid chains:
  - 12.2% correct CN
  - 5.9% correct SAN

Only 18% of certificates are fully verifiable

- Positive ‘trend’: from 14.9% in 2009 to 18% in 2011

Unusual Host Names

CN=plesk or similar

- Found in 7.3% of certificates
- Verified: Plesk/Parallels panels

CN=localhost

- 4.7% of certificates
- Very common: redirection to HTTP after HTTPs

Host Names in Self-signed Certificates

Self-signed means:

- Issuer the same as subject of certificate
- Requires out-of-band distribution of certificate

Active scan

- **2.2%** correct Common Name (CN)
- **0.5%** correct Subject Alternative Name

Top 3 most frequent CNs account for $>$ 50%

- `plesk` or similar in 27.3%
- `localhost` or similar in 25.4% – standard installations?

Certificate Occurrences

Many certificates valid for more than one domain

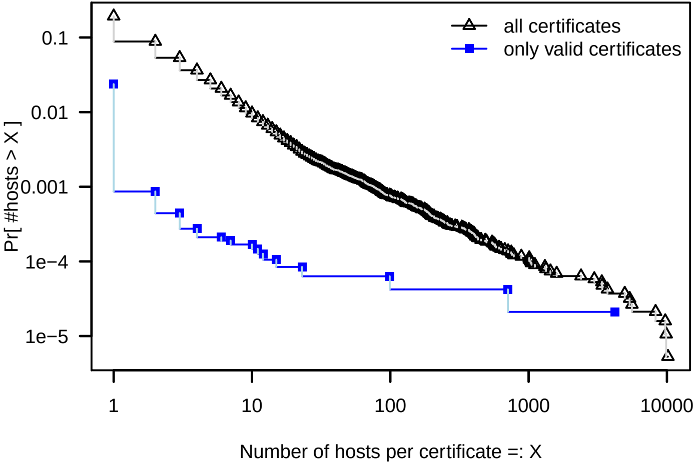
- Domains served by same IP
- Some certificates issued for dozens of domains
- Certificate reuse on multiple machines increases options for attacker

Often found on hosters

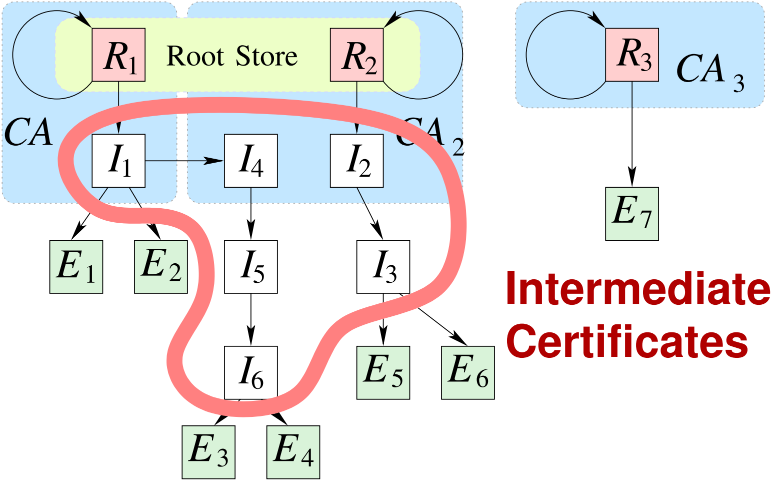
- E. g. `*.blogger.com`, `*.wordpress.com`

Certificate Occurrences

How often does a certificate occur on X hosts?

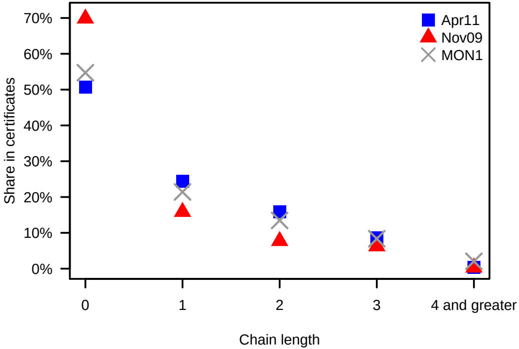


Certificate Chains



Intermediate Certificates

Certificate Chain Lengths

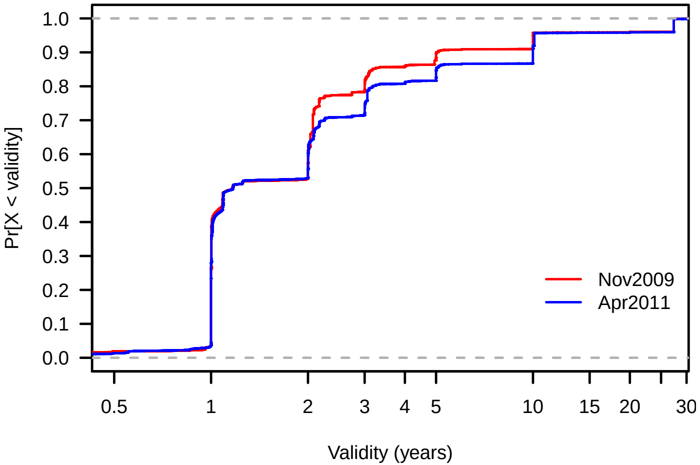


Finding more positive than negative:

- Trend to use intermediate certificates more often
- Allows to keep Root Certificates offline
- But chains still reasonably short

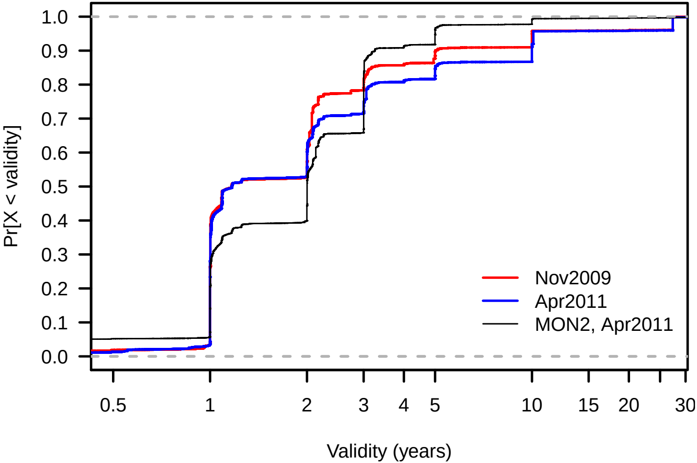
Validity Periods

CDF of validity periods, active scans



Validity Periods

CDF of validity periods, scans and monitoring



Public Key Properties

Key types

- RSA: 99.98% (rest is DSA)
- About 50% have length 1,024 bit
- About 45% have length 2,048 bit
- Clear trend from 1,024 to 2,048 bit

Weird encounters

- 1,504 distinct certificates that share another certificate's key
- Many traced to a handful of hosting companies
- Nadiah Henninger's work: Embedded devices, poor entropy!
- `www.factorable.net`

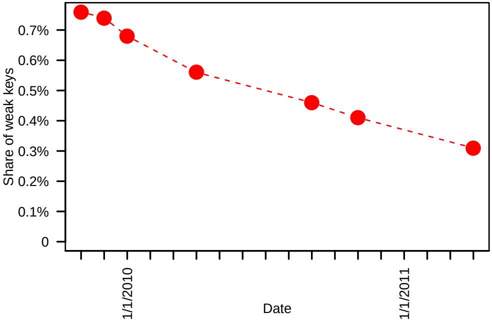
Debian Weak Keys (1)

Bug of 2008

- Generation of random numbers weak (bad initialisation)
- Only 2^{16} public/private key-pairs generated
- Allows pre-computation of private keys
- Debian ships blacklist of keys

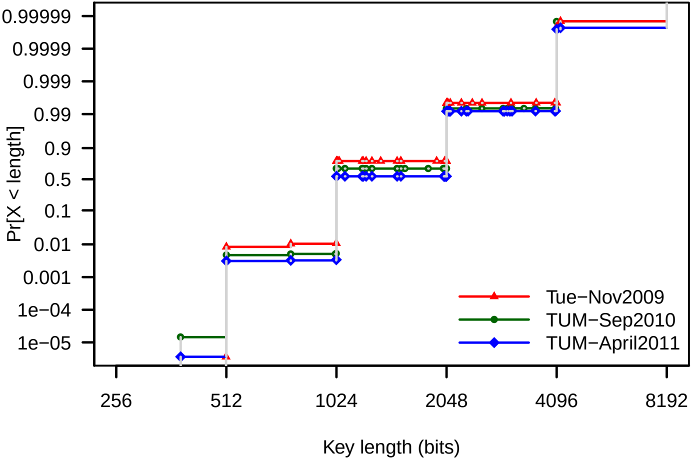
Debian Weak Keys (2)

Weak randomness in key generation – serious bug of 2008



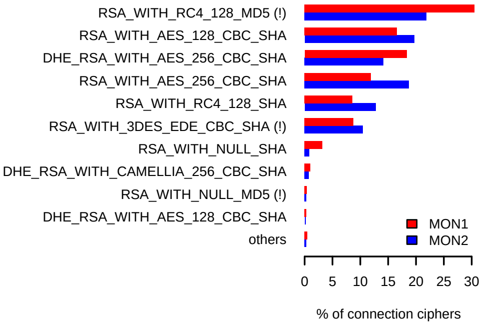
Public Key Lengths

CDF for RSA key lengths – double-log Y axis



Symmetric Ciphers

Results from monitoring

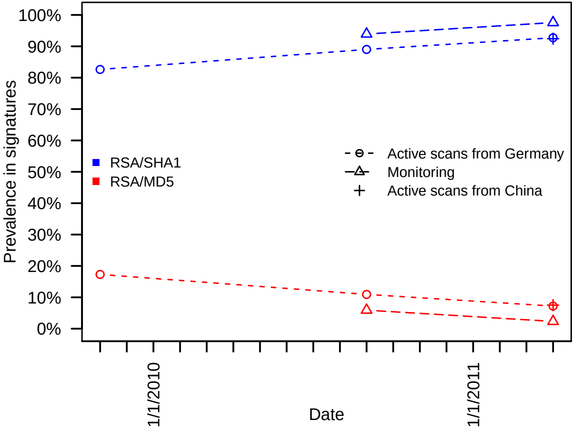


(Mostly) in line with results from 2007 by Lee et al.

- Order of AES and RC4 has shifted, RC4-128 most popular

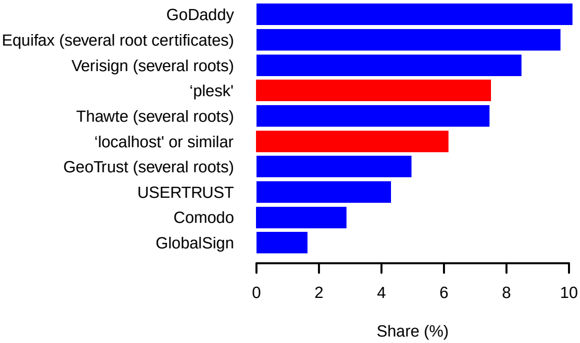
Signature Algorithms

MD5 is being phased out



Certificate Issuers

Very few CAs account for $>$ 50% of certificates



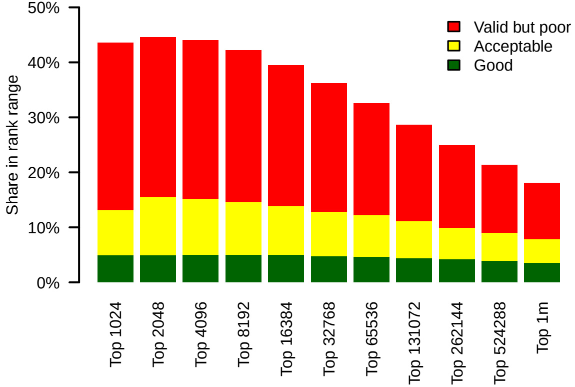
But there are 150+ Root Certificates in Mozilla.

Certificate Quality

We defined 3 categories

- ‘Good’:
  - Correct chains, correct host name
  - Chain ≤ 2
  - No MD5, strong key of > 1024 bit
  - Validity ≤ 13 months
- ‘Acceptable’
  - Chain ≤ 3, validity ≤ 25 months
  - Rest as above
- ‘Poor’: the remainder

Certificate Quality



Validity correlates with rank

- Share of ‘poor’ certificates higher among high-ranking sites

Conclusion

In great part, the X.509 PKI is in a sorry state

- Only 18% of the Top 1 Million Web sites show fully valid certificates
- Invalid chains
  - Expired certificates are common
  - Often no recognisable Root Certificate
  - Lack of correct domain information information
- Frequent sharing of certificates between hosts is problematic
- Much carelessness

Conclusion

Certification practices are very poor. But crypto OK.

Some positive developments

- Very slight trend for fully valid certificates
- Chains short, intermediate certificates used
- Key lengths OK
- Weak MD5 algorithm is being phased out