DNSSEC Musings

Diginotar, DANE, and Deployment

Olaf M. Kolkman

Acknowledgements:
Jakob Schlyter
Geoff Huston
Dan Kaminsky

NLnet Labs

http://www.nlnetlabs.nl/

NLnet Labs

101

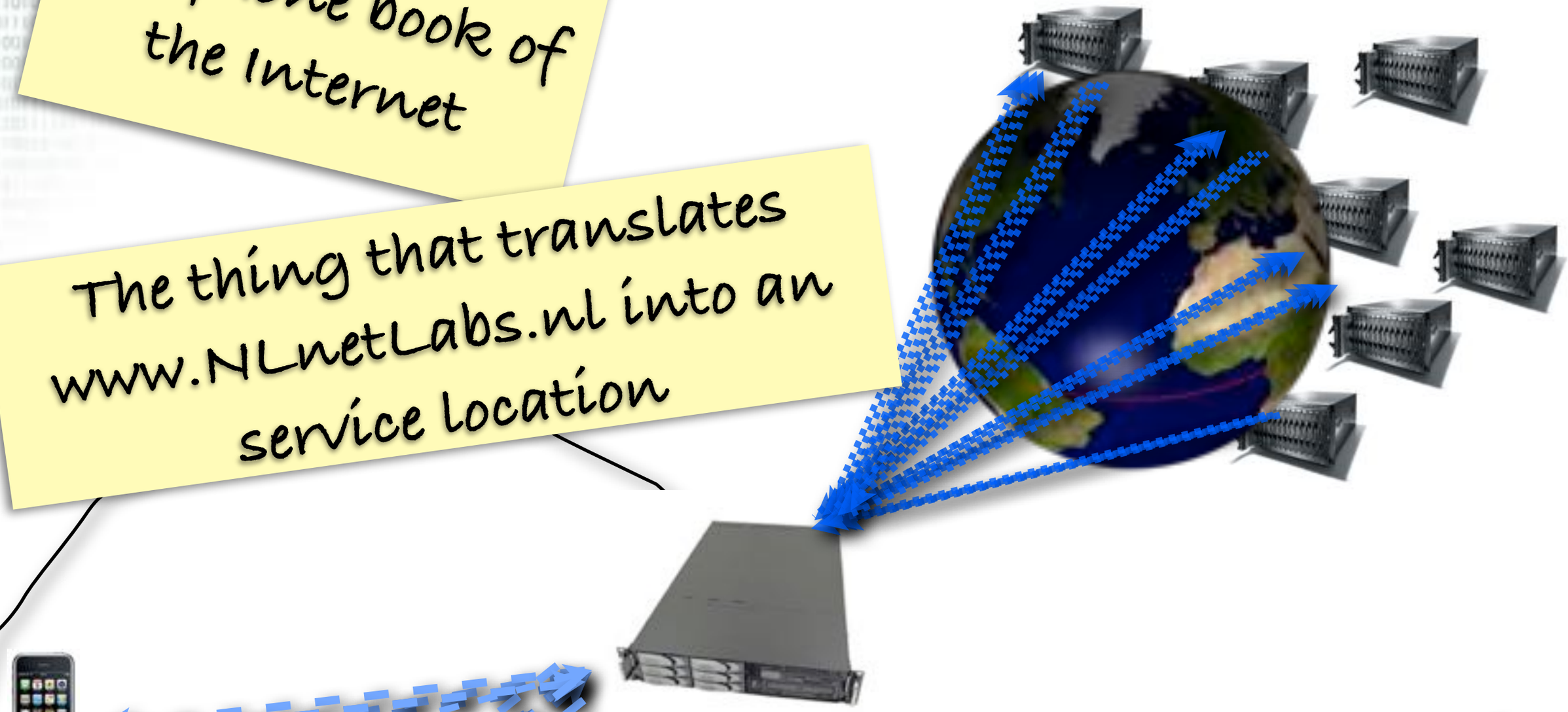
NLnet Labs

DNS

NLnet Labs

Telephone book of the Internet

The thing that translates www.NLnetLabs.nl into an service location



Highly resilient, global, scalable.

NLnet Labs

DNS Provisioning

DNS Protocol

Registrars & Registrants

Server vulnarability

Secondary DNS

Man in the Middle

primary DNS

Registry

spoofing & Man in the Middle

http://www.nlnetlabs.nl/

NLnet Labs

DNSSEC

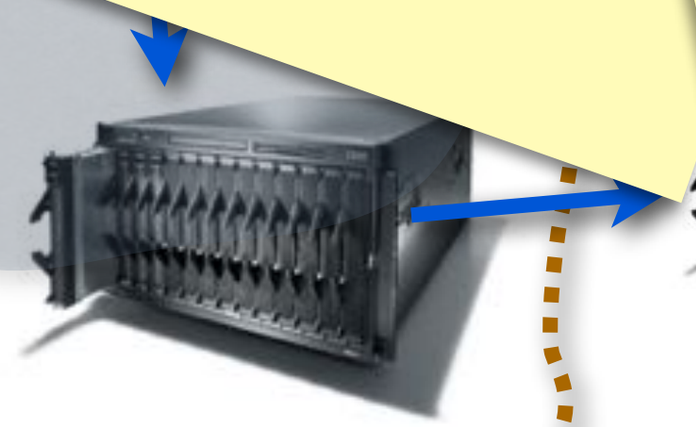
NLnet Labs

DNS Protocol

Cryptographic means to secure the DNS

rver vulnarability

Ads Integrity and authenticity validation to the DNS protocol



Registry

ing
&
Man in the Middle

NLnet Labs

Internet

PKI

NLnet Labs

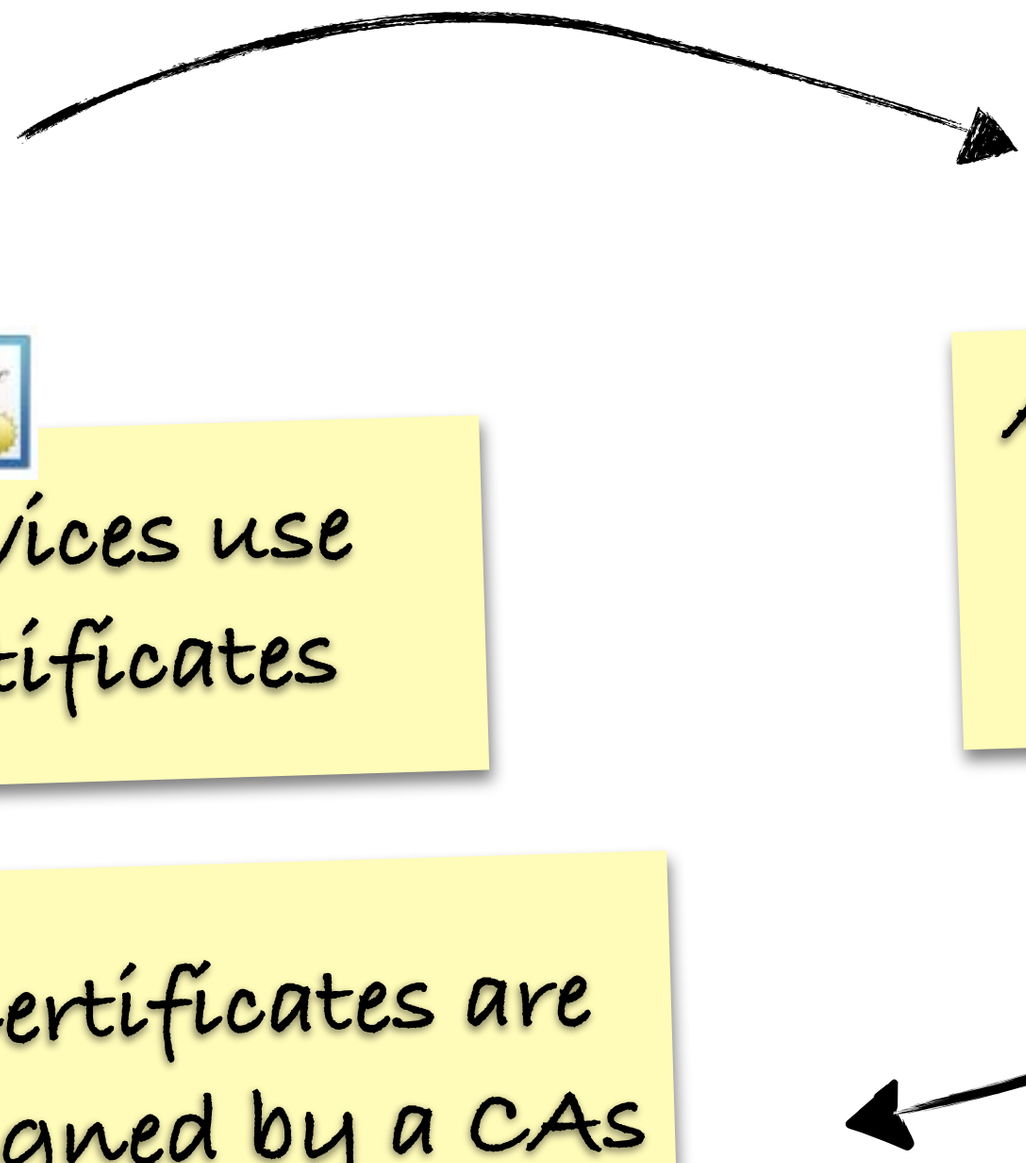
In this context technology to assert authenticity.

Provides a basis for integrity and confidentiality of connections

Depends on trust in specific 3rd parties: Registration and Certificate Authorities

NLnet Labs

TRANSITIVE TRUST



Services use certificates

Applications are configured to trust CAs

Certificates are signed by a CAs

NLnet Labs

Hi and his magic Brouser

how failure in technology and compliance almost brought misery and doom

NLnet Labs

September 2012

DigiNotar®
A VASCO COMPANY

http://www.nlnetlabs.nl/

NLnet Labs

A Bankrupt Certificate Authority

Home Diginotar internet trust services, certificaten, elektronische handtekening

http://www.diginotar.nl/

Home Diginotar internet trust ser...

DigiNotar®
A VASCO COMPANY

HOME | ACTUEEL | PRODUCTEN | 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 Pols
- 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...


Iranian activists feel the chill as hacker taps into e-mails
BY SOMINI SENGUPTA
He claims to be 21 years old, a stu
software engineering in Tehran
reveres Ayatollah Ali Khamenei and
despises dissidents in his country.
He sneaked into the computer sys-
tems of a security firm on the outskirts
of Amsterdam. He created fake creden-
tials 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
chanism that is trus-
sers all over the world.
, as he calls himself, in-
ed on his own and is un-
he notion that his work
een used to spy on anti-
might have
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
Société Générale
Crédit Agricole, are consi
actors in the French economy,
t U.S.
not to
ppens,
ere with
October
you, and I
ne children
ou."
w conducted
nly three that
Mr. Kennedy's
g published as a
e Kennedy: His-
Life With John F.
io recording. In it,
Arthur M.
ide to

Front-Page News

International Herald Tribune
Sep 13, 2011 Front Page

NLnet Labs

Events

Chain of ~~trust~~

NLnet Labs

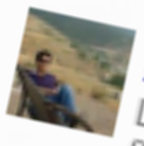
Something fishy

28 Aug 2011

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

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://productforums.google.com/forum/#!category-topic/gmail/share-and-discuss-with-others/3J3r2JqFNTw

link last verified 5 oct 2012 (avatar had changed from the snapshot above)

NLnet Labs

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

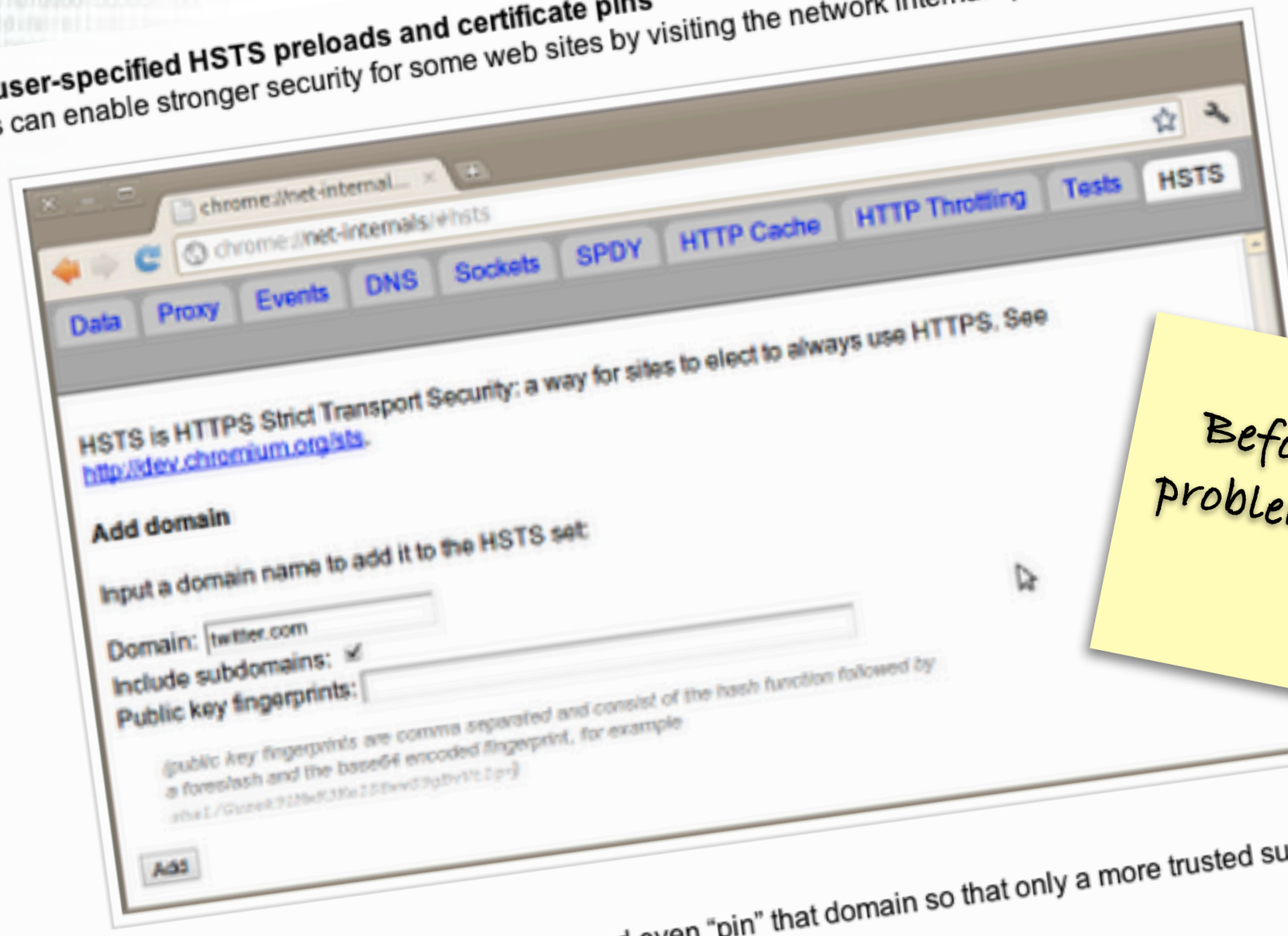
4:06 PM
8/27/2011

Google Chrome magic caught this!

NLnet Labs

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



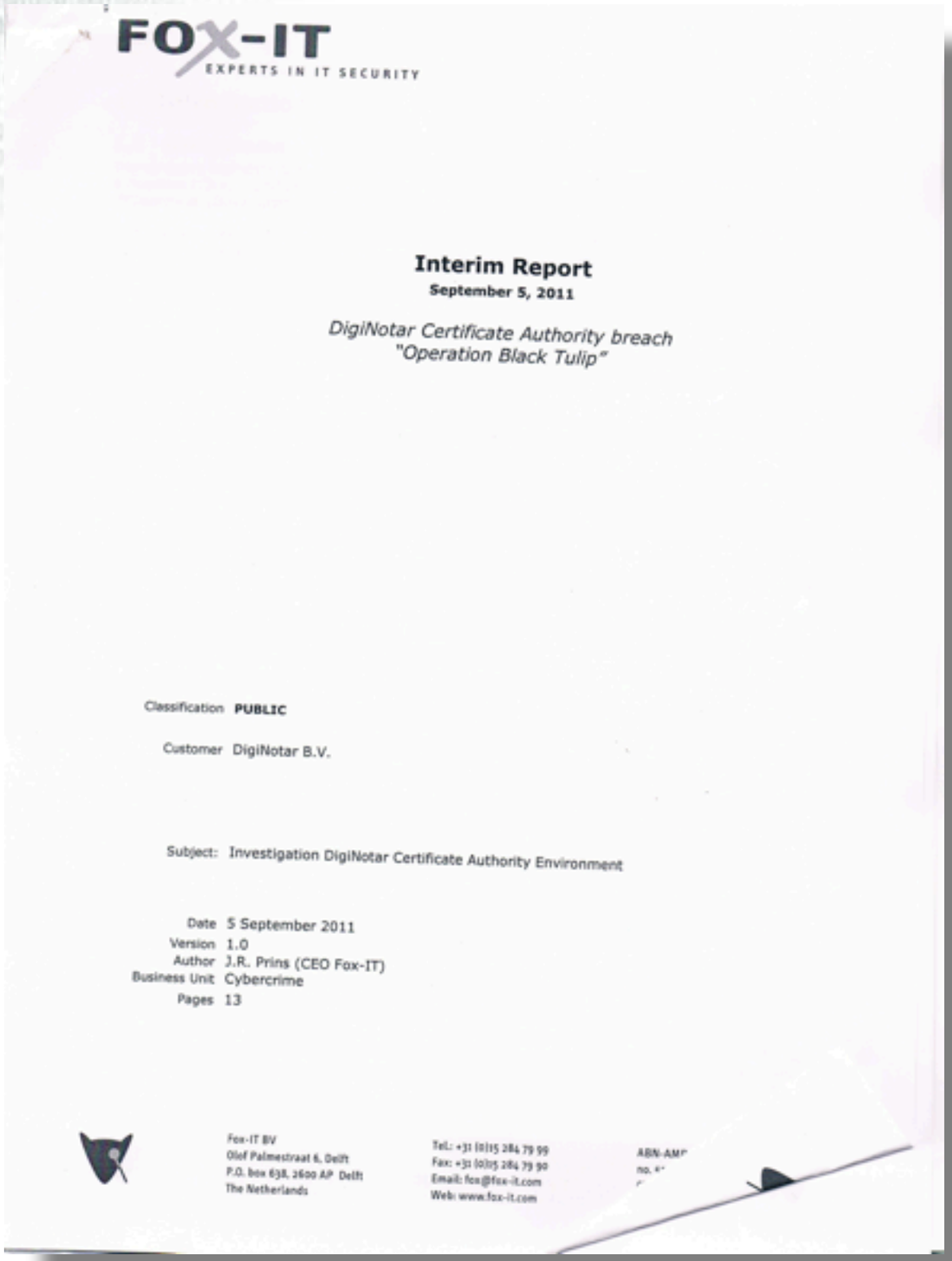
Before June 2011 the problem would not have shown

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

NLnet Labs



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-AMRO
no. 4[illegible]

What went wrong?

http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html
link verified oct 5, 2012

NLnet Labs

Compromised certificate issued by: DigiNotar

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 hacker

NLnet Labs

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: Pr0d@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) you can't even dump hashes of domain if you don't have admin privilege to crack them
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 Adversary Chuck When

1. When Victim Bob wants to get to a destination for which Charlie has a certificate

2. The compromised CERT is not in a blacklist, or not checked otherwise (by Bob)

3. Chuck can divert the Bob's traffic to her service (Man in the Middle)

NLnet Labs

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

3. Chuck can divert the Bob's traffic to Alice's service (Man in the Middle)

Assuming hackers act rational economically

Is the hack worth the investment?

NLnet Labs

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

NLnet Labs

My takeaway

This was a determined adversary

With direct access to Nationwide Infrastructure

NLnet Labs

As a result

Iranian activists saw their communication tapped

(Life Threatening ?)

The Diginotar CA got pulled from the browser

(Inconvenient)

Diginotar was the Dutch Authorities' CA provider

Backend Processing

Tax

Various Gov Sites

NLnet Labs

TAKEAWAY

Compliance failure

Technology weakness

Technology Defenses

NLnet Labs

The Browser and its Trust

NLnet Labs

Who to trust?

Ah, oh.... those smart girls and boys from ... eh..

eh microfox?
must have figured that out...

NLnet Labs

This grandma was borrowed from http://farm3.staticflickr.com/2145/1713612630_2ddcec1d2a_z.jpg

Browser trusts ~60 CAs

And therefore ~1500 Subordinate CAs (~651 organizations)

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

NLnet Labs

The role of a CA

3rd party trust broker

Subject Requests

RA performs checks

RA tells CA to sign

Browser trusts CA signed certificates

NLnet Labs

However all these little men are a wee bit expensive

And do we need them for compliance?

AUTOMATE THE LOT

http://www.nlnetlabs.nl/

NLnet Labs

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

NLnet Labs

DV
Domain Validation

All these checks are based on information fetched from the DNS

Hold that thought

NLnet Labs

Domain validity

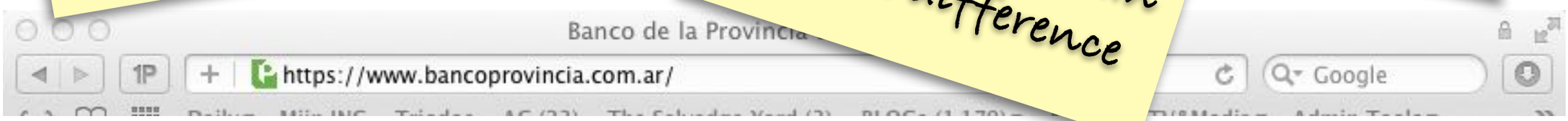
Extended validity

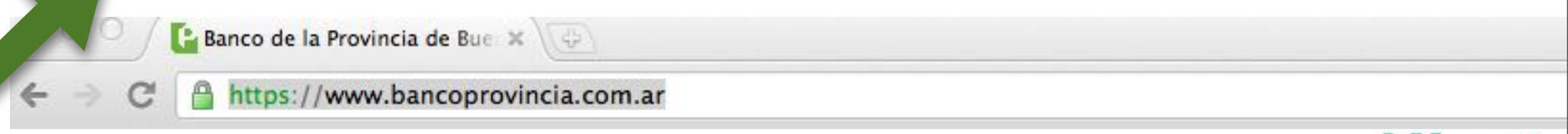
http://www.nlnetlabs.nl/

NLnet Labs

Fortunately

The trained eye can spot the difference





NLnet Labs

In Practice the DV-EV distinction can not be trusted

Zusman and Sotirov demonstrated rebinding attacks

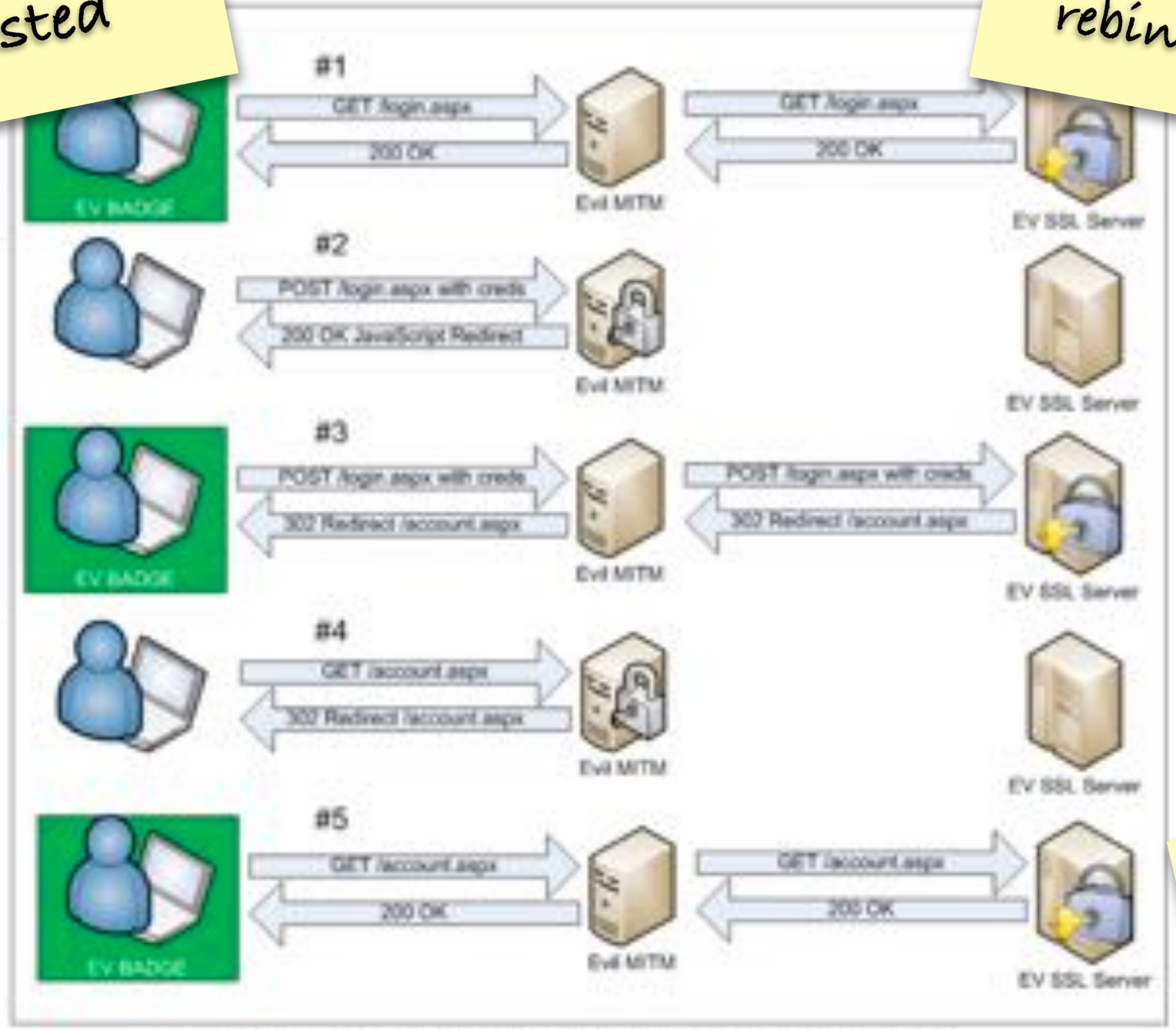


Figure: The request and response flow of an SSL Rebinding attack

U armsrace

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

NLnet Labs

So now and then one of those organizations will make a mistake or be compromised

NLnet Labs

And then there are the economics

NLnet Labs

So suddenly you are confronted with this situation

Bonafide certificate signed by verisign

Adversary certificate signed by another CA

http://www.nlnetlabs.nl/

NLnet Labs

picture from http://e-devotion.blogspot.nl/2012/03/light-at-end-of-tunnel.html

Counter Measures

Blacklisting

Whitelisting

NLnet Labs

Counter Measures

Blacklisting

CRL

OCSP

Doesn't scale well

Only reliable when compromise is known to have happened

NLnet Labs

Counter Measures

Whitelisting

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

HTSP

Leap of Faith

And/Or use an alternative infrastructure

Domain Name System

Independent Hierarchical Registration

One root

Scalable and Global

Namespace maps 1:1 to PKI

Use

Fate sharing

NLnet Labs

DANE

Using Secure DNS to Associate Certificates with Domain Names for TLS

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

RFC 6698

NLnet Labs

Use the independent DNS infrastructure to vouch for the CA

NLnet Labs

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. IN TLSA (
    0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
          7983a1d16e8a410e4561cb106618e971 )
```

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

```
_443._tcp.www.example.com. IN TLSA
    1 1 2 92003ba34942dc74152e2f2c408d29ec
          a5a520e7f2e06bb944f4dca346baf63c
          1b177615d466f6c4b71c216a50292bd5
          8c9ebdd2f74e38fe51ffd48c43326cbc )
```

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

```
_443._tcp.www.example.com. IN TLSA
    2 0 0 30820307308201efa003020102020... )
```


NLnet Labs

Valid CERTs and/or CAs are stored in the the DNS: allow only those for your connection

Prevents DigiNotar CA vouching for google because google can signal they use Thawte

NLnet Labs

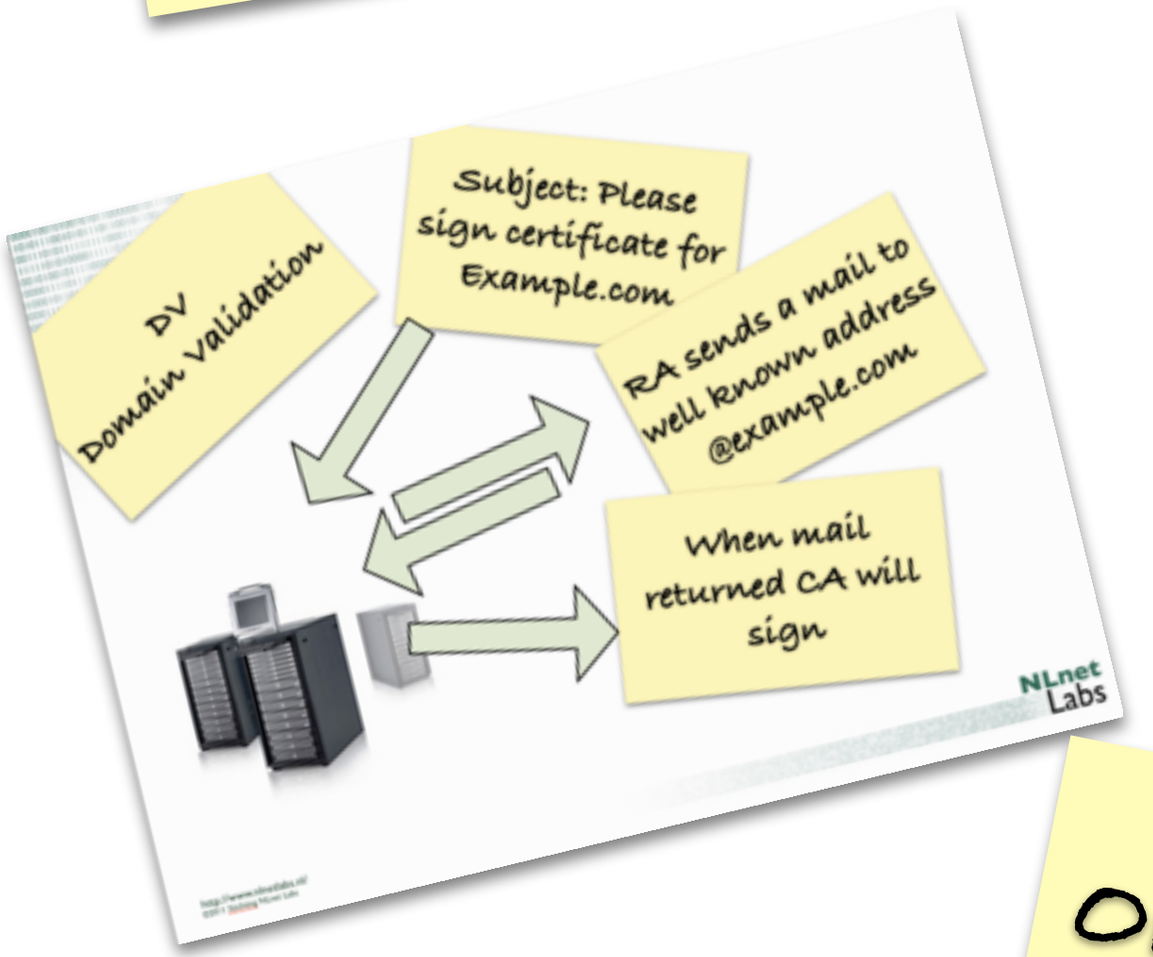
DANE offers the protection that you are looking at a valid EV Certificate

The EV certificate offers you the legal paper trail that you are doing business with a real company

NLnet Labs

How about DV certificates, are they useless?

CAs checking the DNS are not needed



The CERT can be stored in the DNS at once

One of DANE's usecases

NLnet Labs

How does DNSSEC get into the picture

NLnet Labs

DANE depends on the authenticity and integrity

NLnet Labs

But having DNSSEC is useful anyhow

PREVENTS A CLASS OF MAN IN THE MIDDLE ATTACKS THAT MAKE CERTIFICATE EXPLOITS POSSIBLE

And it offers a building for further security innovation

NLnet Labs

DNSSEC in the Wild?

NLnet Labs

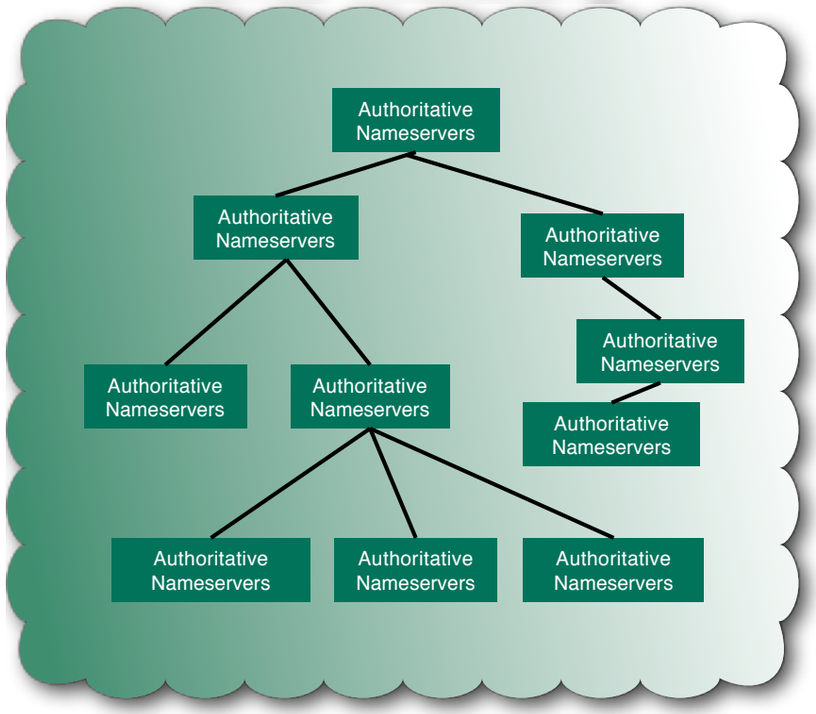
Why invest?

In signing when there is no validation

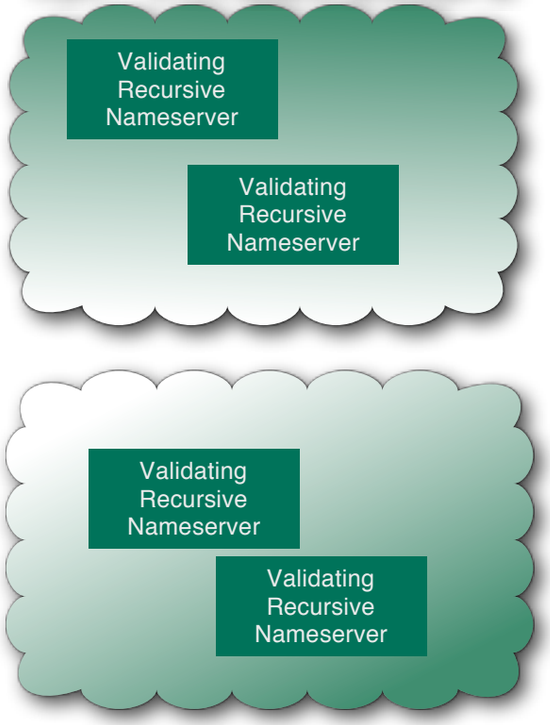
In validation when nothing is signed?

In development if there is no infrastructure?

DNS Hierarchy



ISP infrastructure



OS and Application Support

NLnet Labs

Potential Problems ?!

y invest?

validation

UDP Fragmentation

Tools Availability

Software support

TCP proble

DNS Hierarchy

Increase Costs

Under Provisioned Infrastructy

Trained Staff

Unaware Firewalls

Home gateways

NLnet Labs

Potential Problems ?!

Operational and Technical First Mover Disadvantage

VS

Reputation

Innovation

Responsibility

NLnet Labs

Is global security architecture on your radar?

NLnet Labs

Hold it

you only talked DNSSEC technology

NLnet Labs

DNS Provisioning

DNS Protocol

Registrars & Registrants

Server vulnarability

Secondary DNS

Man in the Middle

primary DNS

Registry

spoofing & Man in the Middle

NLnet Labs

Note though that w.r.t. provisioning DNS has similar weaknesses. Registries and Registrars sometimes make mistakes

NLnet Labs

NLnet Labs

DANE has the potential to solve important PKI/TLS problems

Not a magic bullet

Not the only approach

'convergence'

DNSSEC is needed infrastructure: securing and enabling at the same time

Not a magic bullet either

NLnet Labs

The Internet PKI has a trust issue.

A global trust issue

Scalability problems: compliance and technology

NLnet Labs

http://www.nlnetlabs.nl/

Internet Trust is Global Trust

Local action global effect

misaligned incentives ??

NLnet Labs

How to increase global trust in the Internet?

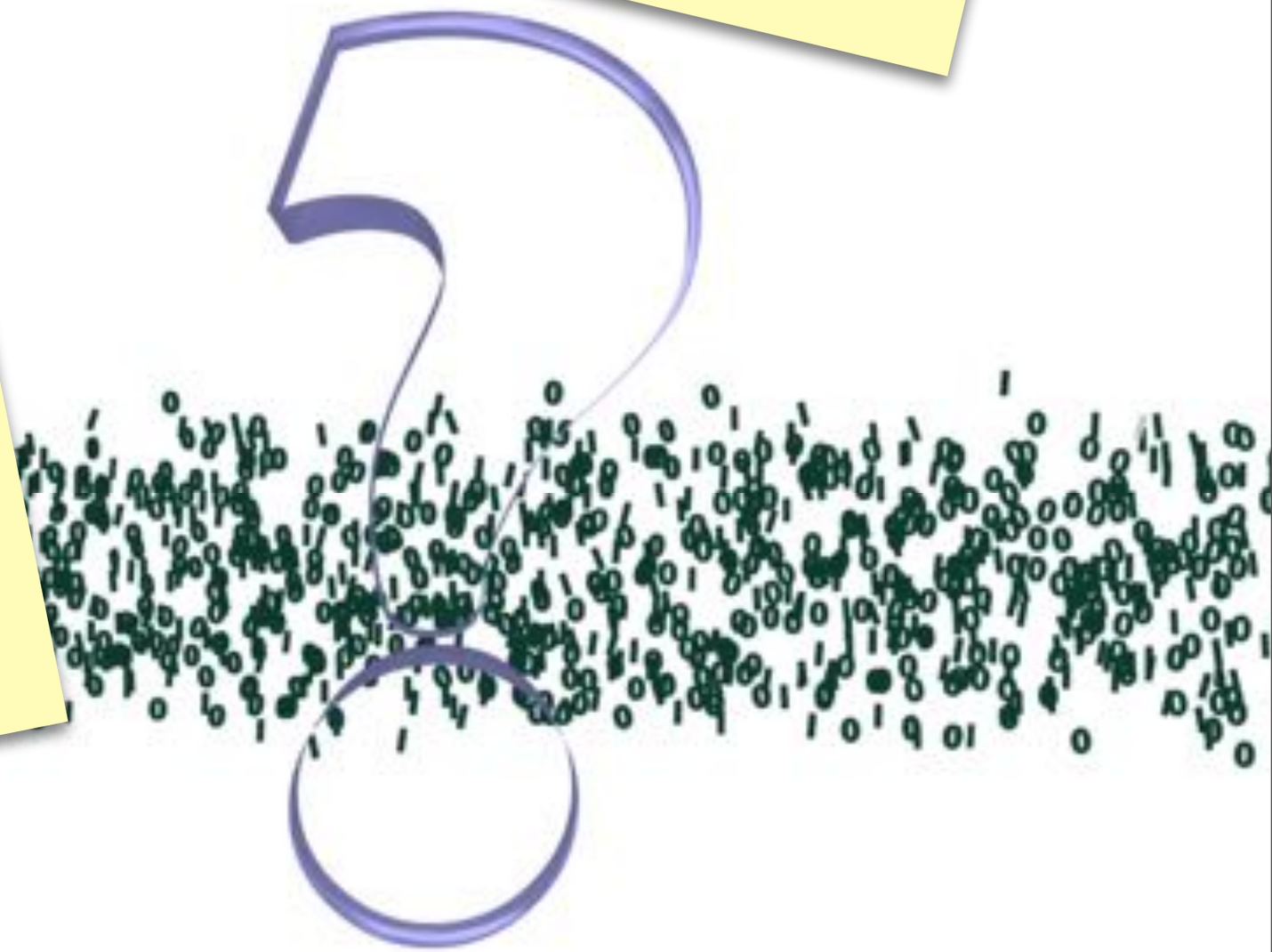
Without a race to the bottom of minimal compliance?

With meaningful incremental steps in improving technology?

NLnet Labs

That's it folk

Questions, comments, ideas:
olaf@nlnetlabs.nl



http://www.nlnetlabs.nl/