Digi who?

Diginotar, DANE, and DNSSEC Deployment

Olaf Kolkman

Fronted by

Geoff Huston

Need I say more?

DigiNotar®
A VASCO COMPANY

Ah well, a quick summary

A Certificate Authority

Home Diginotar internet trust ser… lektronische handtekening.

http://www.diginotar.nl/

Google

Daily ▾ Mijn ING Triodos AG (1) The Selvedge Yard (3… Tools ▾ IAB ▾ NLnetLabs Boeken

Home Diginotar internet trust ser…

DigiNotar®
A VASCO COMPANY

HOME | ACTUEEL | … | KLANTENSERVICE | OVER DIGINOTAR

zoek… zoek

Zorgeloos documenten online uitwisselen
Hoe toont u aan dat uw document de originele en geautoriseerde versie is en dat het bij de juiste persoon komt?
Meer >>

Certificaten | Contact | FAQ

Ga direct naar …

- Digitale Polis
- Elektronische handtekening WABO
- Overgang certificaten
- SHA256 certificaten en sleutellengte 2048
- Tarieven certificaten

Lopende projecten

Belastingdienst Ga

DigiNotar®, Internet Trust Provider

Dé onafhankelijke partij voor het identificeren van personen en organisaties op internet en veilig digitaal documenten uitwisselen, ondertekenen en bewaren.

Expertise in o.a. online identiteiten, veilig documenten uitwisselen, privacy services, elektronisch factureren, mobiele pki, (EV)SSL, pseudonimisatie, digitale kluis, authenticatie, elektronische handtekening
Meer info >>

eHerkenning

eHerkenning

Actueel

> **Faillissement DigiNotar**
De Rechtbank Haarlem heeft op dinsdag 20 september 2011 het faillissement uitgesproken van Diginotar B.V. onder aanstelling van mr. R. Mulder tot cura…

> **DigiNotar failliet. Overheid blijft betrokken bij operationeel beheer**
Lees hier het persbericht

> **Besluit OPTA om de registratie van DigiNotar als certificatiedienstverlener in te trekken**
De OPTA heeft op 13 september jl. besloten om de registratie van DigiNotar als leverancier van gekwalificeerde elektronische handtekeningen (certifica…

Meer nieuws…

A Bankrupt Certificate Authority

Home Diginotar internet trust services, certificaten, elektronische handtekening.

http://www.diginotar.nl/

Google

Daily ▾ Mijn ING Triodos AG (1) The Selvedge Yard (3) BLOGs (979) ▾ AUTO ▾ TV&Media ▾ ools ▾ IAB ▾ NLnetLabs Boeken

Home Diginotar internet trust ser...

DigiNotar®
A VASCO COMPANY

HOME | ACTUEEL | PROD | KLANTENSERVICE | OVER DIGINOTAR

zoek

online uitwisselen

Hoe toont u aan dat uw document de originele en geautoriseerde versie is en dat het bij de juiste persoon komt?
Meer >>

Certificaten | Contact | FAQ

Ga direct naar ...

- Digitale Polis
- Elektronische handtekening WABO
- Overgang certificaten
- SHA256 certificaten en sleutellengte 2048
- Tarieven certificaten

Lopende projecten

Belastingdienst Ga

DigiNotar®, Internet Trust Provider

Dé onafhankelijke partij voor het identificeren van personen en organisaties op internet en veilig digitaal documenten uitwisselen, ondertekenen en bewaren.

Expertise in o.a. online identiteiten, veilig documenten uitwisselen, privacy services, elektronisch factureren, mobiele pki, (EV)SSL, pseudonimisatie, digitale kluis, authenticatie, elektronische handtekening
Meer info >>

eHerkenning

eHerkenning

Actueel

> **Faillissement DigiNotar**
De Rechtbank Haarlem heeft op dinsdag 20 september 2011 het faillissement uitgesproken van Diginotar B.V. onder aanstelling van mr. R. Mulder tot cura...

> **DigiNotar failliet. Overheid blijft betrokken bij operationeel beheer**
Lees hier het persbericht

> **Besluit OPTA om de registratie van DigiNotar als certificatiedienstverlener in te trekken**
De OPTA heeft op 13 september jl. besloten om de registratie van DigiNotar als leverancier van gekwalificeerde elektronische handtekeningen (certifica...

Meer nieuws...

Front-Page News

Iranian activists feel the chill as hacker taps into e-mails

BY SOMINI SENGUPTA

He claims to be 21 years old, a student of software engineering in Tehran who reveres Ayatollah Ali Khamenei and despises dissidents in his country.

He sneaked into the computer systems of a security firm on the outskirts of Amsterdam. He created fake credentials that could allow someone to spy on Internet connections that appeared to be secure. He then shared that bounty with people he declines to identify.

The fruits of his labor are believed to have been used to tap into the online communications of as many as 300,000 unsuspecting Iranians this summer. He punched a hole in an online security mechanism that is trusted by Internet users all over the world.

Comodohacker, as he calls himself, insists that he acted on his own and is unperturbed by the notion that his work might have been used to spy on anti-government compatriots.

"I'm totally independent," he said in an e-mail exchange with The New York Times. "I just share my findings with some people in Iran. They are free to do anything they want with my findings and things I share with them, but I'm not responsible."

In the annals of Internet attacks, this is most likely to go down as a moment of reckoning. For activists, it shows the

HACKER, PAGE 17

International Herald Tribune
Sep 13, 2011 Front Page

Events

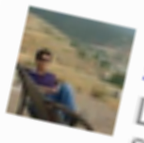
Chain of ~~trust~~

something fishy

Help forum > Gmail > Coffee Shop (off-topic) > Is This MITM Attack to Gmail's SSL ?

Report abuse

Is This MITM Attack to Gmail's SSL ?



alibo
Level 1
8/28/11

28 Aug 2011

Hi,
Today, when I trid to login to my Gmail account I saw a certificate warning in Chrome .
I took a screenshot and I saved certificate to a file .

this is the certificate file with screenshot in a zip file:
http://www.mediafire.com/?rrklb17slctityb

and this is text of decoded fake certificate:
http://pastebin.com/ff7Yg663

when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack (because I live in Iran and you may hear something about the story of Comodo hacker!)

http://www.google.com/support/forum/p/gmail/thread?tid=2da6158b094b225a

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%3D

FUEL - A simple, flex... | FUEL CMS : A Rapid ... | فرودگاه بین المللی شه... | کلینیک تغذیه و کاهش وز... | iMacros | Other bookmarks

Invalid Server Certificate

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

Back

Help me understand

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.

Certificate

General | Details | Certification Path

Certification path

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

View Certificate

Certificate status:

This certificate is OK.

Learn more about certification paths

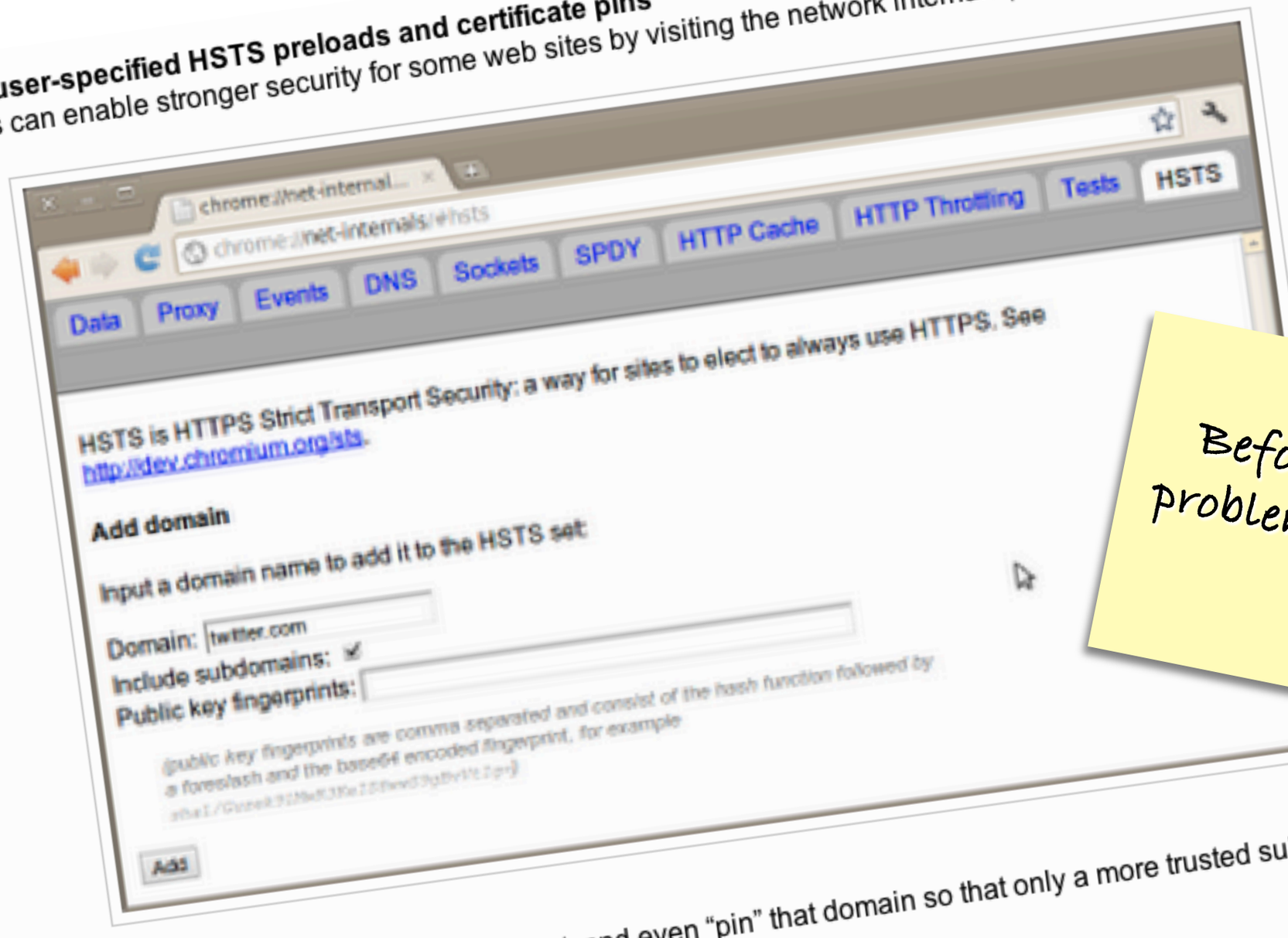
OK

4:06 PM
8/27/2011

Google Chrome magic caught this!

Chromium 12: user-specified HSTS preloads and certificate pins

Advanced users can enable stronger security for some web sites by visiting the network internals page: chrome://net-internals/#hsts

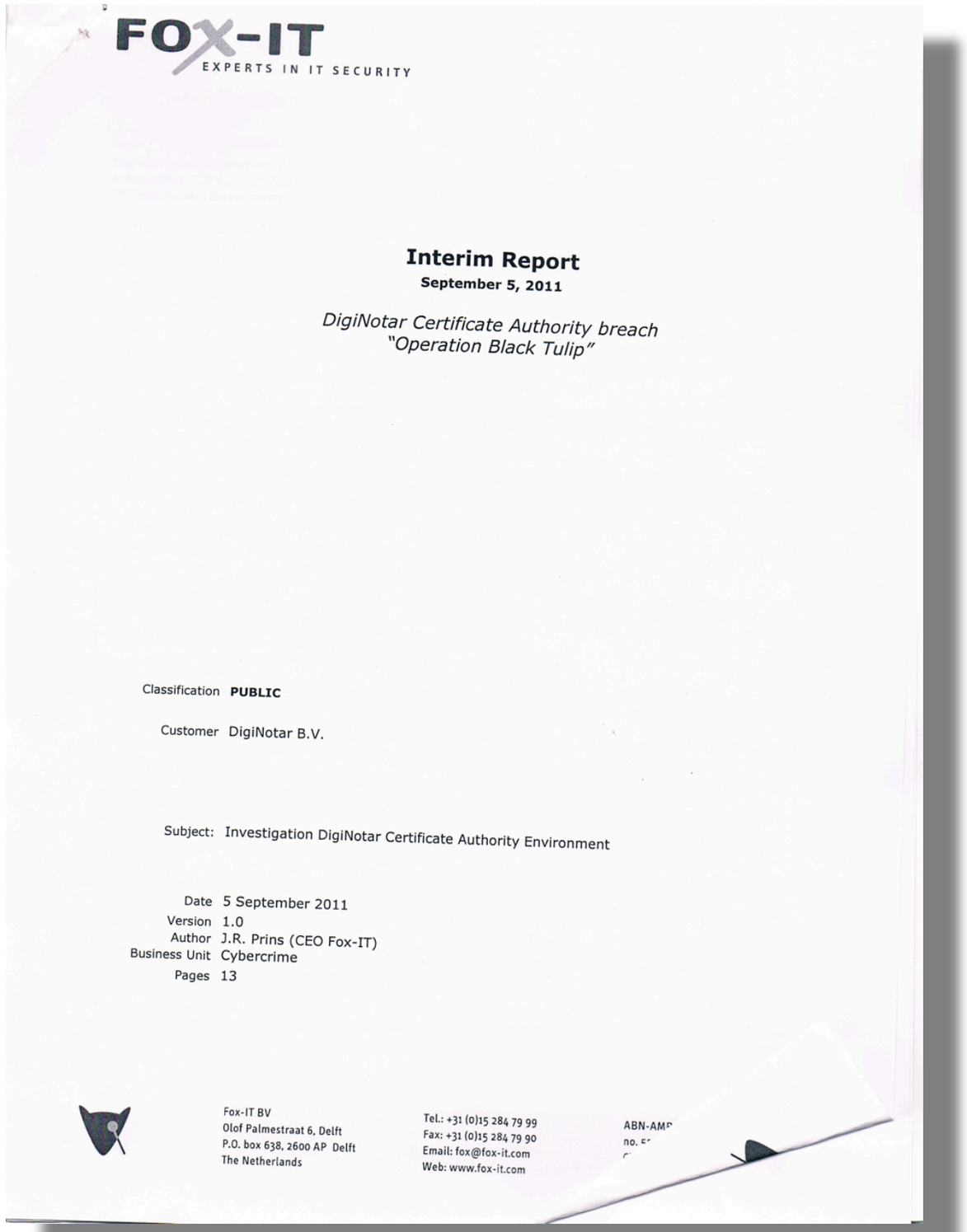


Before June 2011 the problem would not have shown

You can now force HTTPS for any domain you want, and even "pin" that domain so that only a more trusted subset of CAs are permitted to identify that domain.

It's an exciting feature but we'd like to warn that it's easy to break things! We recommend that only experts experiment with net internals settings.

http://blog.chromium.org/2011/06/new-chromium-security-features-june.html



FOX-IT
EXPERTS IN IT SECURITY

Interim Report
September 5, 2011

DigiNotar Certificate Authority breach
"Operation Black Tulip"

Classification **PUBLIC**

Customer DigiNotar B.V.

Subject: Investigation DigiNotar Certificate Authority Environment

Date 5 September 2011
Version 1.0
Author J.R. Prins (CEO Fox-IT)
Business Unit Cybercrime
Pages 13

Fox-IT BV
Olof Palmestraat 6, Delft
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: fox@fox-it.com
Web: www.fox-it.com

ABN-AMR
no. 5[illegible]

What went wrong?

http://www.diginotar.nl/Portals/7/Persberichten/Operation%20Black%20Tulip%20v1.0a.pdf

Compromised certificate issued by: DigiNotar® A VASCO COMPANY

Fox-IT hired to investigate

Earlier report (Jul 27): Compromise of External web servers

Incomplete audit trails

Multiple hacker tools on the servers

Specialized PKI scripts

Advanced and Amateur

Fingerprint Similarity to Comodo Hacker

And a claim by the guy

Hi again! I strike back again, huh?

I told all that I can do it again, I told all in interviews that I still have accesses in Comodo resellers, I told all I have access to most of CAs, you see that words now?

You know, I have access to 4 more so HIGH profile CAs, which I can issue certs from them too which I will, I won't name them, I also had access to StartCom CA, I hacked their server too with so sophisticated methods, he was lucky by being sitted in front of HSM for signing, I will name just one more which I still have access: GlobalSign, let me use these accesses and CAs, later I'll talk about them too..

I won't talk so many detail for now, just I wanted to let the world know that ANYTHING you do will have consequences, ANYTHING your country did in past, you have to pay for it...

I was sure if I issue those certificates for myself from a company, company will be closed and will not be able to issue certs anymore, Comodo was really really lucky!

I thought if I issue certs from Dutch Gov. CA, they'll lose a lot of money:
http://www.nasdaq.com/aspx/dynamic_charting.aspx?selected=VDSI&timeframe=6m&charttype=line

But I remembered something and I hacked DigiNotar without more thinking in anniversary of that mistake:
http://www.tepav.org.tr/en/kose-yazisi-tepav/s/2551

When Dutch government, exchanged 8000 Muslim for 30 Dutch soldiers and Animal Serbian soldiers killed 8000 Muslims in same day, Dutch government have to pay for it, nothing is changed, just 16 years has been passed. Dutch government's 13 million dollars which paid for DigiNotar will have to go DIRECTLY into trash, it's what I can do from KMs away! It's enough for Dutch government for now, to understand that 1 Muslim soldier worth 10000 Dutch government.

I'll talk technical details of hack later, I don't have time now... How I got access to 6 layer network behind internet servers of DigiNotar, how I found passwords, how I got SYSTEM privilage in fully patched and up-to-date system, how I bypassed their nCipher NetHSM, their hardware keys, their RSA certificate manager, their 6th layer internal "CERT NETWORK" which have no ANY connection to internet, how I got full remote desktop connection when there was firewalls that blocked all ports except 80 and 443 and doesn't allow Reverse or direct VNC connections, more and more and more...

After I explain, you'll understand how sophisticated attack it was, It will be a good hacking course for hackers like Anonymous and Lulzsec :) There was so many 0-day bugs, methods and skill shows...

Have you ever heard of XUDA programming language which RSA Certificate manager uses it? NO! I heard of it in RSA Certificate Manager and I learned programming in it in same night, it is so unusual like greater than sign in all programming languages is "<" but in XUDA it is "{"

Anyway... I'll talk about DigiNotar later! For now keep thinking about what Dutch government did in 16 years ago in same day of my hack, I'll talk later and I'll introduce to you MOST sophisticated hack of the year which will come more, you have to also wait for other CA's certificates to be used by me, then I'll talk about them too.

Interviews will be done via email ichsun [at] ymail.com

By the way, ask DigiNotar about this username/password combination: Username: PRODUCTION\Administrator (domain administrator of certificate network)Password: PrOd@dm1n

It's not all about passwords or cracking them,
1)you can't have remote desktop connection in a really closed and protected network by firewalls which doesn't allow Reverse VNC, VNC, remote desktop, etc. by packet detection.
2)2) you can't even dump hashes of domain if you don't have admin privilege to crack them
3)3) you can't access 6th layer network which have no ANY connection to internet from internet

Yeah!

Bye for now

http://pastebin.com/1AxH30em

A Rogue Certificate is Useful to an Adversary When:

1. The victim wants to go to the site where the attacker has a rogue certificate

2. The compromised certificate is not in a blacklist (OCSP CRL), or not checked otherwise

3. The attacker can divert the user's traffic (Man in the Middle)

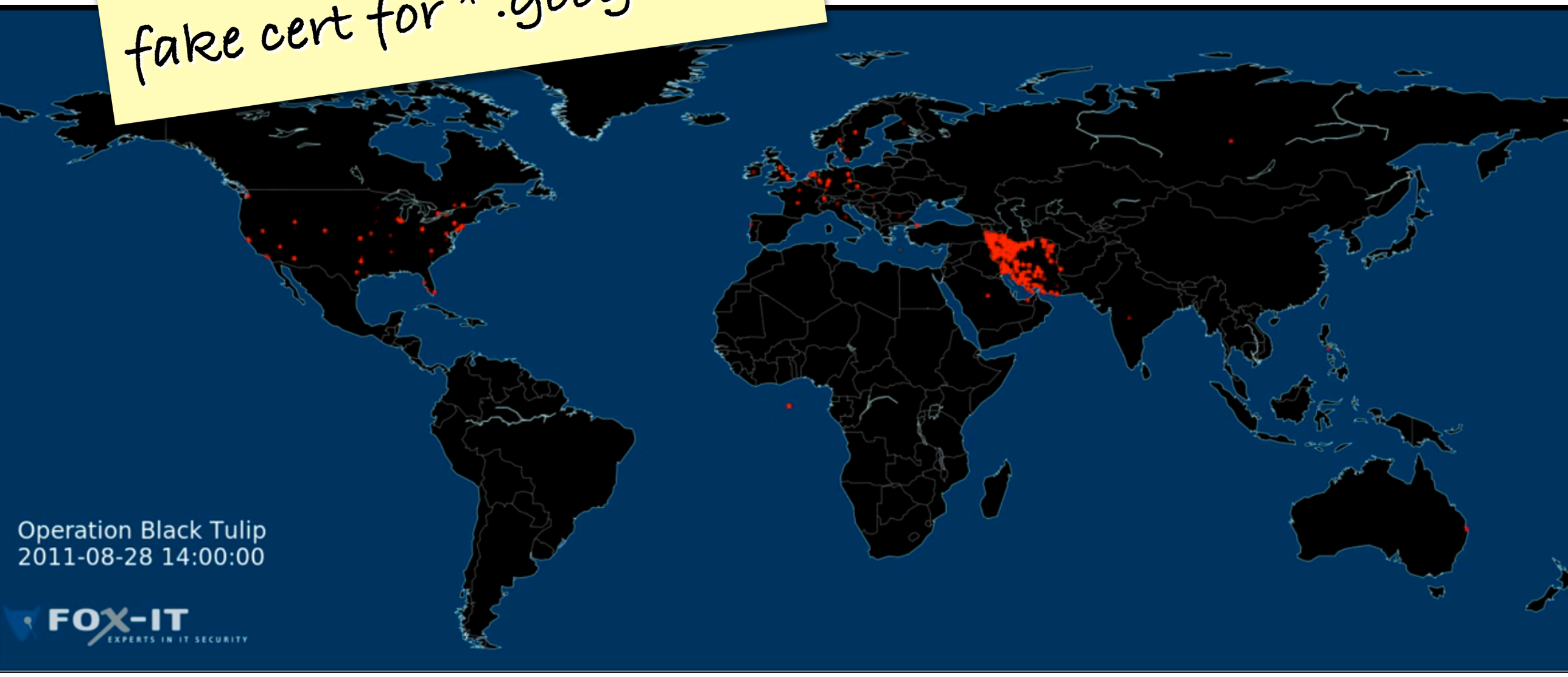
What kind of adversary has a-priori knowledge that it can effectively be a man in the middle?

Assuming hackers act rational economically

3. The attacker can divert the user's traffic (Man in the Middle

Is the hack worth the investment?

Geo-Locating the source of OCSP queries for the fake cert for *.google.com



http://www.youtube.com/watch?v=wZsWoSxxwVY&hd=1

This particular attack...

Was a determined adversary

with direct access to Nationwide Infrastructure

The attack vector would work at any scale, large or small as long as you can position the attack on path

As a result

Iranian users had some of their communications, including username/ passwords tapped by an eavesdropper

The Diginotar CA got pulled from browsers

(Inconvenient, and not everyone updates their browsers)

Diginotar was the Dutch Authorities' CA provider

Backend Processing

Tax

Various Gov Sites

Why could it happen?

The TLS session cannot say WHICH CA is to be used to validate the digital signature

Your browser will allow ANY CA to be used to validate a digital si

Rogue CAs imperil the ENTIRE DNS!

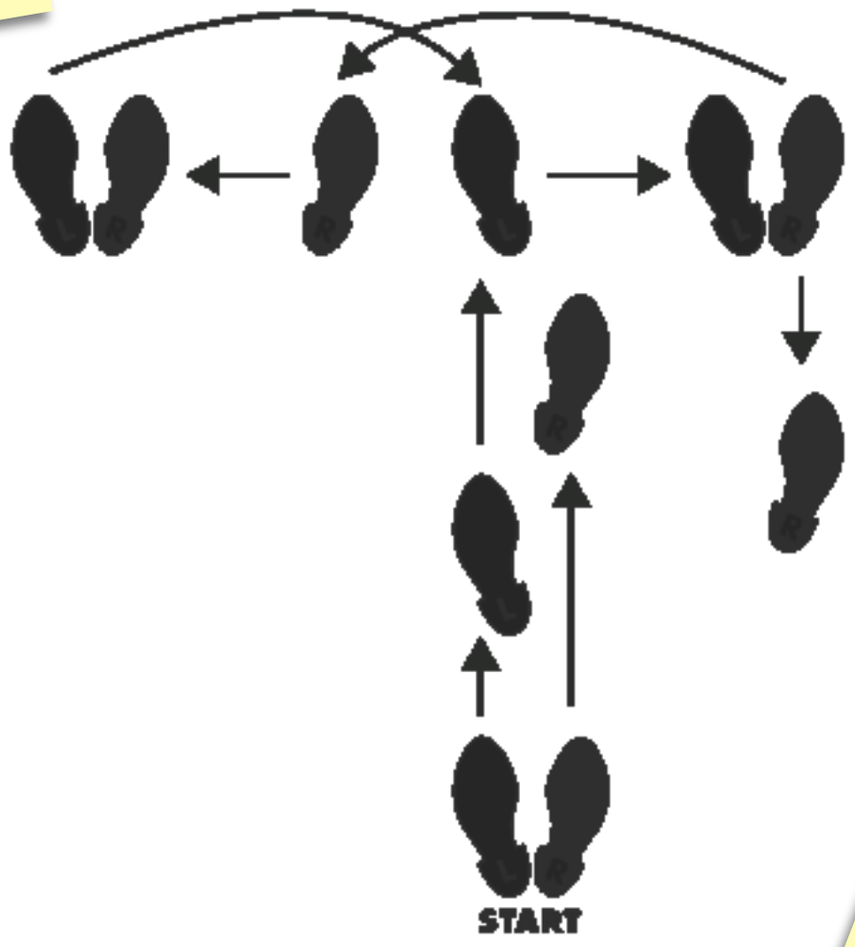
Domain Name Certificates are structurally weak:

Its hard to differentiate services within the domain name

The entire domain name certification setup is only as good as the weakest CA!

y compromised CA can issue rogue certificates for ANY domain name

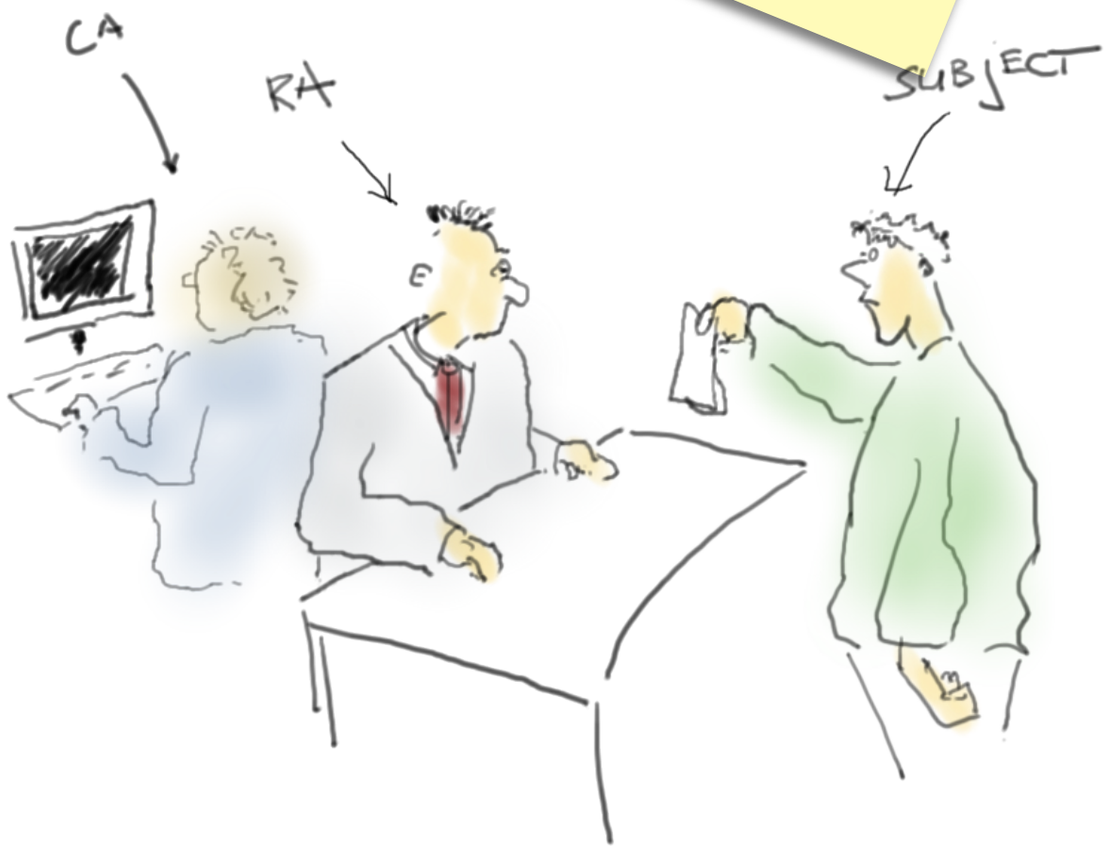
Lets take a step back



and talk about PKI

The role of a CA:

3rd party trust broker

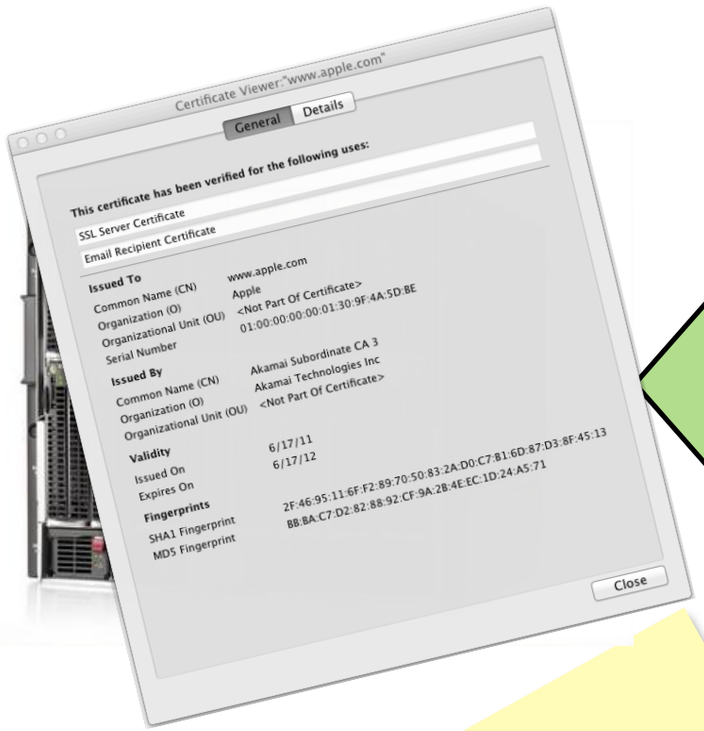


Subject Requests

RA performs checks

RA tells CA to sign

Browser trusts CA signed certificates



Browser trusts
~60 CAs

And therefore
~1500 Subordinate CAs
(~651 organizations)

See the EFF SSL observatory
http://www.eff.org/files/
DefconSSLiverse.pdf

In a commercial world...

what succeeds in the market?

Some CAs don't apply rigorous identity checks to issued domain name validation certificates

An important motivation for using digital c trust to online transactions by requiring website operator undergo vetting with a certificate authority (CA) in order to get an SSL certificate. However, commercial pressures have led some CAs to introduce "domain validation only" SSL certificates for which minimal verification is performed of the details in the certificate.

Most browsers' user interfaces did not clearly differentiate between low-validation certificates and those that have undergone more rigorous vetting. Since any successful SSL connection causes the padlock icon to appear, users are not likely to be aware of whether the website owner has been validated or not. As a result, fraudsters (including phishing websites) have started to use SSL to add perceived credibility to their websites.

By establishing stricter issuing criteria and requiring consistent application of those criteria by all participating CAs, EV SSL certificates are intended to restore confidence among users that a website operator is a legally established business or organization with a verifiable identity.

http://en.wikipedia.org/wiki/Extended_Validation_Certificate

All these CA worker bees and all these manual checks are a tad expensive

And the certificate market is undifferentiated

Reduce CA costs through automation of the process

DV
Domain Validation

Subject: Please sign certificate for "example.com"

RA sends a mail to well known address @example.com

When mail returned CA will sign

DV
Domain Validation

Subject: Please sign certificate for Exam

mail to address ple.com

All these checks are based on information fetched from the DNS

When mail returned CA will sign

Hold that thought!

An important motivation f digital certificates with SSL was to add trust to online transactions by re perators to undergo vetting with a certificate authority (CA) in o te. However, commercial pressures have led some CAs to intro SSL certificates for which minimal verification is perform ate.

Not everyone is honest!

Most brov did not clearly differentiate between low-validation certificates that have undergone more rigorous vetting. Since any successful SSL connection causes the padlock icon to appear, users are not likely to be aware of whether the website owner has been validated or not. As a result, fraudsters (including phishing websites) have started to use SSL to add perceived credibility to their websites.

By establishing stricter issuing criteria and requiring consistent application of those criteria by all participating CAs, EV SSL certificates are intended to restore confidence among users that a website operator is a legally established business or organization with a verifiable identity.

http://en.wikipedia.org/wiki/Extended_Validation_Certificate

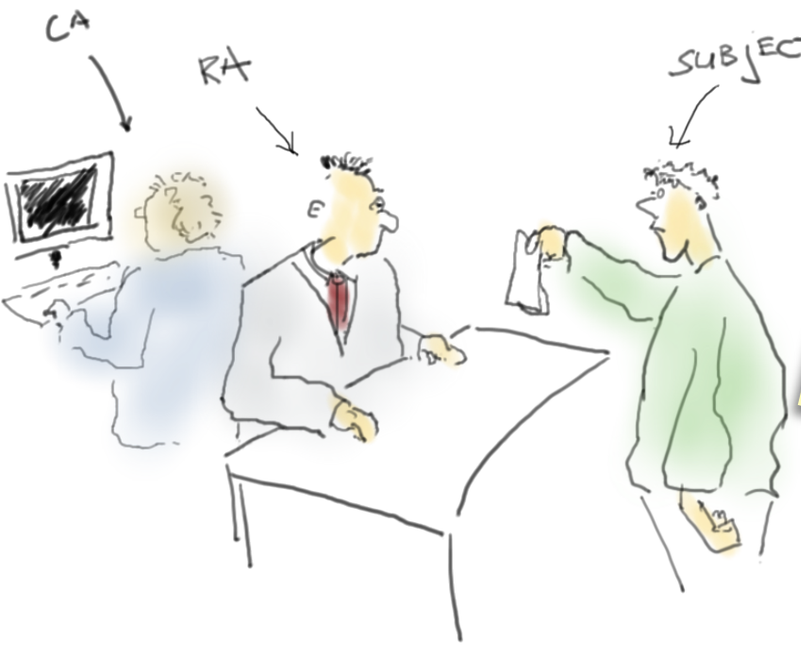
EV Extended Validation

Subject Requests

RA performs checks

- Who are you?
- Do you own the domain name?
- What web site are you using?
- Who is operating the web site?
- Are you authorized to act on behalf of the domain name holder?

http://www.cabforum.org/Guidelines_v1_3.pdf

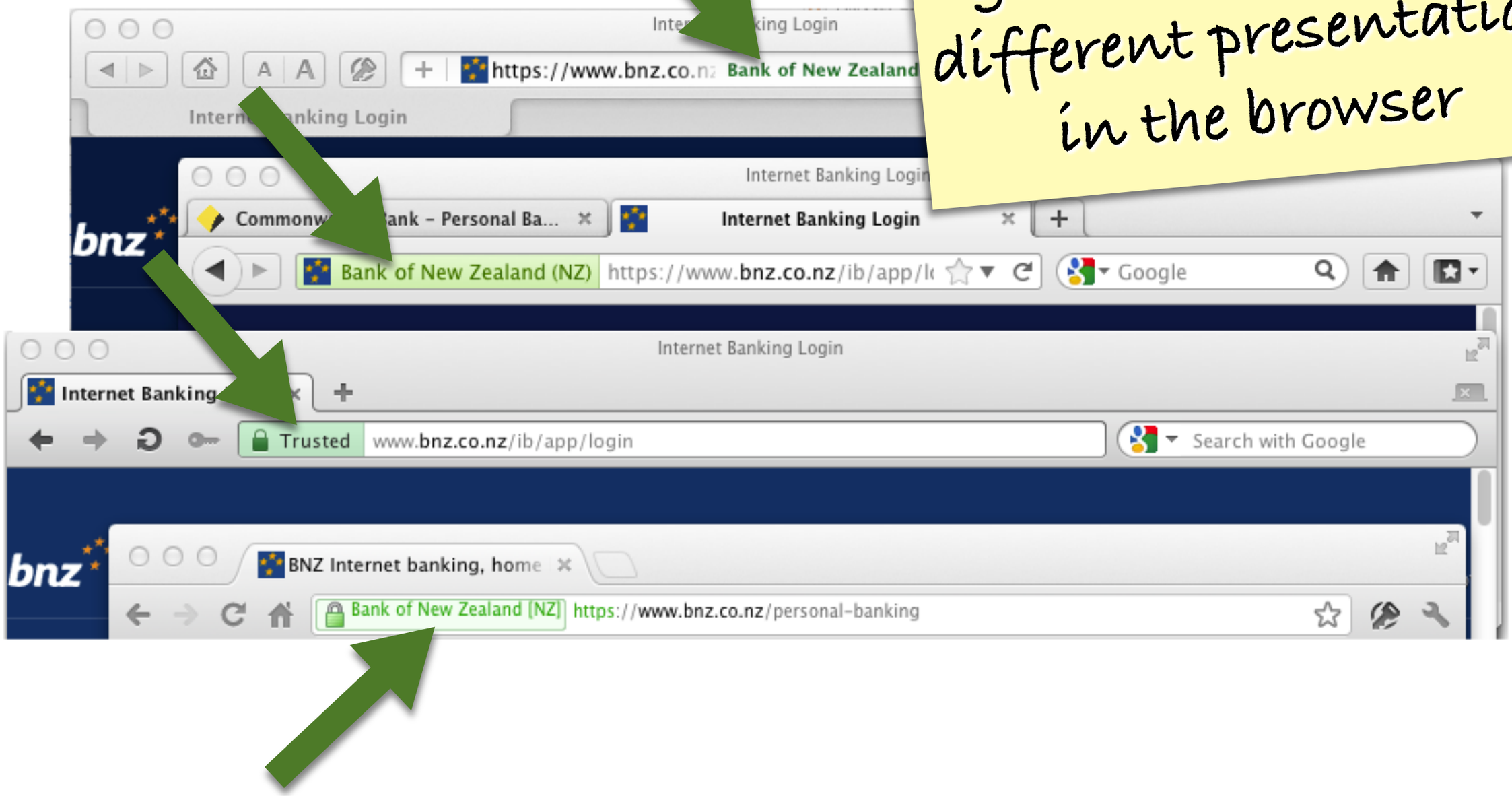


RA tells CA to sign

Browser recognises CA signed EV certificates

Certificate with EV policy Identifier

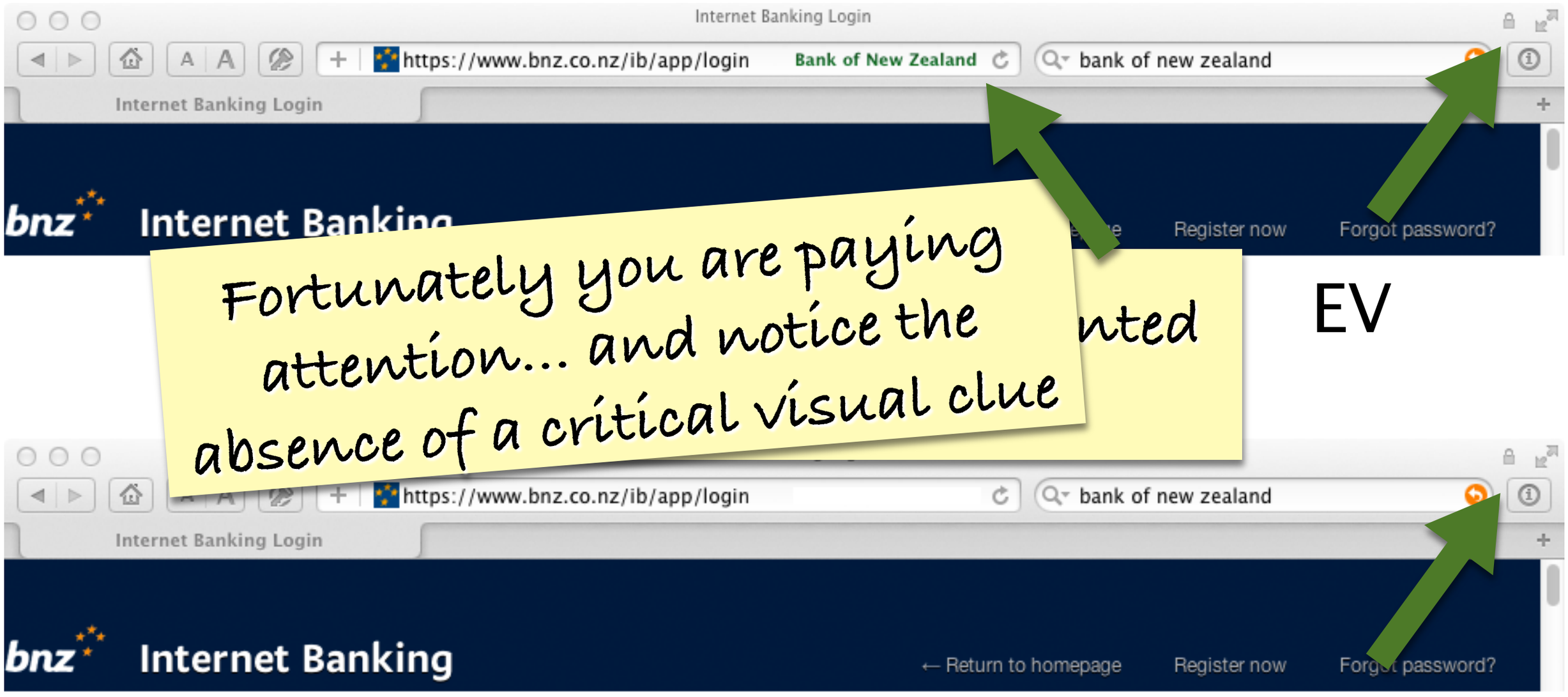
EV certificates generate a slightly different presentation in the browser



Why should I care about DV or EV anyway?

Now and then its possible that one of those CA organizations will make a mistake or be compromised

And then there are two signed certificates for a domain name, and only one is the "good" EV one.... while the other one might be a DV cert from a duped CA

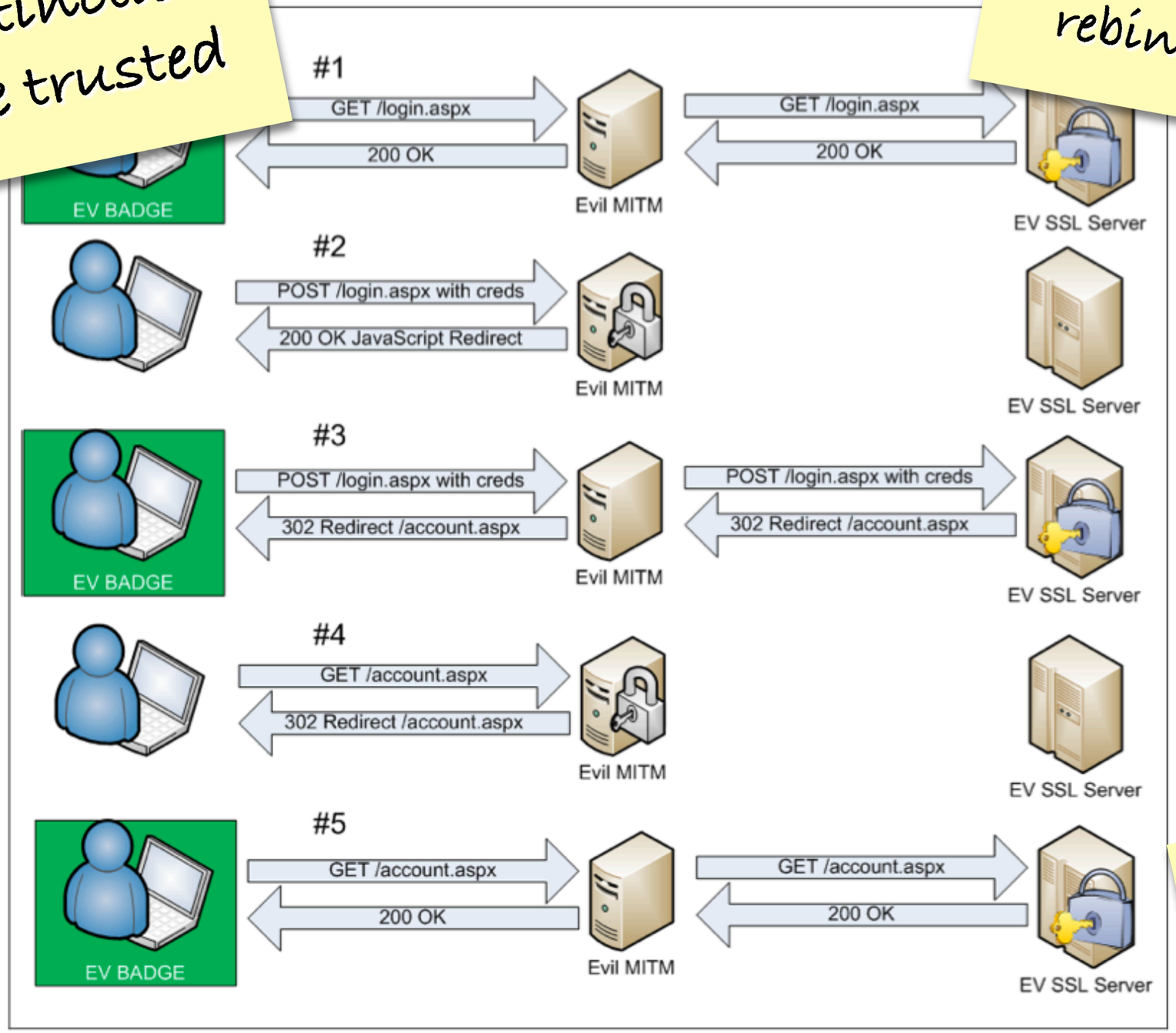

Internet Banking Login
https://www.bnz.co.nz/ib/app/login
Bank of New Zealand
bank of new zealand
Internet Banking Login
bnz
Internet Banking
Register now
Forgot password?
Fortunately you are paying attention... and notice the absence of a critical visual clue
https://www.bnz.co.nz/ib/app/login
bank of new zealand
Internet Banking Login
bnz
Internet Banking
← Return to homepage
Register now
Forgot password?

EV

DV

BUT: In Practice the DV-EV distinction can not be trusted

Zusman and Sotirov demonstrated rebinding attacks



UI armsrace

Figure: The request and response flow of an SSL Rebinding attack

Zusman & Sotirov 2009: http://www.blackhat.com/presentations/bh-usa-09/SOTIROV/BHUSA09-Sotirov-AttackExtSSL-PAPER.pdf


isdooo

Rogue Certificate Counter Measu

Blacklisting

CRL

OCSP

Doesn't scale well
Only available when compromise is known to have happened
Relies on OCSP use!

Whitelisting

next page

Extended Validity

DV-EV distinction cannot be made reliably without external knowledge

What if you know before starting the TLS/SSL session that a certain certificate is to be expected?

Whitelisting

HTSP

Leap of Faith

Or use an alternative infrastructure

Domain Name System

Independent Hierarchical Registration

One root

Scalable and Global

Namespace maps 1:1 to PKI Use

DANE

Using Secure DNS to Associate Certificates with Domain Names for TLS

http://tools.ietf.org/wg/dane

draft-ietf-dane-protocol

TLSA RR

2.3. TLSA RR Examples

An example of a hashed (SHA-256) association of a PKIX CA certificate:

```
_443._tcp.www.example.com. 1
    0 0 1 d2abde240d7cd3ee6b4
          7983a1d16e8a410e456
```

CA Cert

An example of a hashed (SHA-512) subject public key association of a PKIX end entity certificate:

```
_443._tcp.www.example.c
    1 1 2 92003ba34942dc
          a5a520e7f2e06b
          1b177615d466f6
          8c9ebdd2f74e38fe51ffd48c43326cbc
```

EE Cert

An example of a full certificate association of a PKIX trust anchor:

```
_443._tcp.www.example.com
    2 0 0 30820307308201e
```

Trust Anchor

Valid CERTs and/or CAs are stored in the the DNS: allow **only** those CAs to validate presented certs for your SSL connection

Prevents a rogue DigiNotar CA vouching for Google's gmail

If DANE provides the CA's identity, then DANE offers the protection that you are looking at a valid EV certificate issued by the CA that performed the EV validation checks in the first place

CA compromise then has limited liability to those certificates issued by the compromised CA

How about DV certificates: are they useless?

CAs checking the DNS are not needed

Not with DANE

The CERT can be stored in the DNS at once

DV becomes a commodity

Encryption is free

How does DNSSEC get into the picture?

DANE Specification REQUIRES it

Even Before DANE gets deployed DNSSEC is useful

Obtaining Rogue (DV) Certificates

Use of Rogue Certificates

Obtaining Rogue (DV) Certificates

Hacking the provisioning path

Impersonation during the request (Men in the Middle)

Diginotar CA compromise

Comodo reseller impersonation

For DV certificates you have to impersonate the Domain

For EV, much more fraud (Social Engineering)

Did you keep this thought?

DV
Domain Validation

Obtaining Rogue (DV) Certificates

All these checks are based on information fetched from the DNS

Own the DNS and the DV is yours

DANE has the potential to solve important PKI/TLS problems

Not a magic bullet

And for DANE to work then DNSSEC is necessary

DNSSEC Potential Problems

Why now?

UDP fragmentation

TCP proble

Software support

Tools availability

Increase Costs

Under Provisioned Infrast

Trained staff

Unaware Firewalls

Home gateways

Challenges

DNSSEC last mile

Libraries and APIs

Tunnel Hacks

DNSSEC for SUS Admins

BIND9.8

OpenDNSSEC

Tools, Trainers, and Consultants are available

Registrar support

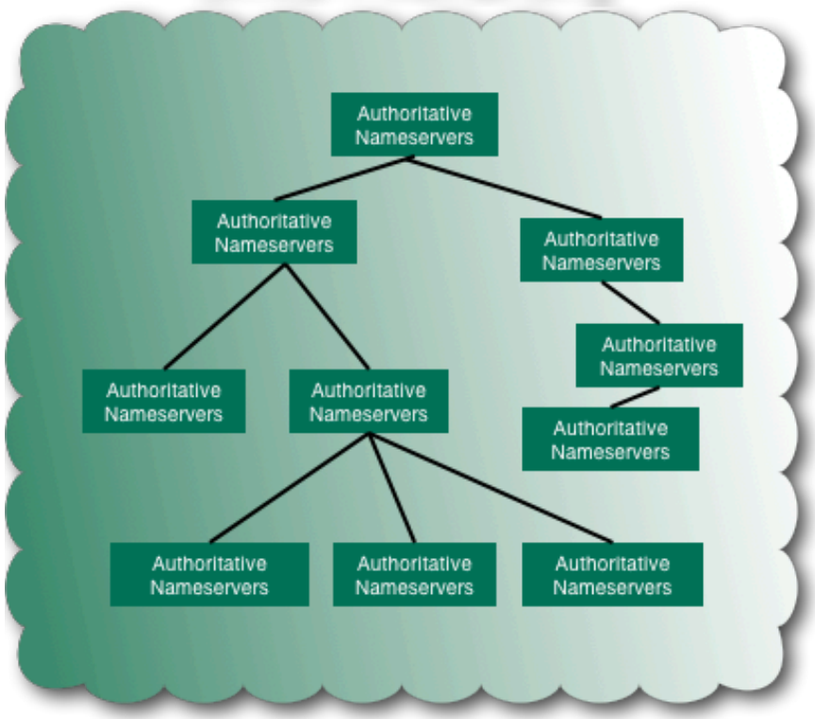
Why invest in DNSSEC?

In signing when there is no validation

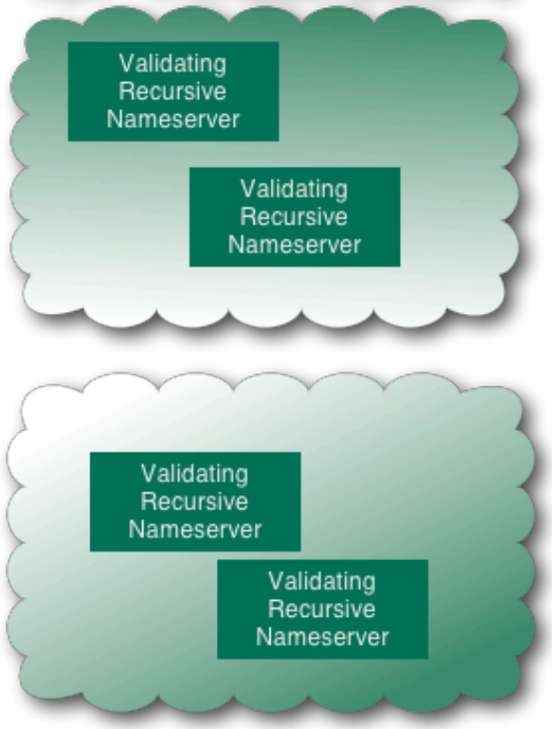
In validation when nothing is signed?

In development if there is no infrastructure?

DNS Hierarchy



ISP infrastructure



OS and Application Support

Why invest in DNSSEC?

Because the DNS represents a major point of vulnerability in today's networks

Cyber attacks are no longer just a teenage hobby or even petty crime

Attacks on the DNS are highly effective for all kinds of reasons!

You MUST play a role

It's not about short term economics
It's about long term maintenance of
the Public Good

Thats it!