Dane?

DigiNotar®
A VASCO COMPANY

DigiNotar®
A VASCO COMPANY

Enough said?

No?

The Longer Version…

https://www.flickr.com/photos/hyper7/7287993694

Home Diginotar internet trust ser… … ktronische handtekening.

http://www.diginotar.nl/

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

Home Diginotar internet trust ser…

A Certificate Authority

DigiNotar®
A VASCO COMPANY

HOME | ACTUEEL | … GEN | KLANTENSERVICE | OVER DIGINOTAR

zoek… zoek

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 ser… … ktronische handtekening.

http://www.diginotar.nl/

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

Home Diginotar internet trust ser…

DigiNotar®
A VASCO COMPANY

HOME | ACTUEEL | … | 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

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

What went wrong?

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


Multiple hacker tools on the servers
Online Certification Authority
Server Compromise
Specialized PKI scripts
Incomplete audit trails
Fake certificate issued for *.google.com
Fake certific
private key published
Iran users of gmail are compromised by a mitm attack

Fake certificate issued for *.google.com

+

Fake certificate private key published

=

Any attacker-in-the-middle can intercept a connection request for mail.google.com, and initiate a “secure” connection using the fake certificate, and your browser could be fooled into believing that this was the genuine server!

Fake certificate

+

Fake certificate private key published

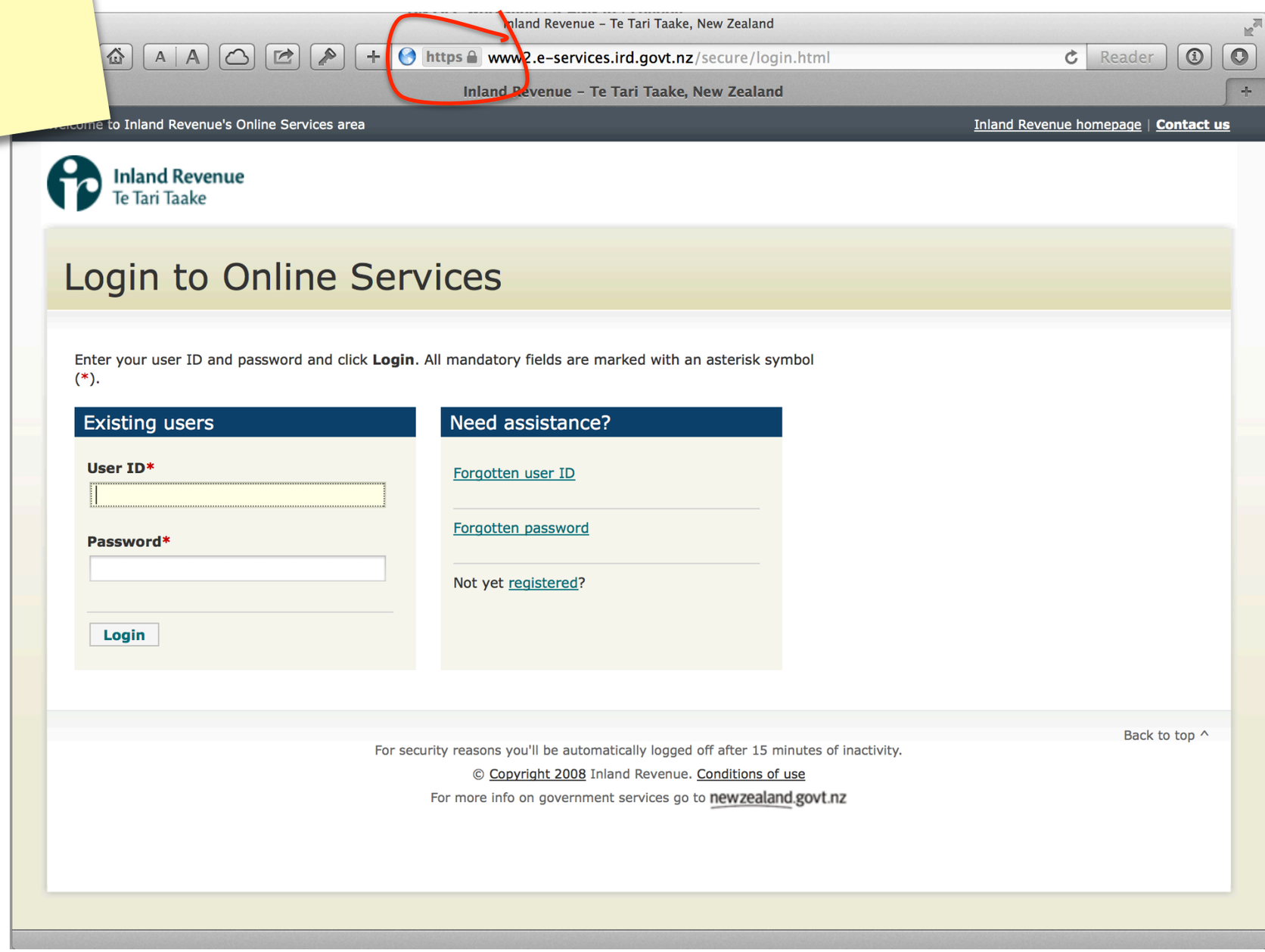
=

Was this a one-off?

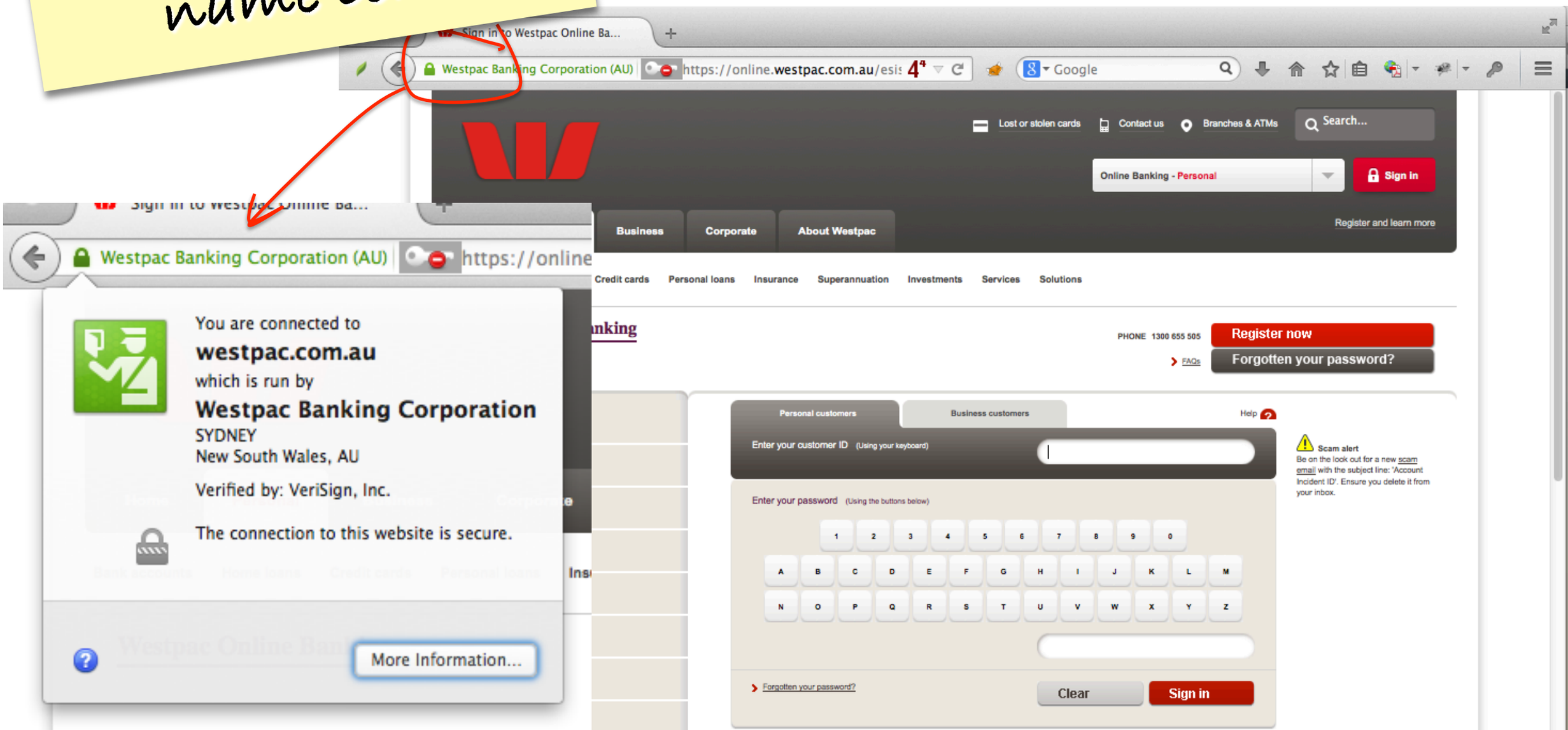
Any attacker
can intercep
request for
and initiate a "
using the fa
your browser could be
into believing that this was the genuine server!

Or are there implications for the larger issue of our security framework on the Internet?

So much of the Internet relies on trust in security offered by domain name certs

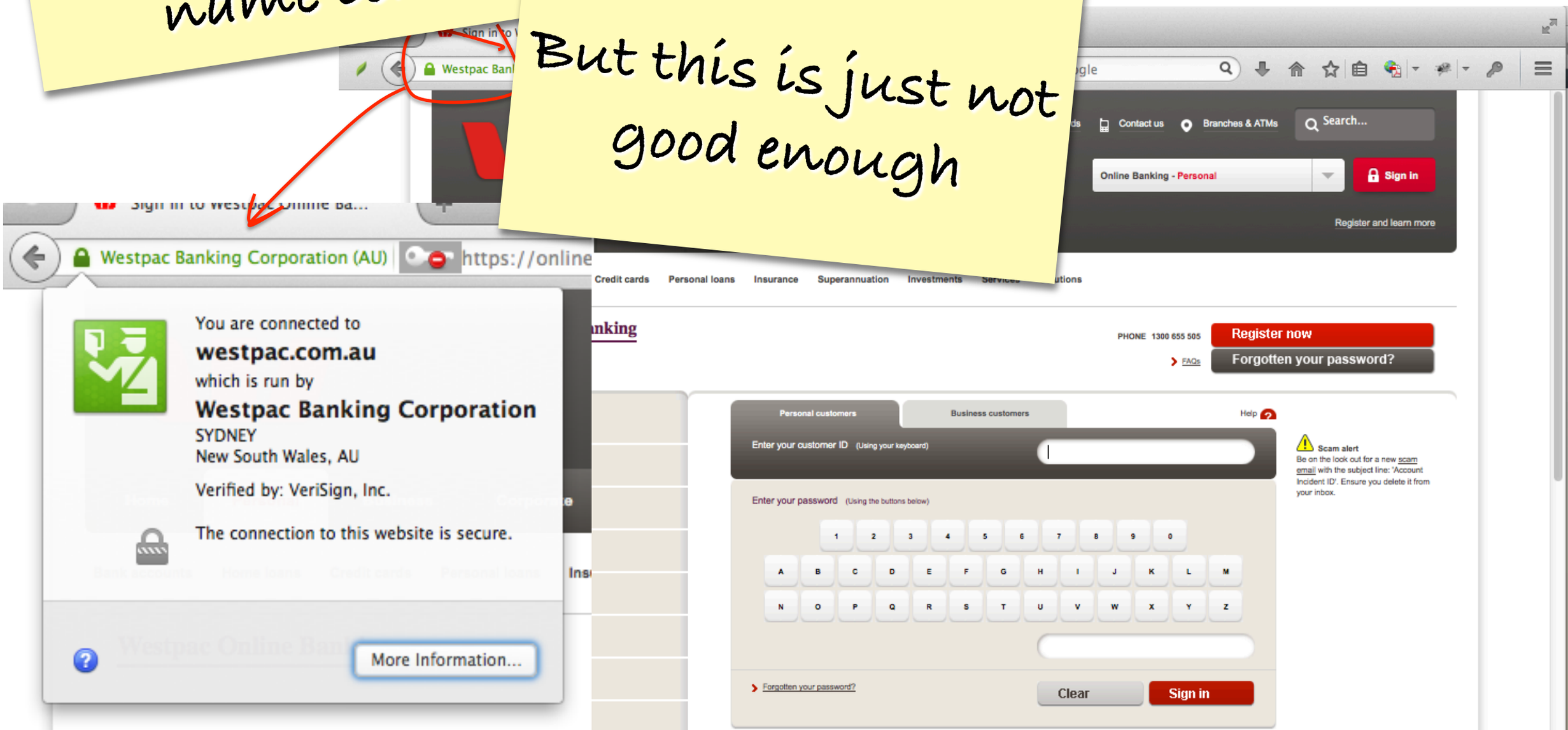


So much of the Internet relies on trust in security offered by domain name certs



So much of the Internet relies on trust in security offered by domain name certs

But this is just not good enough



Two problems:

1. I may not have landed up where I wanted to be:
   DNS cache poisoning
   DNS resolver compromise
   Local host compromise
   Routing compromise

2. The domain name certificate may be fake

The combination of the two implies that I, and the browser I use, may not even notice that we have been mislead. This is bad.

How could it happen?

The 2011 mitm attack was evidently performed by a state-based organisation in Iran, with direct access to national infrastructure, exploiting a fake cert issued by a compromised CA

You don't need to be the NSA or its equivalent to play this game – this form of attack would work at any scale.

Either the attacker is already on path to the intended site, or the attacker can use access to routing to inject routes that direct the data flows to the attack point

Why could it happen?

The TLS session cannot say WHICH CA is to be used to validate the server certificate

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

Compromised CAs imperil the entire framework of security!

This is broken!

Domain Name certification should use trust and integrity of operation as a differentiator

- If you pay more money you would expect to use a service that operates with greater levels of care and data protection of your data and users of your service would be “more secure” – right?

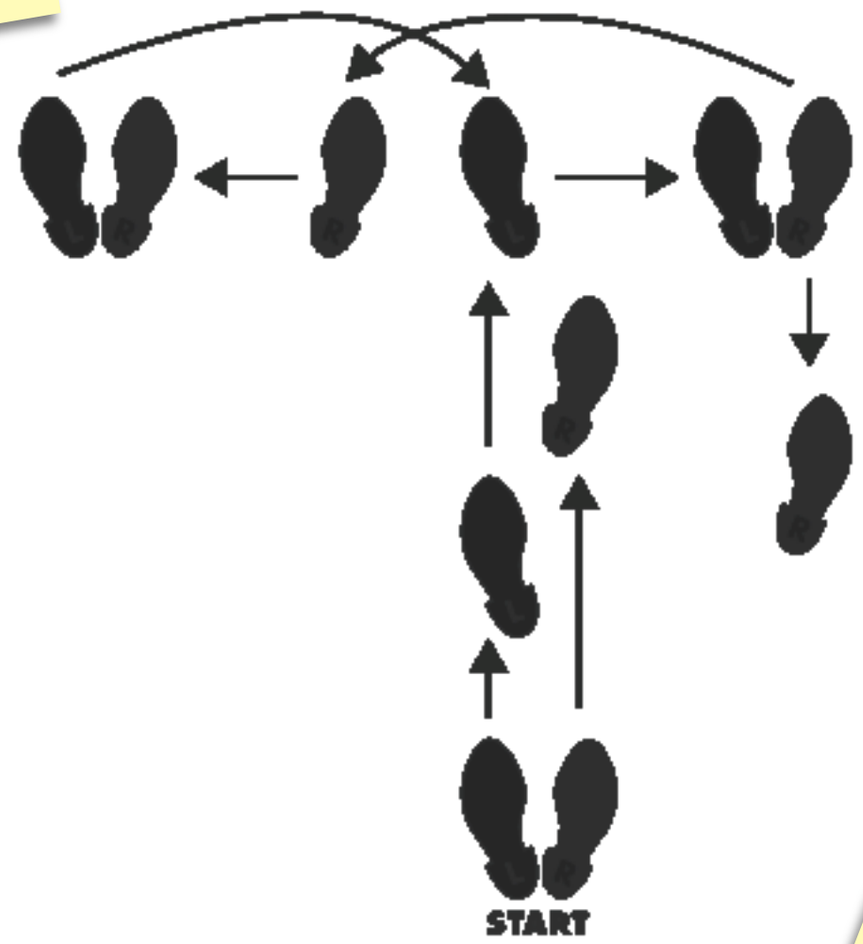
But a compromised CA can issue a domain name certificate for ANY domain name

- If you trust this compromised CA then you are going to trust its products

The entire Domain Name CA operation is only as good as the worst CA!

- It does not matter what CA service you use, because any compromised CA can compromise users of your service

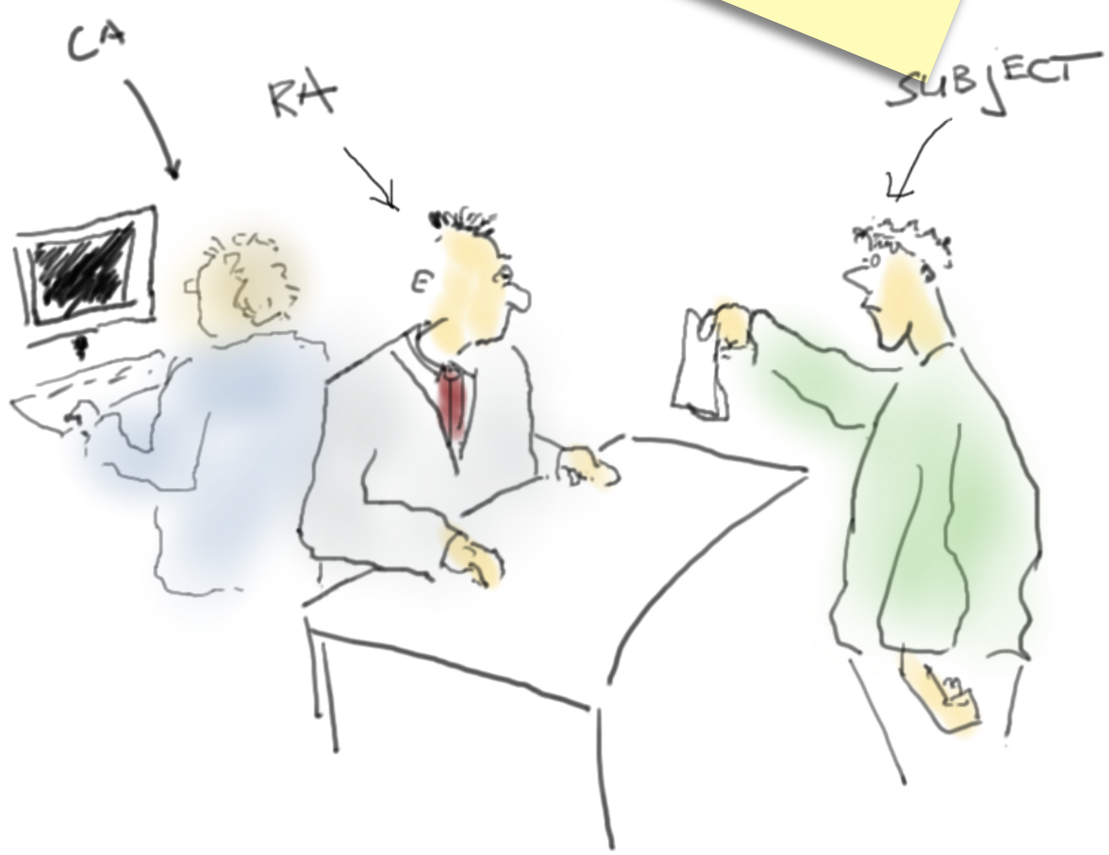
Lets take a step back



and talk about PKI

The role of a CA:

3rd party trust broker

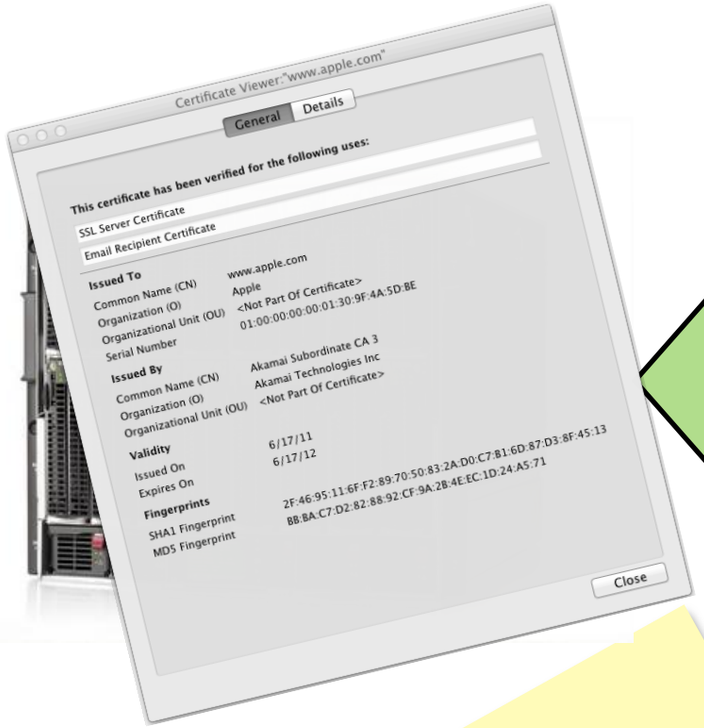


Subject Requests

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 [illegible] trust to online transactions by requiring website operator [illegible] 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 Example

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 hat have undergone more rigorous vetting. Since any successful SSL connection ses 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

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

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

HSTS

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

DNS-Based Authentication of Named Entities

RFC 6394

RFC 6698

How to represent and authenticate "named entities" in the DNS, using DNSSEC

Web sites

Email addres

Jabber IDs

RFC6394: TLSA RR

2.3. TLSA RR Examples

In the following examples, the domain name is f
in Section 3.

An example of a hashed (SHA-256) association c
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 end entity
certificate:

```
_443._tcp.www.example.com. IN TLSA (
   3 0 0 30820307308201efa003020102020... )
```

CA Cert

EE Cert

Trust Anchor

valid CERTs and/or CAs are stored in the the DNS

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

i.e. your service is compromised only if your chosen CA is compromised!

valid CERTS and/or CAs are stored in the the DN

If the DNS provides the EE cert, then DANE offers the protection that you are looking at a valid Certificate issued by the entity that holds the domain name in the first place

Name Certificate publication is controlled by the zone authority – no CA intermediary is needed

security is "free"

How does DNSSEC get into the picture?

How doe
DNSSEC
into the pic

DANE assumes a DNS that operates with integrity

Is the certificate provided in a TLSA response genuine?

To answer that you need to be able to validate the DNS response

And to do that you need DNSSEC

Did you keep this thought?

DV
Domain validation

Obtaining Rogue (DV) Certificates

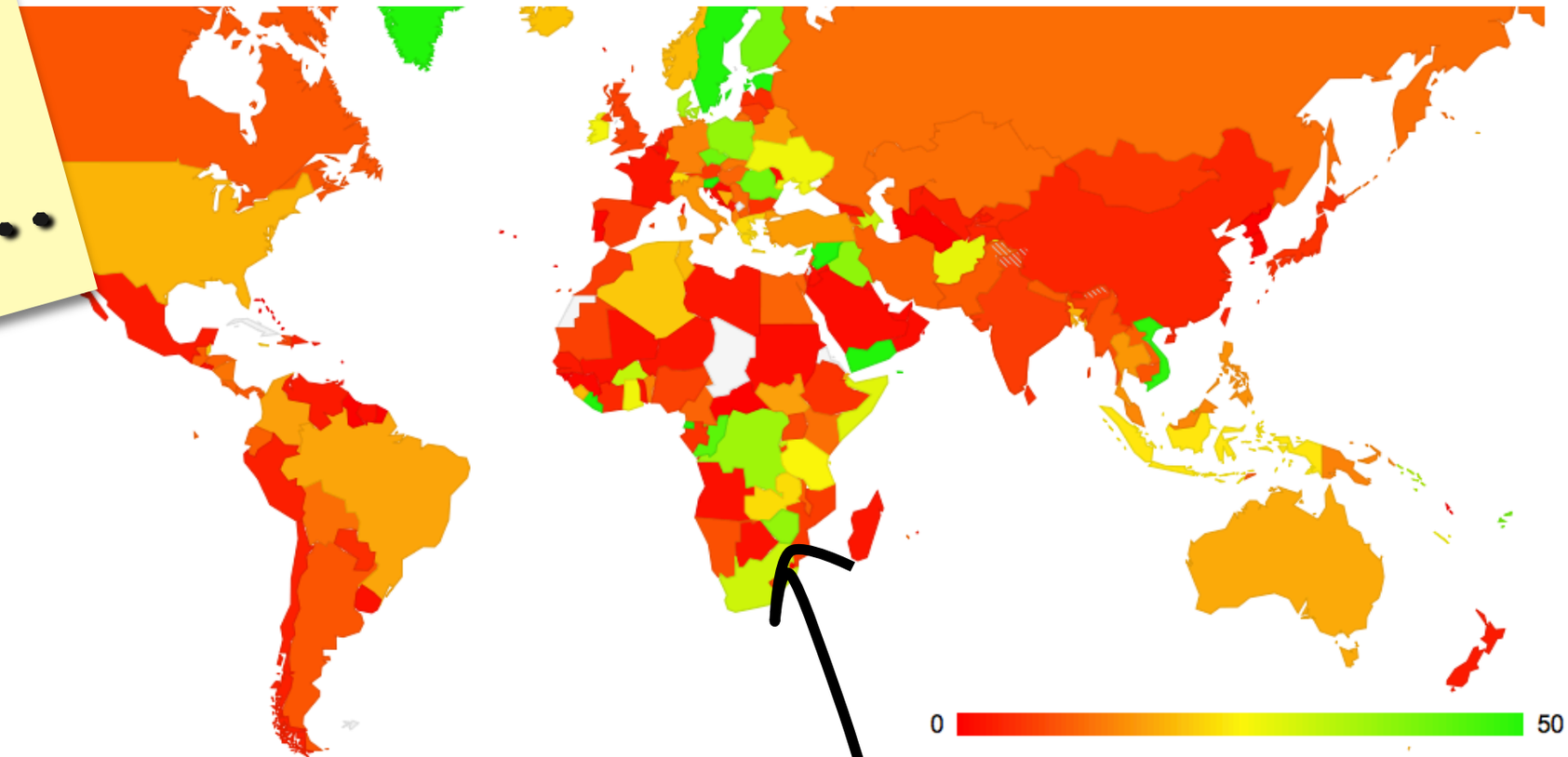
All these checks are based on information fetched from the DNS

Own the DNS and the DV is yours

DANE has the potential to solve important PKI/TLS problems in securing access to named entities

And for DANE to work then DNSSEC is necessary

How are we going with DNSSEC?..



High levels of DNSSEC use seen in Africa, Eastern and Northern Europe

11% of users send their DNS queries to DNSSEC-validating resolvers

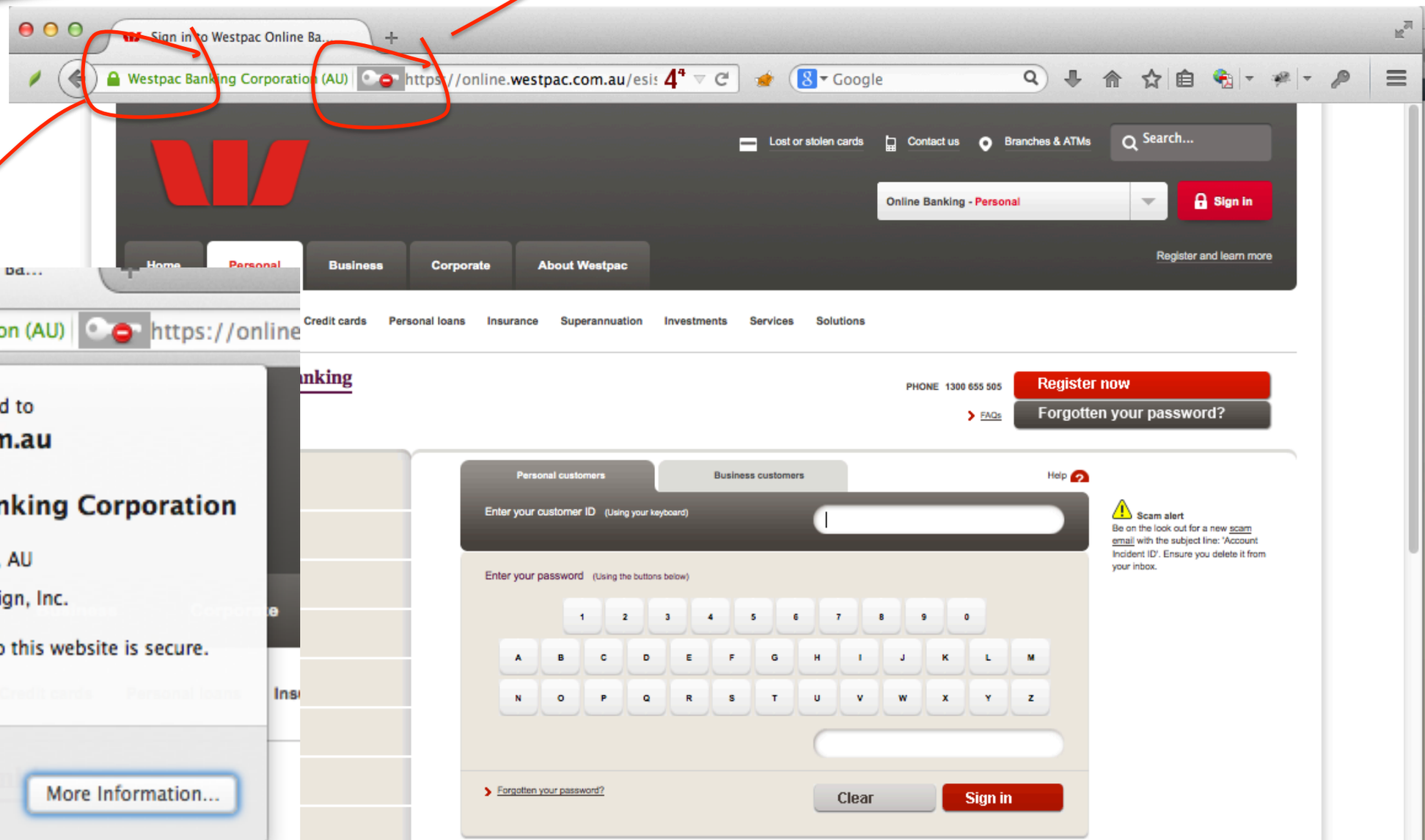
Why invest in DNSSEC?

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!

this is just not good enough any more



What needs to happen?

- The local name management infrastructure should support the use of DNSSEC in all aspects of name management

What needs to happen?

- The local name management infrastructure should support the use of DNSSEC in all aspects of name management
- ISPs should add DNSSEC validation to their forwarding resolvers

Use of DNSSEC Validation for New Zealand (NZ)

ASN	AS Name	DNSSEC Validates	Samples
AS58600	FLIP-AS-AP Flip Services Limited	85.52%	145
AS17705	INSPIRENET-AS-AP InSPire Net Ltd	48.39%	62
AS24183	DTS-ISP-CORE1-AP DTS LTD	37.25%	51
AS9503	FX-PRIMARY-AS FX Networks Limited	32.67%	150
AS55853	MEGATEL-AS-AP Megatel	16.55%	145
AS9245	COMPASS-NZ-AP COMPASS	5.26%	76
AS10200	NETSMART-AP Web hosting provider and ISP connectivity.	3.70%	54
AS55850	TRUSTPOWERLTD-AS-AP TrustPower Ltd	3.45%	145
AS58610	TELNET-AS-AP Telnet Telecommunication Limited	3.16%	95
AS17412	WOOSHWIRELESSNZ Woosh Wireless	2.96%	169
AS45267	LIGHTWIRE-AS-AP Lightwire LTD	2.78%	144
AS9876	AIRNET-HB-AS-AP NOW	2.70%	74
AS17746	ORCONINTERNET-NZ-AP Orcon Internet	1.82%	1483
AS23655	SNAP-NZ-AS Snap Internet Limited	1.60%	500
AS9790	CALLPLUS-NZ-AP CallPlus Services Limited	1.55%	1995
AS38793	NZCOMMS-AS-AP Two Degrees Mobile Limited	1.14%	88
AS4768	CLIX-NZ TelstraClear Ltd	1.02%	2347
AS4771	NZTELECOM Telecom New Zealand Ltd.	0.97%	9004
AS7657	VODAFONE-NZ-NGN-AS Vodafone NZ Ltd.	0.89%	3696
AS4648	NZIX-2 Netgate	0.86%	348
AS9431	AKUNI-NZ The University of Auckland	0.62%	162
AS23905	VUW-AS-AP Victoria University of Wellington	0.00%	71
AS55872	BAYCITY-AS-AP BayCity Communications Limited	0.00%	64
AS18199	LINKTELECOM-NZ-AP Link Telecom (NZ) Limited	0.00%	141
AS38305	OTAGO-UNIVERSITY-AS-NZ-AP The University of Otago	0.00%	77
AS56030	VOYAGERNET-AS-AP Voyager Internet Ltd.	0.00%	65
AS17435	WXC-AS-NZ WorldxChange Communications LTD	0.00%	88

Use of DNSSEC Validation for Australia (AU)

What needs to happen?

- The local name management infrastructure should support the use of DNSSEC in all aspects of name management
- ISPs should add DNSSEC validation to their forwarding resolvers
- And if you want to push it a bit in the right direction...

  For secure named services using a domain name certificate, add the Issuer's public CA cert as a DANE record into your DNSSEC-signed zone

That's it!