Certificate Authority Collapse

Will the EU Succeed in Regulating HTTPS?

Institute for Information Law
University of Amsterdam

@axelarnbak

29c3, Hamburg, 28 December 2012

Cloud Computing, Patriot Act, FISAA

CBSNews.com / CBS Evening News / CBS This Morning / 48 Hours / 60 Minutes / Sunday Morning / Face the Nation

CBSNEWS Video | US | World | Politics | Entertainment | Health | MoneyWatch | SciTech | Sports | Crime | More | Log In

By ZACK WHITTAKER / CBS NEWS / December 4, 2012, 3:59 PM

Patriot Act can "obtain" data in Europe, researchers say

AP FILE

Comment / Shares / 15 Tweets / Stumble / Email More +

LONDON | European data stored in the "cloud" could be acquired and inspected by U.S. law enforcement and intelligence agencies, despite Europe's strong data protection laws, university researchers have suggested.

The research paper, titled "Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act," written by legal experts at the University of Amsterdam's Institute for Information Law, support previous reports that the anti-terror Patriot Act could be theoretically used by U.S. law enforcement to bypass strict European privacy laws to acquire citizen data within the European Union.

Most Popular

01 Poll: GOP to blame if "fiscal cliff" talks fail — 32612 views

02 Prince William visits pregnant Kate in hospital — 28634 views

03 Obama signals wiggle room in "fiscal cliff" talks — 25030 views

04 Zimmerman's lawyers release bloody nose photo — 22078 views

05 Man pushed in front of NYC subway train, killed — 19795 views

12 Photos
Victoria's Secret "Fantasy Bra" through the years

Paper ‘Certificate Authority Collapse’ Work in Progress!

ABOUT | PEOPLE | RESEARCH | PUBLICATIONS | TEACHING | EVENTS | INTERACTIVE

BERKMAN CENTER FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

Certificate Authority Collapse

Nico A.N.M. van Eijk & Axel Arnbak, Institute for Information Law

sep **20** 2012

Thursday, September 20, 12:30 pm
Wasserstein Hall, Room 3018
RSVP required for those attending in person via the form below
This event will be archived on our site shortly after.

Hypertext Transfer Protocol Secure (‘HTTPS’) has evolved into the de facto standard for secure web browsing. Through the certificate-based authentication protocol, web services and internet users protect valuable communications and transactions against interception and alteration by cybercriminals, governments and business. In only one decade, it has facilitated trust in a thriving global E-Commerce economy, while every internet user has come to depend on HTTPS for social, political and economic activities on the internet.

Recent breaches and malpractices at several Certificate Authorities (CA’s) have led to a collapse of trust in these central mediators of HTTPS communications as they revealed ‘fundamental weaknesses in the design of HTTPS’ (ENISA 2011). In particular, the breach at Dutch CA Diginotar shows how a successful attack on one of the 650 Certificate Authorities across 54 jurisdictions enables attackers to create false SSL-certificates for any given website or service. Moreover, Diginotar kept the breach silent. So for 90 days, web browsers continued to trust Diginotar certificates, enabling attackers to intercept the communications of 300.000 Iranians. In its aftermath, Dutch public authorities overtook operations at Diginotar and convinced Microsoft to delay updates to its market-leading web browser to ensure ‘the continuity of the internet’. These bold interventions lacked a legitimate basis.

While serving as the de facto standard for secure web browsing, in many ways the security of HTTPS is broken. Given our dependence on secure web browsing, the security of HTTPS has become a top priority in telecommunications policy. In June

SSRN: http://ssrn.com/abstract=2031409

Outline Presentation

- HTTPS Authentication Model
- DigiNotar hack
  - landmark breach
  - Insightful, illegitimate mitigation
  - Pretty damn good story
- Systemic vulnerabilities
- EU eSignatures Regulation: Will the EU Succeed?
- Regulating HTTPS: What to do?
  - Not about best tech alternative

Main Messages

- HTTPS Authentication is broken, someone needs to fix it
- That someone, is not the legislature – it is you!
- The eSignatures proposal will do more harm than good
- When regulating HTTPS, be humble on technology, and focus on:
  - Apprising all underlying values: economy, comsec **and** digital rights
  - All stakeholders involved, not only CAs
  - Optimising economic and bureaucratic incentives

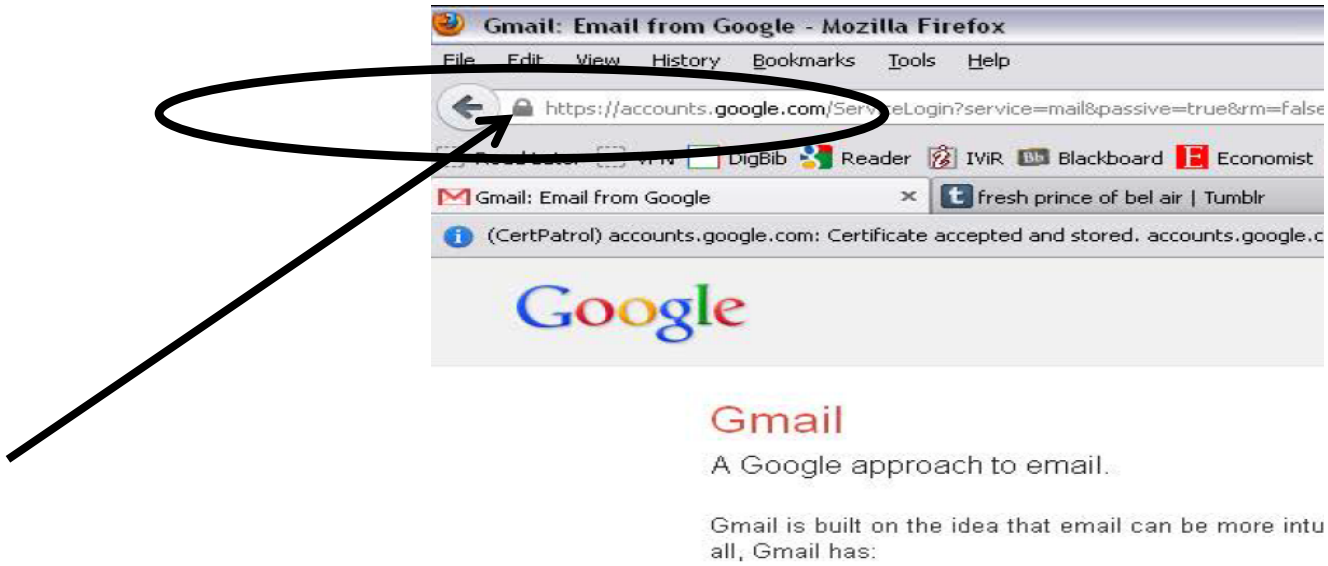
Outline Presentation

- HTTPS Authentication Model
- DigiNotar hack
  - landmark breach
  - Insightful, illegitimate mitigation
  - Pretty damn good story
- Systemic vulnerabilities
- EU eSignatures Regulation: Will the EU Succeed?
- Regulating HTTPS: What to do?
  - Not about best tech alternative

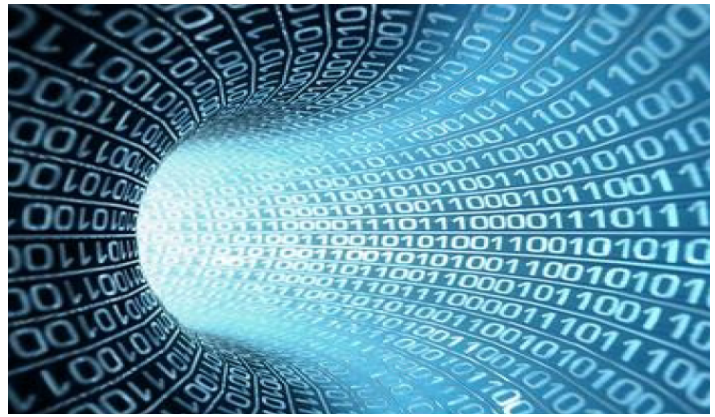
HTTPS


https://www.
Free hi-res JPG file download - Resolution 4800x3500 px - www.psdgraphics.com

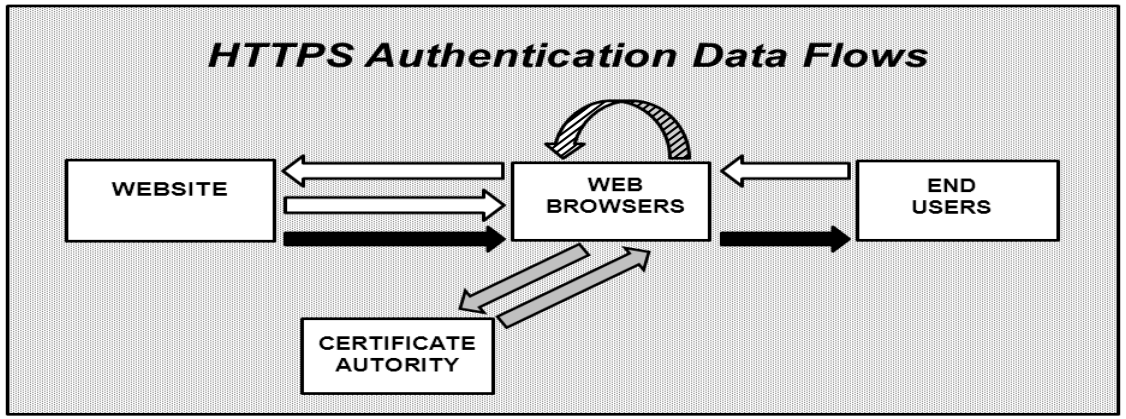
The Padlock


Gmail: Email from Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false
DigBib Reader IViR Blackboard Economist
Gmail: Email from Google
fresh prince of bel air | Tumblr
(CertPatrol) accounts.google.com: Certificate accepted and stored. accounts.google.c
Google
Gmail
A Google approach to email.
Gmail is built on the idea that email can be more intu
all, Gmail has:

HTTPS: Handshake → Encryption



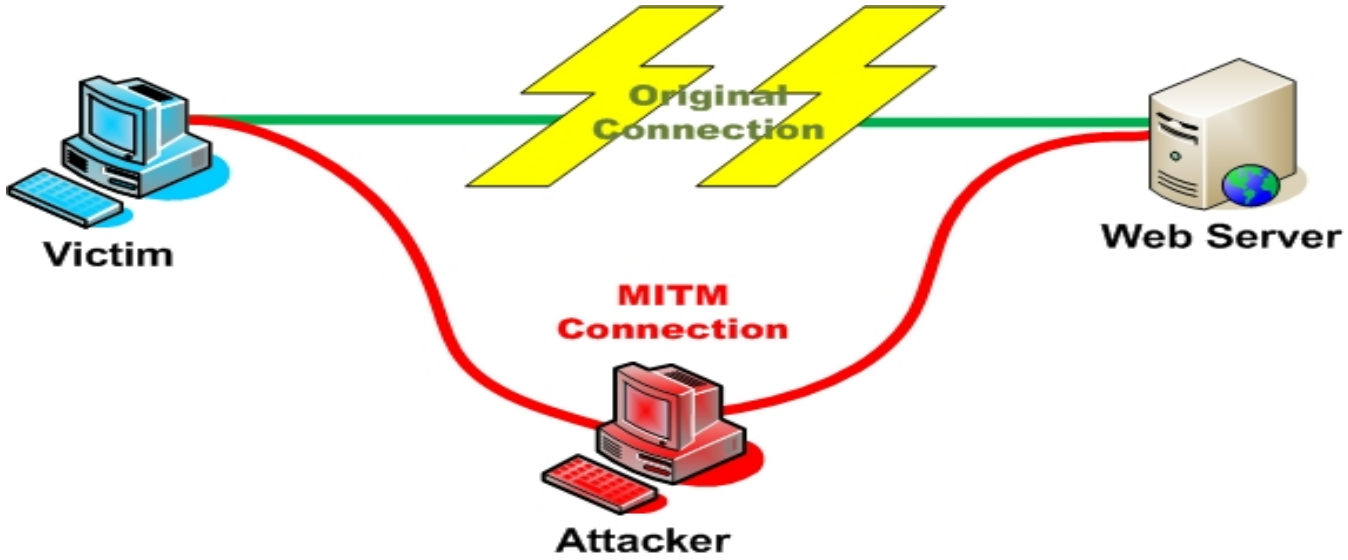
Data Flows HTTPS Authentication



Data Flows: 4 Phases

1. *White* = *HTTPS request and SSL Certificate offering*
2. *Pattern* = *CA Root verification*
3. *Grey* = *Certificate signature verification (OSCP)*
4. *Black* = *'Handshake' – authentication*

Prevents (?) Man in the Middle Attack



Security HTTPS Authentication Crucial For

- De facto standard for ‘secure’ browsing
- $8 Trillion E-Commerce market (McKinsey, 2011)
- (Relative) confidential communications internet users
  - Governments
  - Business
  - Consumers
- Software patches
- Machine-to-machine communications

Outline Presentation

- HTTPS Authentication Model
- DigiNotar hack
  - Landmark breach
  - Insightful, illegitimate mitigation
  - Pretty damn good story
- Systemic vulnerabilities
- EU eSignatures Regulation: Will the EU Succeed?
- Regulating HTTPS: What to do?
  - Not about best tech alternative

DigiNotar


zeker weten met wie u via
internet afspraken maakt
www.diginotar.nl
DigiNotar
Internet Trust Services
sche handtekening

Root Certificate Authority

DigiD

‘One server to rule them all’

Security Practises?

Username:

PRODUCTION\Administrator

Password:

Pr0d@dm1n

DigiNotar: 30 Software Updates Ignored

DutchNews.nl

FRIDAY 28 DECEMBER 2012

Home | Opinion | Features | International | In Dutch | Dictionary | What's On | Jo

«« previous next »»

Services

- New to Amsterdam and in need of a helping hand? Expats in Amsterdam
- Rent an open boat in Amsterdam with Sloep Huren Amsterdam
- Delicious food provided by Catering Amsterdam
- Make the most of your teeth with Dentist Amsterdam

DigiNotar hack made possible as 30 software updates were ignored

Sunday 18 November 2012

Last year's hack of Dutch digital security company DigiNotar was due to aging software which was at least 30 updates out of date, website nu.nl reported on Sunday.

In addition, news of the hack only became public knowledge a month after the site had been disabled, documents obtained by nu.nl using freedom of information show.

The information comes from research carried out by internet security firm ITsec on behalf of DigiNotar before the hack was in the public domain.

Security certificates

DigiNotar's systems were hacked in mid-July 2011 and over 500 website security certificates were stolen, including ones for intelligence services like the CIA, Mossad and MI6. Experts said at the time they thought Iran was behind the attack and that Iranian dissidents were the main target.

A preliminary report for the government by internet research group Fox-IT into DigiNotar also revealed the company used old software and did not have sufficient security measures in place.

False certificates

- Forensic report:

5 Appendix

5.1 Fraudulent issued certificates

The following list of Common Names in certificates are presumed to be generated by the attacker(s):

Common Name	Number of certs issued
CN=*.*.com	1
CN=*.*.org	1
CN=*.10million.org	2
CN=*.JanamFadayeRahbar.com	1
CN=*.RamzShekaneBozorg.com	1
CN=*.SahebeDonyayeDigital.com	1
CN=*.android.com	1
CN=*.aol.com	1
CN=*.azadegi.com	1
CN=*.balatarin.com	3
CN=*.comodo.com	3
CN=*.digicert.com	2
CN=*.globalsign.com	7
CN=*.google.com	26
CN=*.logmein.com	1
CN=*.microsoft.com	3
CN=*.mossad.gov.il	2
CN=*.mozilla.org	1
CN=*.skype.com	22
CN=*.startssl.com	1
CN=*.thawte.com	6
CN=*.torproject.org	14
CN=*.walla.co.il	2
CN=*.windowsupdate.com	3
CN=*.wordpress.com	14
CN=Comodo Root CA	20
CN=CyberTrust Root CA	20
CN=DigiCert Root CA	21
CN=Equifax Root CA	40
CN=GlobalSign Root CA	20
CN=Thawte Root CA	45
CN=VeriSign Root CA	21
CN=addons.mozilla.org	17
CN=azadegi.com	16
CN=friends.walla.co.il	8
CN=login.live.com	17
CN=login.yahoo.com	19
CN=my.screenname.aol.com	1
CN=secure.logmein.com	17
CN=twitter.com	19
CN=wordpress.com	12
CN=www.10million.org	8
CN=www.Equifax.com	1
CN=www.balatarin.com	16
CN=www.cia.gov	25
CN=www.cybertrust.com	1
CN=www.facebook.com	14
CN=www.globalsign.com	1
CN=www.google.com	12
CN=www.hamdami.com	1
CN=www.mossad.gov.il	5
CN=www.sis.gov.uk	10
CN=www.update.microsoft.com	4

- 26: *.google.com
- 22: *.skype.com
- 14: *.torproject.org
- 20: Comodo Root CA
- 45: Thawte Root CA
- 17: addons.mozilla.org
- 4: update.microsoft.com
- 25: www.cia.gov

Targets of the MITM attack ...

10.2.5 Targets of the MITM attack

The accumulated affected IP addresses were plotted to provide an insight into how the MITM attack developed over time. It was noted that the number of affected IP addresses seemed to have grown fas from August 4, 2011 onwards.

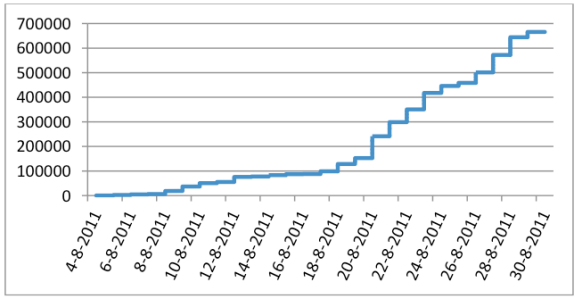


Figure 6 Cumulative number of originating IP addresses

The location information showed that 95% of the OCSP requests for the `*.google.com` certificate originated from Iran (634,665 out of the 665,974 OCSP requests). A1 in the figure below refers to 'Anonymous Proxy' according to the GeoIP results.

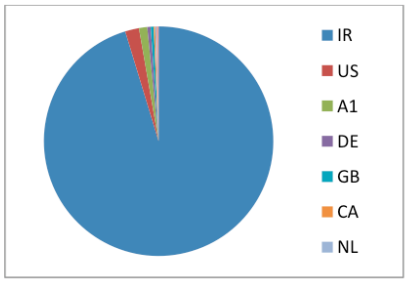


Figure 7 Originating country OCSP requests for the Google.com certificate

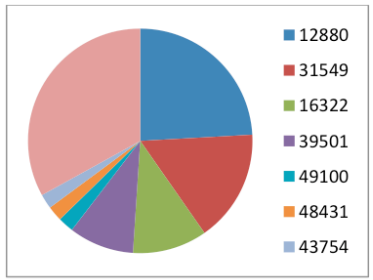


Figure 8 Originating Autonomous System Number (ASN) of the requests

... seem very uncertain

- OCSP logging highly contentious
  - Not supported by all browsers and clients
  - Could have been faked by attackers
- This seems the case. From the new forensic report:

In addition to the rogue `*.google.com` certificate, validation requests were made for serial numbers that correspond with known rogue certificates as well as for unknown serial numbers. Initially these requests were answered by the OCSP responder as if they were valid. This makes it plausible that other rogue and unknown certificates may have been used for other MITM attacks on a much smaller scale. An attempt

http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf

Clearly…

…how to fix it?

Dutch Government Got off to a Good Start: 'Stop Using Teh Interwebz!'

Donner ontraadt internet

Van onze parlementaire redactie

DEN HAAG, zaterdag

Minister Donner (Binnenlandse Zaken) heeft een opmerkelijk advies voor mensen die twijfelen aan de betrouwbaarheid van internet door de problemen met veiligheidscertificaten.

„Doe dat niet meer, werk net als ik met brieven en overschrijvingsbiljetten", aldus de 62-jarige bewindsman.

- Minister Donner:

"Don't do it; use <u>letters and bank cheques</u>, just like me"

De Telegraaf, Frontpage, 5 Sept. 2011:

The Man Who Saved Teh Interwebz

Mitigation Measures Taken

- Government overtook Diginotar
  - ‘Enforcement on a private law basis’ ??
  - ‘We had to show our teeth’
- Diginotar Trust Revocation Delayed in Dutch Market
  - Patch to remove Diginotar Root status delayed for weeks

- Mitigation labeled ‘success story’ in bureaucratic circles
- Perhaps good reasons, but the mitigation **illegitimate**
- What was the role of Microsoft in all this?

Policy Responses: The 18 Months after

- 06 June 2011: Possibly first exploration by the attacker(s)
- 19 June: Incident detected by DigiNotar by daily audit procedure
- 10 July: The first succeeded rogue certificate (*.google.com)
- 04 August: Start massive activity of *.google.com
- 27 August: First mention of *.google.com certificate in blog
- 29 August: DigiNotar's *.google.com certificate is revoked
- 2-3 September 2011: Dutch government takes over DigiNotar
- All September: Microsoft delays automatic security patches
- Until August 2012: Govt still allows DigiNotar certificates!

Policy Responses: The 18 Months after

- 06 June 2011: Possibly first exploration by the attacker(s)
- 19 June: Incident detected by DigiNotar by daily audit procedure
- 10 July: The first succeeded rogue certificate (*.google.com)
- 04 August: Start massive activity of *.google.com
- 27 August: First mention of *.google.com certificate in blog
- 29 August: DigiNotar's *.google.com certificate is revoked
- 2-3 September 2011: Dutch government takes over DigiNotar
- All September: Microsoft delays automatic security patches
- Until August 2012: Govt still allows DigiNotar certificates!

Dutch Gov't Still Allows DigiNotar Certs!

English Papiamento Papiamentu Other languages Contact Abonneren RSS Vacatures Sitemap Help

Rijksoverheid

Home Nieuws Onderwerpen Ministeries Regering Documenten en publicaties Doe mee Zoek

Home > Nieuws > Belastingdienst waarschuwt adviseurs die nog gebruik maken van Diginotar certificaten

Nieuws

> Nieuwsoverzicht

Belastingdienst waarschuwt adviseurs die nog gebruik maken van Diginotar certificaten

Nieuwsbericht | 23-07-2012

De Belastingdienst ontvangt nog steeds aangiftes van belastingadviseurs die gebruik maken van oude Diginotar BAPI-certificaten. Het gaat om fiscaal dienstverleners die verantwoordelijk zijn voor 6% van het totaal aantal aangiftes. Zij zijn er de afgelopen maanden meer malen op gewezen dat zij voor 1 juli moesten overstappen op nieuwe certificaten. Inmiddels hebben ruim 15.000 adviseurs een nieuw certificaat.

Adviseurs die nog niet zijn overgestapt krijgen nu nog een brief met de waarschuwing dat ze nog steeds gebruik maken van oude certificaten. Zo nodig zal de Belastingdienst ook nog telefonisch contact opnemen. Vanaf begin augustus kunnen aangiften met een Diginotar certificaat helemaal niet meer worden ingestuurd en zal de aangifte niet in behandeling worden genomen.

Verantwoordelijk ministerie

> Ministerie van Financiën

Zie ook

> Belasting betalen
Onderwerp | Financiën

Vragen?
Bel Informatie Rijksoverheid:
1400

… HTTPS: widely used, high risk …

- Global socio-technical system
- A wide range of incidents
- An ‘essential facility’ – world depends on HTTPS
- Breaches have serious damages (financial/non financial)
- Unjustified trust increases damage
- No regulatory framework in place

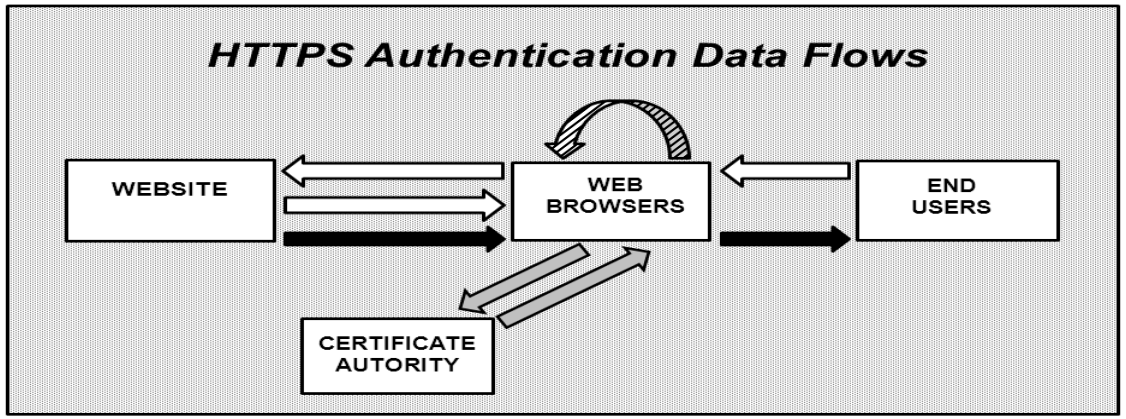
Outline Presentation

- HTTPS Authentication Model
- DigiNotar hack
  - landmark breach
  - Insightful, illegitimate mitigation
  - Pretty damn good story
- Systemic vulnerabilities
- EU eSignatures Regulation: Will the EU Succeed?
- Regulating HTTPS: What to do?
  - Not about best tech alternative

Systemic Security Vulnerabilities

- Systemic ↔ incidental
  - Many, many, many systemic vulnerabilities
  - Known for a long time in security community
- Described in paper: § 2 & § 3
- To name a few …

Data Flows HTTPS Authentication



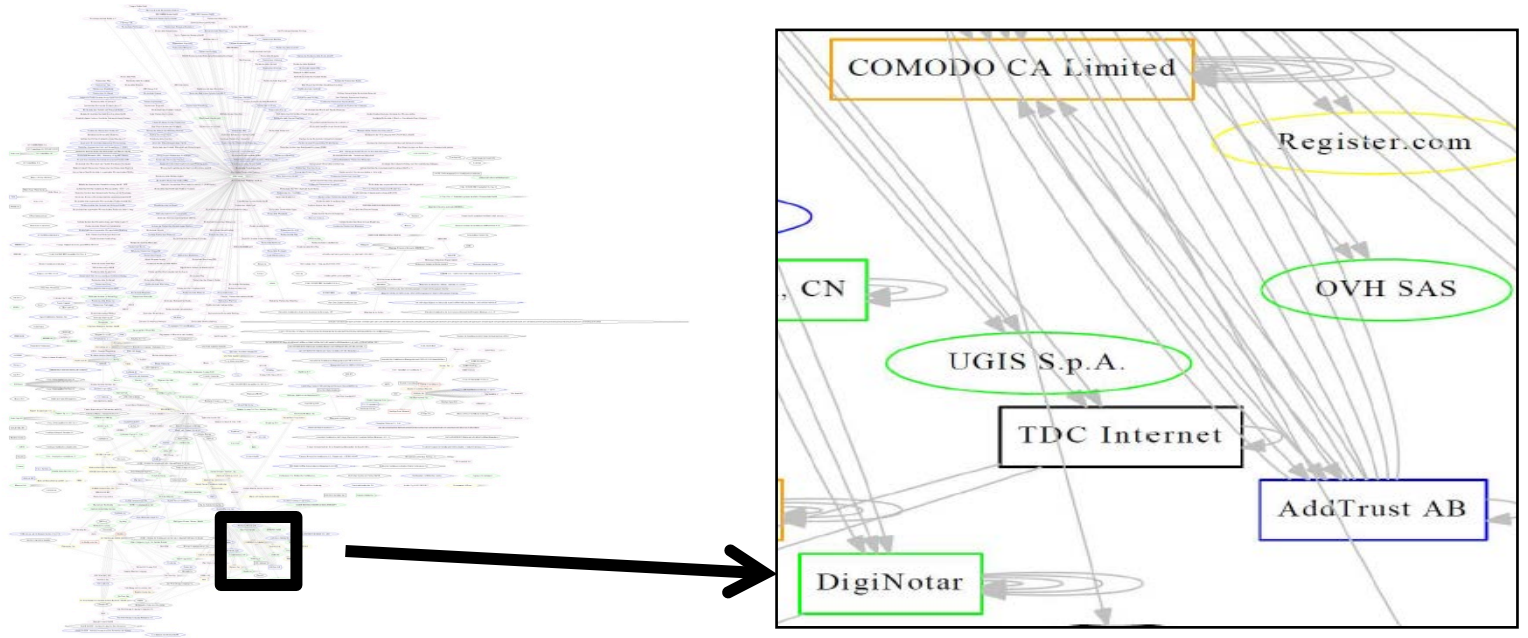
Data Flows: 4 Phases

1. *White* = *HTTPS request and SSL Certificate offering*
2. *Pattern* = *CA Root verification*
3. *Grey* = *Certificate signature verification (OSCP)*
4. *Black* = *'Handshake' – authentication*

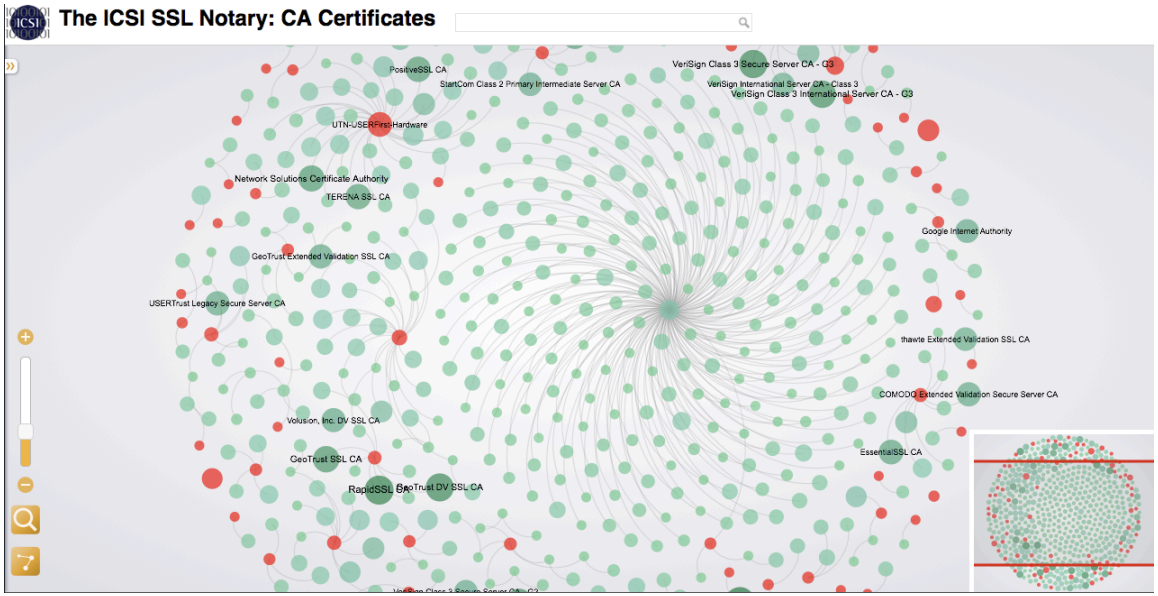
Any CA can vouch for any domain name, or: Any CA single point of failure entire system

AOL
LIVEJOURNAL
orange
VeriSign
Microsoft
plaxo
Google
myspace.com
a place for friends.
Technorati
Blogger
WordPress
YAHOO!

EFF SSL Observatory: 650+ CA's, 54 jurisdictions, 50+ government-owned

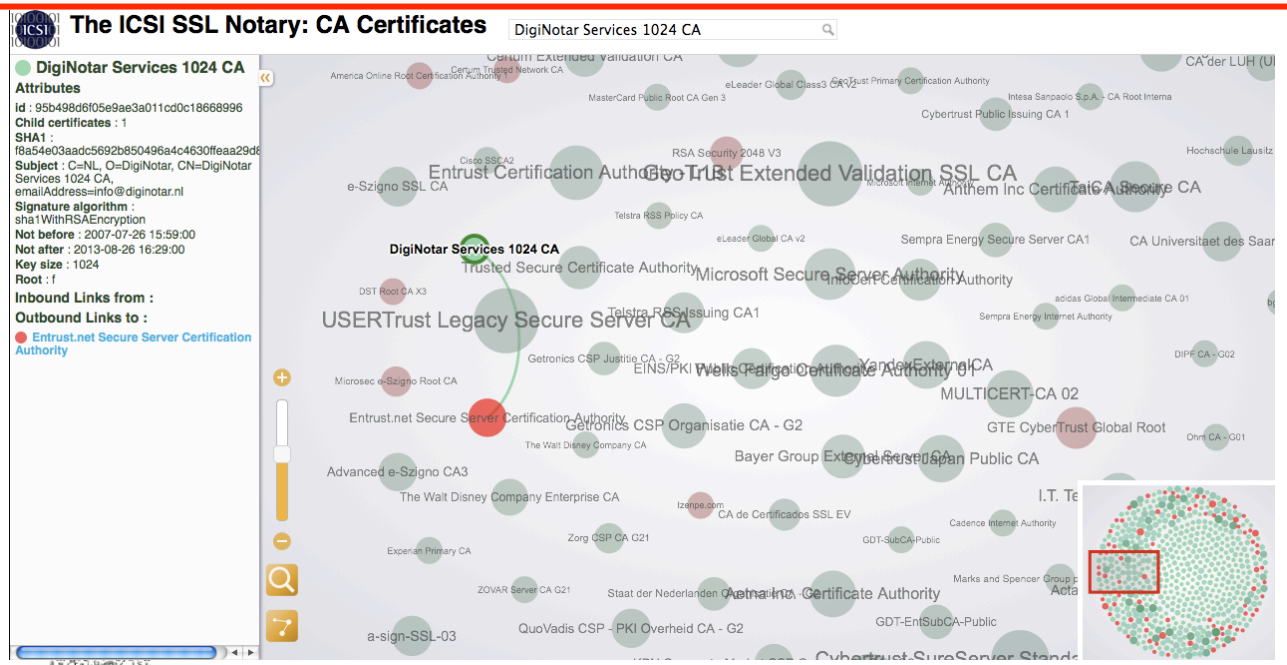


UC Berkeley: ICSI SSL Notary Trust Tree



http://notary.icsi.berkeley.edu/trust-tree/

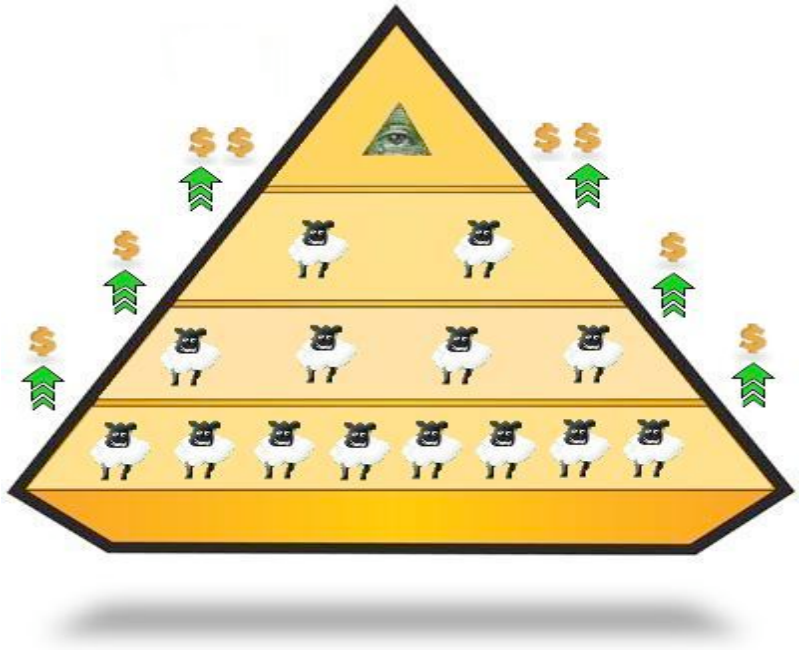
DigiNotar, Still Up and Running!



Root CA status: Browser Trust by Default

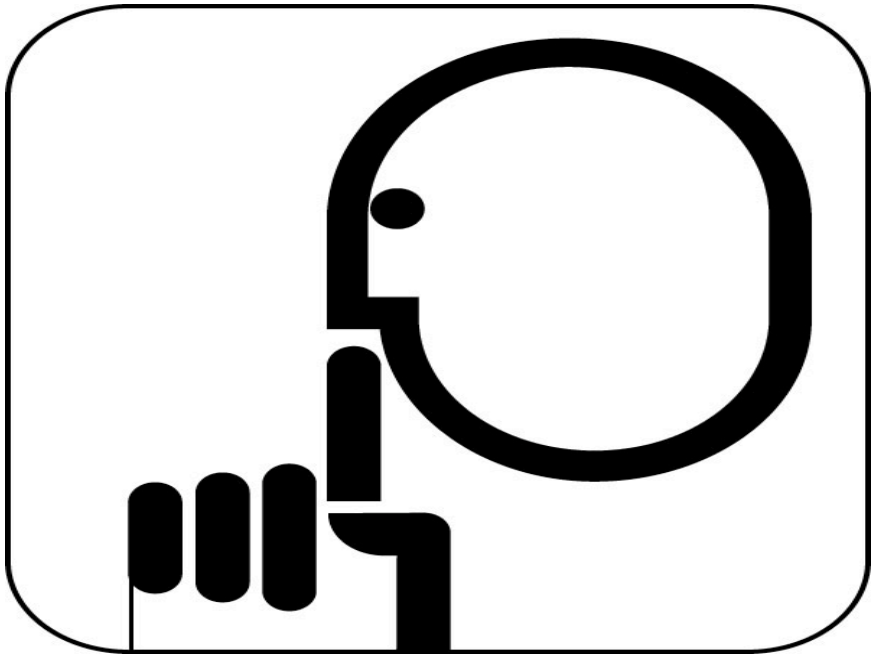
IV2R

Root CA versus intermediate CA: Thriving market for subletting root status



Attribution Problem: actor and intent unknown

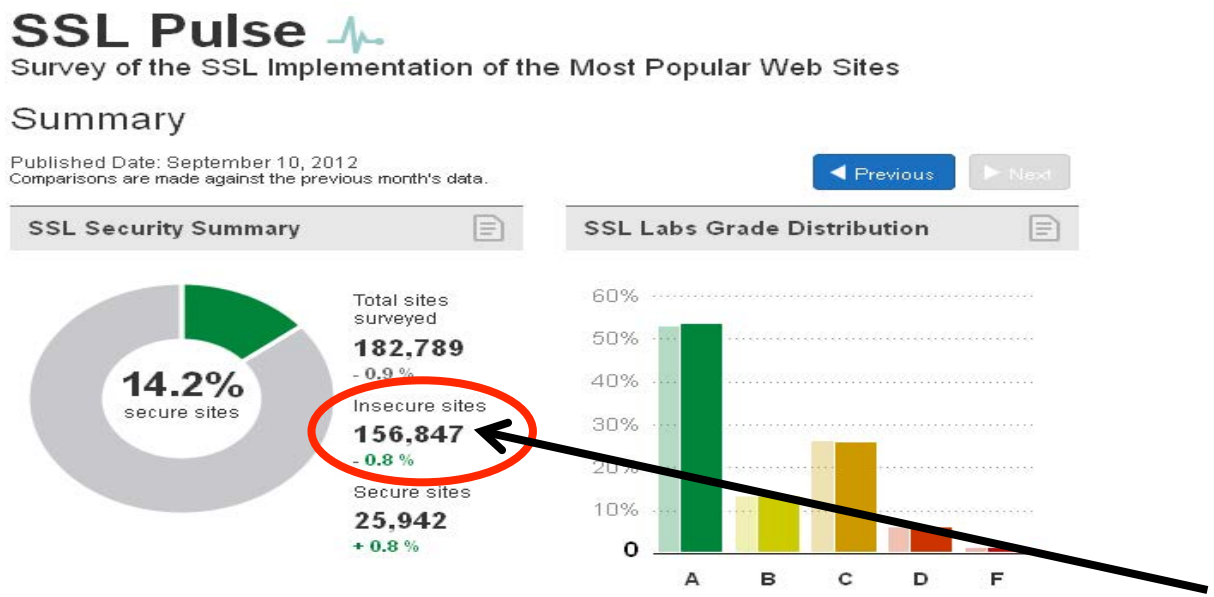
Information asymmetries



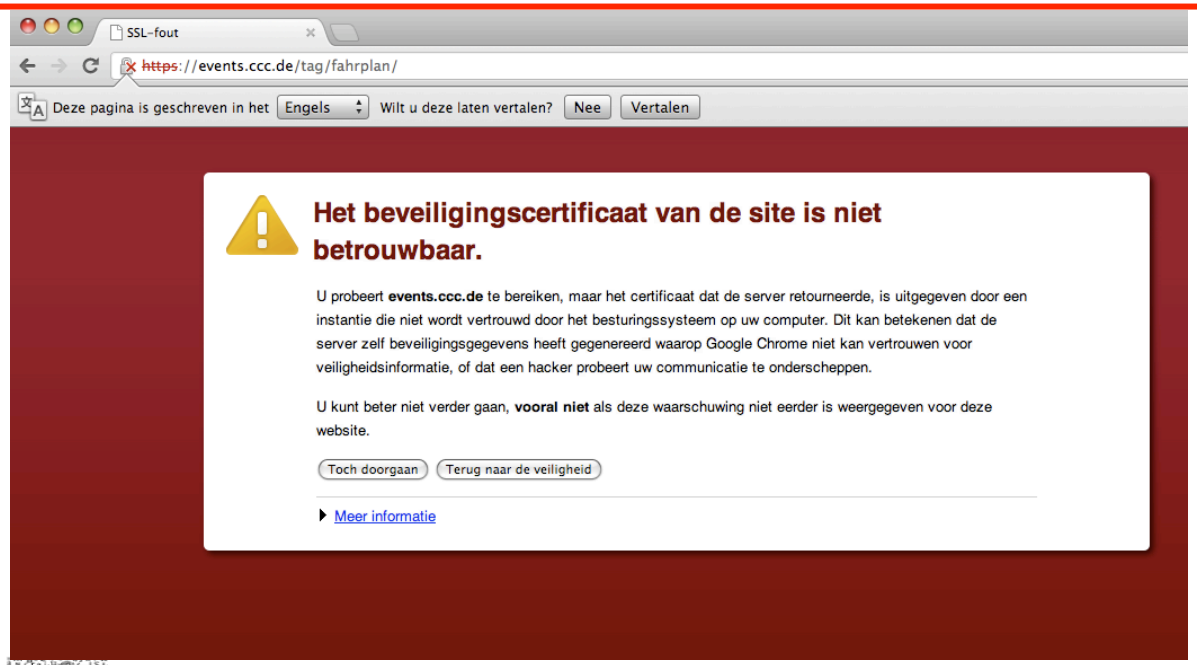
Browsers re certificate/CA trust revocation: trade-off connectivity ↔ security

- End-user: connectivity
- Depends on responses CA
- CA trust, scale risk factor
  - The bigger, the harder
    - Fx. Comodo

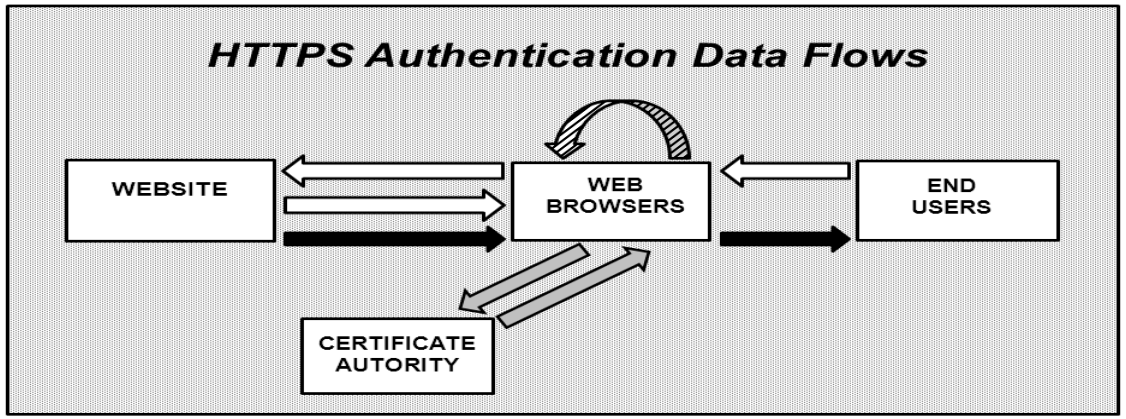
Websites Implement HTTPS Poorly



End Users? Go Figure!



So, Every Stakeholder Part of the Problem



Data Flows: 4 Phases

1. *White* = *HTTPS request and SSL Certificate offering*
2. *Pattern* = *CA Root verification*
3. *Grey* = *Certificate signature verification (OSCP)*
4. *Black* = *'Handshake' – authentication*

But… Every stakeholder part of solution?

Outline Presentation

- HTTPS Authentication Model
- DigiNotar hack
  - landmark breach
  - Insightful, illegitimate mitigation
  - Pretty damn good story
- Systemic vulnerabilities
- EU eSignatures Regulation: Will the EU Succeed?
- Regulating HTTPS: What to do?
  - Not about best tech alternative

EU Proposal: eSignatures Regulation

- eSignatures Regulation
  - Proposal by European Commission in June 2012
  - Ordinary legislative procedure
    - Ping pong: EU Council ↔ EU Parliament
  - **Red Flag**: Once adopted, direct binding force in 27 Member States
- Paradigm shift in the making
  - Unregulated environment
  - Strictly regulated after adoption?

Contents eSignatures Proposal

- All crucial issues discussed in § 4 paper:
  - Rationale regulation
  - Scope
  - New provisions introduced for ‘trust service providers’:
    - Liability
    - Security Requirements
    - Security Breach Notification
    - Supervision

In focus: scope

- EU proposal
  - 'Trust service providers' established in EU
    - Includes CA's issuing SSL certificates
- Other critical stakeholders unregulated
  - Explanatory memo. hints at requirements for websites
  - But: 'responsibility of the HTTPS market'
    - Exceptionally poor argument: 'not all EU organisations are securing their website' (p. 35 & 87 Imp. Assessment)
- Real consequence: disproportionate burden on subset of HTTPS value chain

In focus: liability [1]

- EU proposal, art. 9(1):
  - *'liable for any direct damage (..) due to failure to comply with Article 15(1), unless (..) he has not acted negligently.'*
    - » Art. 15(1): open security norm – 'state of the art'
- Other stakeholders unmentioned
  - Websites: cheap certificates / poor HTTPS implementation?
  - Untimely patching by browsers, OS manufacturers?
  - Software liability?

In focus: liability [2]

- Real consequences
  - Liability may be helpful to incentivise CA's
    - Security practises
    - Proper logging, as they bear burden of proof
  - But art. 9(1):
    - 'Any direct damage'
      - Single company liable for entire HTTPS system?
        - » DigiNotar liable for damages Google, Microsoft?
        - » Favourable to incumbents able to pay insurance fees

Outline Presentation

- HTTPS Authentication Model
- DigiNotar hack
  - landmark breach
  - Insightful, illegitimate mitigation
  - Pretty damn good story
- Systemic vulnerabilities
- EU eSignatures Regulation: Will the EU Succeed?
- Regulating HTTPS: What to do?
  - Not about best tech alternative

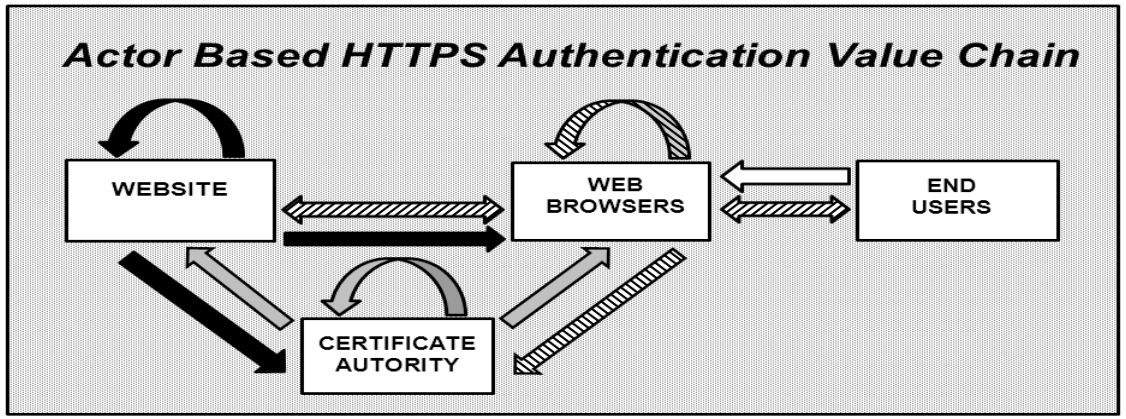
IViR

Not About Best Technical Solution???

- Law cannot force technology development
- IETF is your forum, Harry Halpin seems to be your man!
  - http://events.ccc.de/congress/2012/Fahrplan/events/5374.en.html
- But law may help to incentivise economic and political actors

EU Parliament: Ehm… HTTPS ???

‘Value’ Chain Approach: stakeholder interactions, impact security



HTTPS Value Flows

1. *End User (white)* = *HTTPS Request, Valuable Information*
2. *Browser (pattern)* = *Verification of CA Root Application*
   = *Verification of Certificate*
   = *HTTPS Communication Conduit*
3. *CA (grey)* = *CA Root Status Application with Browsers*
   = *SSL Certificate sale to Website*
   = *OCSP Responses to Browsers*
   = *Certificate Revocation*
4. *Website (black)* = *SSL Certificate purchase with CA*
   = *SSL Certificate offering to browser*
   = *SSL server implementation*

IV2R

Broader Findings: Regulating Systemic Design Flaws

- Global socio-technical system hard to regulate
- Requires robust technical (and policy) solutions
  - Marlinspike: IETF proposal on 'TACK Pinning'
  - Google: CA pinning
  - Firefox add-ons: CertPatrol, HTTPS Everywhere, etc.
- Even if adopted, critical vulnerabilities remain
- Perpetual effort absolutely vital

Broader Findings: HTTPS Governance

- Make full set of underlying values explicit
  - E-Commerce, trust, reliable communications, etc.
  - Information security entails more than ‘availability’
- Apprise constitutional values
  - privacy, communications freedom, etc.
- Provide solid legal basis for exercise executive power
- Adopt ‘value’ chain approach
  - Identify all stakeholders and their interactions
- Analyse if incentives lead to desired outcomes: security economics

Glimpse of Future Work

- Enhancing paper with empirical data
  - SSL Observatory, ICSI Trust Tree
- Ph.D. project 'Communications Security Governance'
  - What is, and how should regulators approach comsec?
    - Define underlying values and interests
    - Develop framework for balancing them
  - What are structural legal vulnerabilities to comsec?
  - What is regulation good for in global socio-technical systems?
  - New case studies, similar to HTTPS

Main Messages

- HTTPS Authentication is broken, someone needs to fix it
- That someone, is not the legislature – it is you!
- The eSignatures proposal will do more harm than good
- When regulating HTTPS, be humble on technology, and focus on:
  - Apprising all underlying values: economy, comsec **and** digital rights
  - All stakeholders involved, not only CAs
  - Optimising economic and bureaucratic incentives

Discussion

More information in paper

- SSRN: http://ssrn.com/abstract=2031409
- References to amongst others:
  - Forensic Reports DigiNotar hack
  - EFF SSL Observatory
  - Moxie Marlinspike
    - Black Hat talks
    - IETF proposal
  - Chris Soghoian & Sid Stamm: ‘Certified Lies’
  - Princeton: Freedom to Tinker blog, Steve Schultze & Steve Roosa

Contact Info

Institute for Information Law (IViR)
University of Amsterdam
http://www.ivir.nl

A.M. Arnbak, LL.M. – a.m.arnbak@uva.nl, @axelarnbak