DNSSEC Musings

Diginetar, DANE, and Deployment

Olaf M. Kolkman

ACKnowledgements:
Jakob Schlyter
Geoff Huston
Dan Kaminsky
DNS
Telephone book of the Internet

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

Highly resilient, global, scalable.
DNS Provisioning

Registrars & Registrants

Registry

DNS Protocol

Server vulnerability

Man in the Middle

Primary DNS

Secondary DNS

spoofing & Man in the Middle
DNS Protocol

Cryptographic means to secure the DNS

Server vulnerability

Man in the Middle

Ads Integrity and authenticity validation to the DNS protocol

Registry
Internet PKI
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.
Transitive Trust

Applications are configured to trust CAs

Services use Certificates

Certificates are Signed by a CAs

Certificates are Signed by a CAs
Ali and his magic Browser

how failure in technology and compliance
almost brought misery and doom
A Bankrupt Certificate Authority
Iranian activists feel the chill

Front-Page News

In a move that is truly
mechanism that is true
erators all over the world,
ners he calls himself, Mr.
he not only his own and is ur
ed on his own and his work.

as hacker taps e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mails

Front-Page News

Iranian hackers tap e-mail
Events

Chain of trust
Hi,

Today, when I tried 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/?rkk1b17s1ctityb

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)
Invalid Server Certificate

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

Help me understand

When you connect to a secure website, the server hosting that site presents your browser with something called a certificate. This certificate contains identity information, such as the address of the website, which is verified by a third party. Checking that the address in the certificate matches the address of the website, it is possible to verify that the 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. This certificate is malformed, contains invalid fields, or is not supported.

Certificate status:
This certificate is OK.

Learn more about certification paths

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.

Interim Report
September 5, 2011

DigiNotar Certificate Authority breach
"Operation Black Tulip"

What went wrong?

link verified oct 5, 2012

http://www.nlnetlabs.nl/
©2011 Stichting 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

Fingerprint Similarity to Comodo Hacker

Advanced and Amateur

And a claim by the hacker

http://www.nlnetlabs.nl/
©2011 Stichting NLnet Labs

Wednesday, October 10, 12
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 sited 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:

But I remembered something and I hacked DigiNotar without more thinking in anniversary of that mistake:

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

Assuming hackers act rational economically, is the hack worth the investment?

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

This was a determined adversary

With direct access to Nationwide Infrastructure
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

Various Gov Sites

Backend Processing

Tax
Takeaway

Compliance failure

Technology weakness

Technology Defenses
The Browser and its Trust
Who to trust?

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

eh microfox? must have figured that out...

This grandma was borrowed from http://farm3.staticflickr.com/2145/1713612630_2ddcecid2a_z.jpg
Browser trusts ~60 CAs

And therefore ~1500 Subordinate CAs (~651 organizations)

See the EFF SSL observatory
http://www.eff.org/files/Defcon.SSLiverse.pdf
The role of a CA

3rd party trust broker

Subject Requests

RA performs checks

RA tells CA to sign

Browser trusts CA signed certificates
However all these little men are a wee bit expensive.

And do we need them for compliance?

AUTOMATE THE LOT
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

All these checks are based on information fetched from the DNS

Hold that thought
Fortunately, the trained eye can spot the difference.
In practice, the DV-EV distinction cannot be trusted.

Zusman and Sotirov demonstrated rebinding attacks.

So now and then one of those organizations will make a mistake or be compromised.
And then there are the economics
So suddenly you are confronted with this situation

Bonafide Certificate
Signed by verisign

Adversary certificate signed by another CA

http://www.nlnetlabs.nl/
©2011 Stichting NLnet Labs

Wednesday, October 10, 12
Technology + Compliance = Trust
Counter Measures

Blacklisting

Whitelisting
Counter Measures

Blacklisting

CRL

OCSP

Doesn't scale well

Only reliable when compromise is known to have happened
Counter Measures

Whitelisting

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

And/Or use an alternative infrastructure

HTSP

Leap of Faith
Domain Name System

Independent Hierarchical Registration

One root

Scalable and Global

Namespace maps 1:1 to PKI Use

Fate sharing

Wednesday, October 10, 12
DANE

Using Secure DNS to Associate Certificates with Domain Names for TLS

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

RFC 6698
Use the independent DNS infrastructure to vouch for the CA
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
  a5a520e7f2e06bb944f4dca346bafe63c
  1b177615d466f6c4b71c216a50292bd5
  8c9ebdd2f74e38fe51ffdf48c43326cbe )
```

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

```
_443._tcp.www.example.com. IN TLSA
  2 0 0 30820307308201efa003020102020...
```
Valid CERTs and/or CAs are stored in the DNS: allow only those for your connection

Prevents DigiNotar CA vouching for google because google can signal they use Thawte
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.
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
How does DNSSEC get into the picture
DANE depends on the authenticity and integrity
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
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
Potential problems?!

Why invest?

Increased Costs

TCP problems when nothing is signed?

TCP problems when there is no validation

In development if there is no infrastructure?

In signing when there is no validation

Potential Problems?!

Home gateways

Unaware firewalls

UDP fragmentation

Under provisioned infrastructure

Trained staff

Software support

Tools

Availability

Fragmentation management

UDP

Increased costs

Authoritative nameservers

Authoritative nameservers

Authoritative nameservers

Authoritative nameservers

Authoritative nameservers

Authoritative nameservers

Authoritative nameservers

Authoritative nameservers
Is global security architecture on your radar?
Hold it

you only talked DNSSEC technology
DNS Provisioning

Registrars & Registrants

Registry

Primary DNS

Secondary DNS

Server vulnerability

Man in the Middle

spoofing & Man in the Middle
Note though that w.r.t. provisioning DNS has similar weaknesses. Registries and Registrars sometimes make mistakes.
Wrap-up
DANE has the potential to solve important PKI/TLS problems

Not a magic bullet

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

Not the only approach

‘convergence’

Not a magic bullet either
The Internet PKI has a trust issue.

A global trust issue

Scalability problems: compliance and technology
Internet Trust is Global
Trust

Local action
global effect

misaligned
incentives ??
How to increase global trust in the Internet?

Without a race to the bottom of minimal compliance?

With meaningful incremental steps in improving technology?
That's it folk

Questions, comments, ideas:
olaf@nlnetlabs.nl