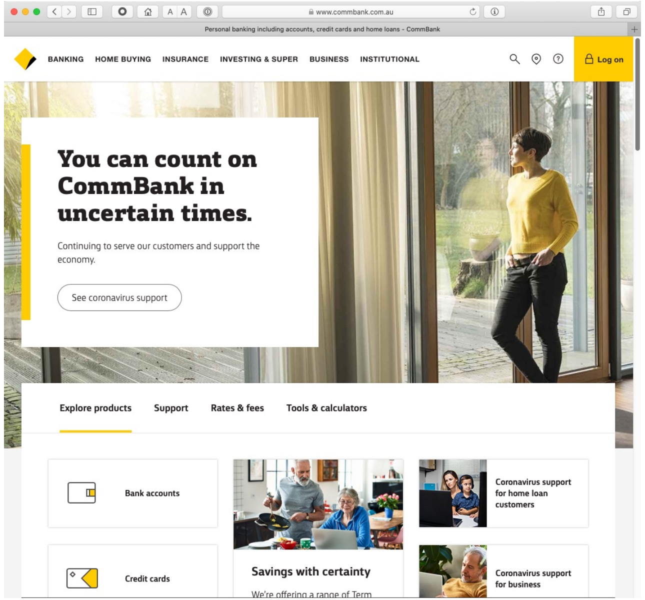
Trust and Security

Geoff Huston AM
Chief Scientist, APNIC

Which Bank?



You can count on CommBank in uncertain times.

Continuing to serve our customers and support the economy.

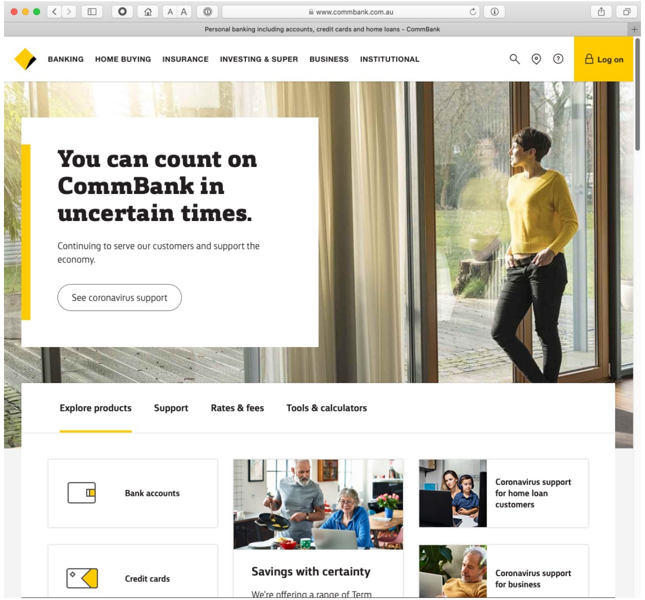
Savings with certainty

We're offering a range of Term

Coronavirus support for home loan customers
Coronavirus support for business

Which Bank? My Bank!

i hope!



You can count on CommBank in uncertain times.

Continuing to serve our customers and support the economy.

Savings with certainty

We're offering a range of Term

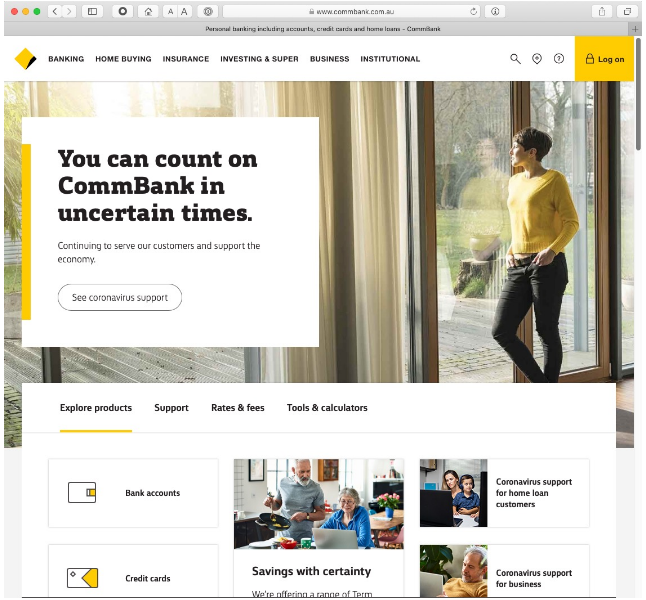
Coronavirus support for home loan customers

Coronavirus support for business

Security on the Internet

How do you know that you are really going to where you thought you were going to?

its trivial to create a web page to look exactly like another



You can count on CommBank in uncertain times.

Continuing to serve our customers and support the economy.

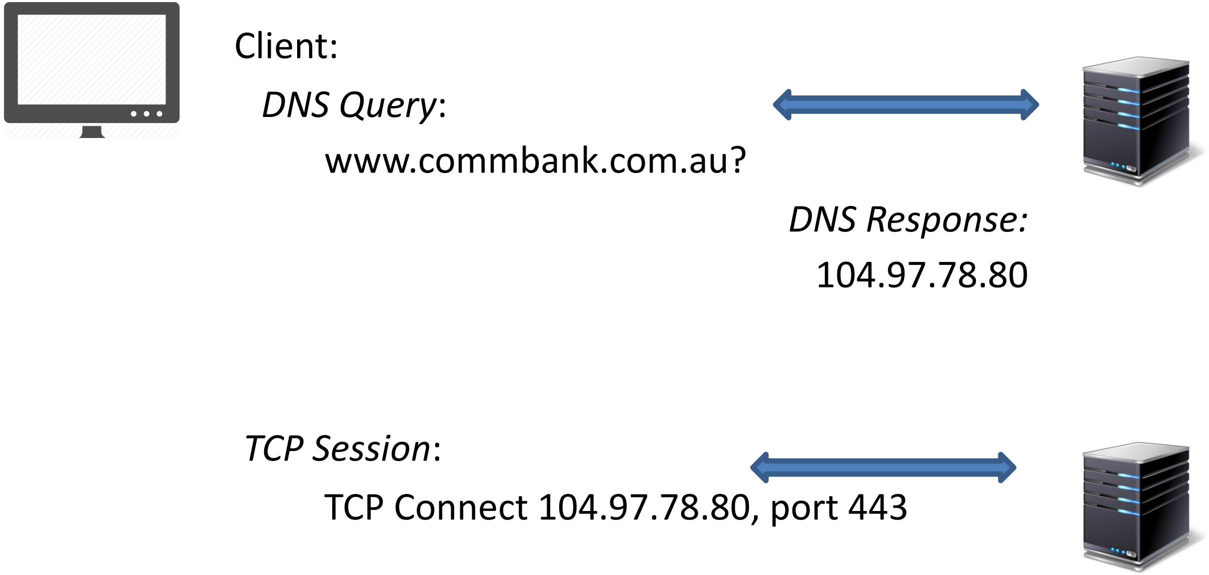
Savings with certainty

We're offering a range of Term

Coronavirus support for home loan customers

Coronavirus support for business

Opening the Connection: First Steps



Client:

DNS Query:

www.commbank.com.au?

DNS Response:

104.97.78.80

TCP Session:

TCP Connect 104.97.78.80, port 443

Hang on…

Who “owns” that IP address? The Commonwealth Bank? Someone else?

Let’s look at little more:

```
$ dig -x 104.97.78.80 +short
a104-97-78-80.deploy.static.akamaitechnologies.com
```

Hang on…

```
$ dig -x 104.97.78.80 +short
a104-97-78-80.deploy.static.akamaitechnologies.com
```

That’s **not** an IP addresses that was allocated to the Commonwealth Bank!

The Commonwealth Bank of Australia has the address blocks

140.168.0.0 - 140.168.255.255 and

203.17.185.0 - 203.17.185.255

Hang on…

```
$ dig -x 104.97.78.80 +short
a104-97-78-80.deploy.static.akamaitechnologies.com
```

That’s an Akamai IP address

And I’m NOT a customer of the Internet Bank of Akamai!

Why should my browser trust that 104.97.78.80 is really the authentic web site for the Commonwealth Bank of Australia, and not some dastardly evil scam designed to steal my passwords and my money?

And why should I trust my browser?

Trust

More generally: **Who and What am I trusting?**

It seems that I’m trusting in the “correct” operation of:

- My browser
- My host platform
- My system clock
- DNS name resolution
- The Internet’s Routing System
- All of the Web PKI CAs
- Public/Private key cryptographic algorithms
- The other end’s infrastructure

How?

- HOW is this trust authenticated?

Asymmetric Cryptography

Using public/private key cryptography requires a pair of keys (A,B) such that:

- Anything encrypted using key A can ONLY be decrypted using key B, and no other key
- Anything encrypted using key B can ONLY be decrypted using key A, and no other key
- Knowing the value of one key WILL NOT let you work out the value of the other key!

This form of asymmetric cryptography lies at the heart of the Internet’s security framework

Public/Private Key Pairs

If I have a copy of your PUBLIC key, and you encrypt a message with your PRIVATE key, and I can decrypt the message using your PUBLIC key, then

- I know no one has tampered with your original message
- And I know it was you that sent it.
- And you can't deny it.

If we negotiate a session key using the combination of your public key and a local private session key and encrypt all session messages using this session key, then

- I am confident no one else can eavesdrop on our conversation in this session

Public Key Certificates

But how do I know this is YOUR public key?

- And not the public key of some dastardly evil agent pretending to be you?

- I don't know you
- I've never met you
- So, I have absolutely no clue if this public key value is yours or not!

Public Key Certificates

What if I ‘trust’ an intermediary*?

  - Who has contacted you and validated your identity and conducted a ‘proof of possession’ test that you have control of a private key that matches your public key

- If this trusted intermediary signs an attestation that this is your public key (with their private key) then I would be able to trust this public key
- This ‘attestation’ takes the form of a “public key certificate”

** If you have ever used “public notaries” to validate a document, then this is a digital equivalent*

TLS - Transport Layer Security

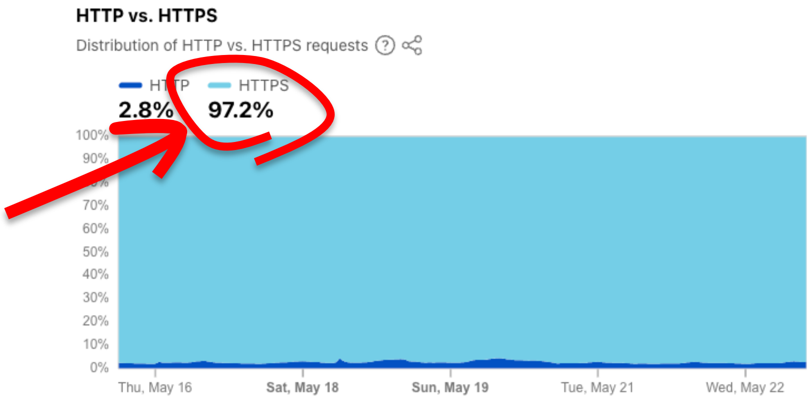
“Am I connecting to the named service that I intended to to connect to?”

- Almost universally used in the web context

TLS - Transport Layer Security

“Am I connecting to the named service that I intended to to connect to?”

- Almost universally used in the web context



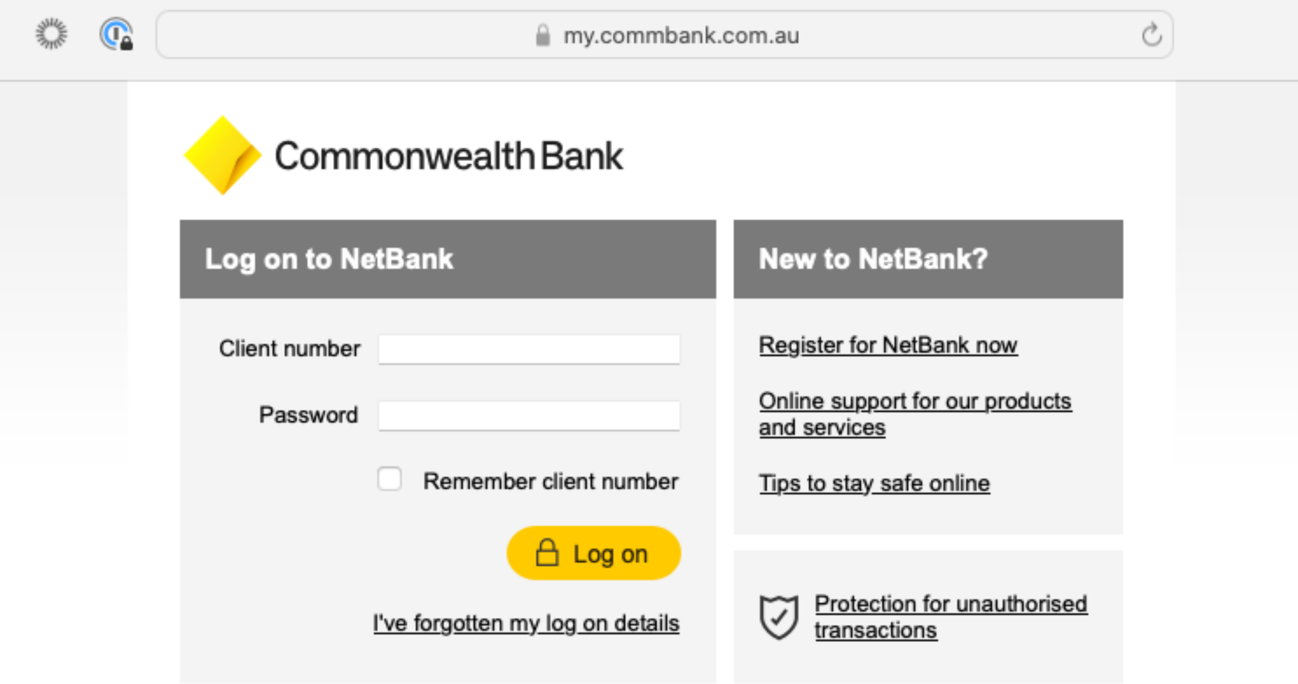
HTTP vs. HTTPS

Distribution of HTTP vs. HTTPS requests

How does TLS work?

- The domain name owner demonstrates to a trusted Certification Authority that is has **control over a domain name**
- The CA certifies the domain name owner's public key in the form of a **domain name certificate** as an X.509 domain name certificate
- This certificate (and the public key) is passed to the client in the Server Hello party of a TLS handshake, together with a cipher text that was encrypted using the matching private key
- If the client application can decode the cipher text using the provided public key, and validate the certificate against any of its trusted CAs then it assumes that it is connecting to the authentic service

TLS on Safari



my.commbank.com.au

Commonwealth Bank

Log on to NetBank

Client number

Password

□ Remember client number

Log on

I've forgotten my log on details

New to NetBank?

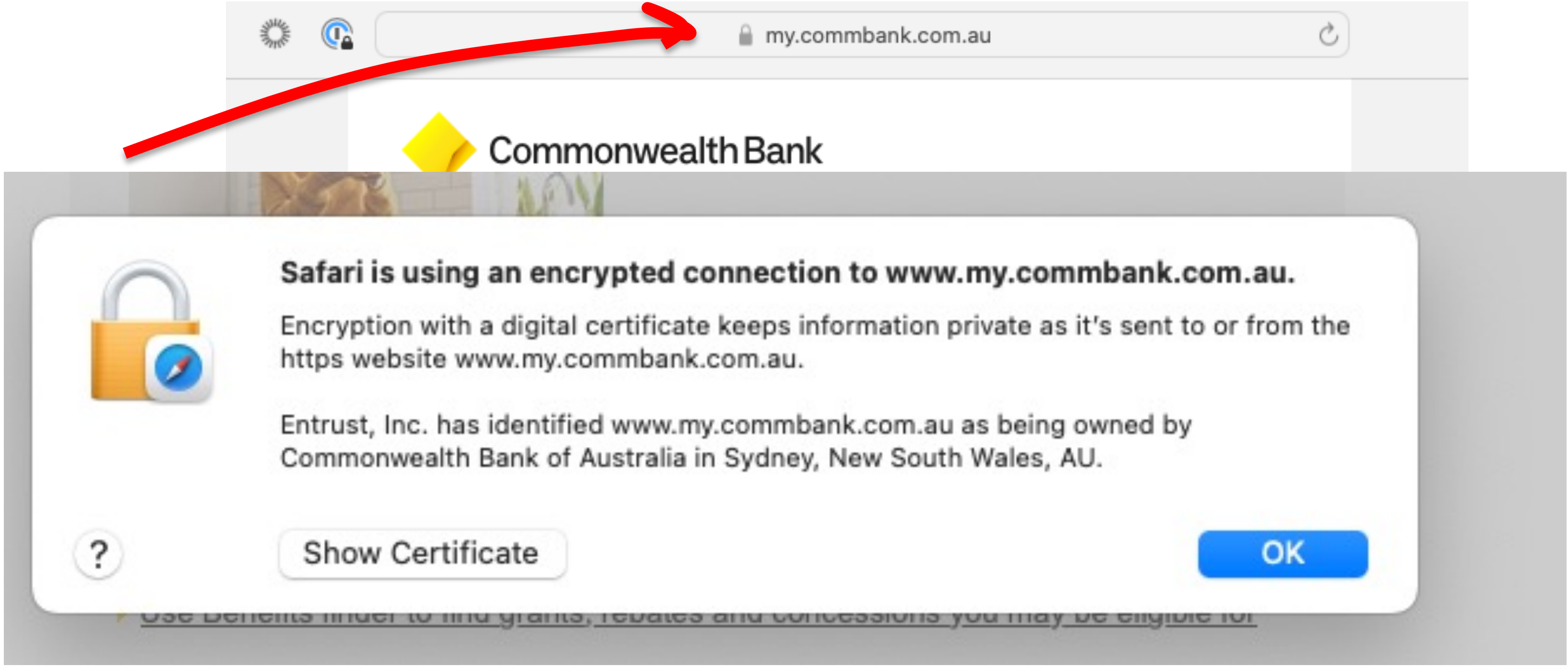
Register for NetBank now

Online support for our products and services

Tips to stay safe online

Protection for unauthorised transactions

TLS on Safari

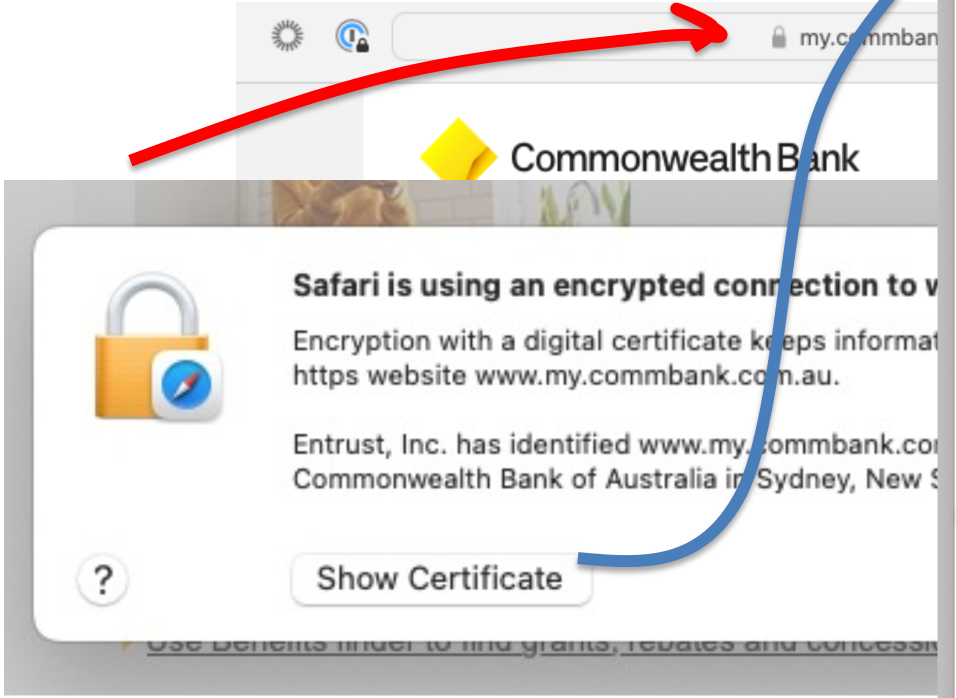


Safari is using an encrypted connection to www.my.commbank.com.au.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.my.commbank.com.au.

Entrust, Inc. has identified www.my.commbank.com.au as being owned by Commonwealth Bank of Australia in Sydney, New South Wales, AU.

TLS on S



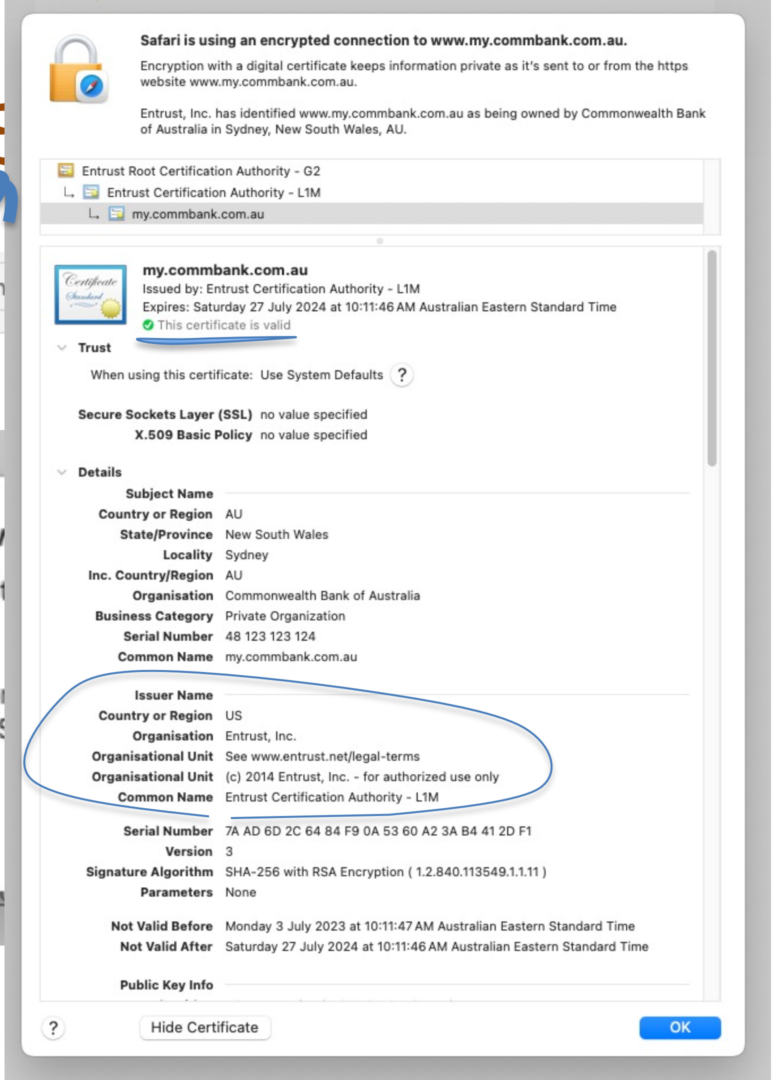
my.commban

Commonwealth Bank

Safari is using an encrypted connection to w

Encryption with a digital certificate keeps informat
https website www.my.commbank.com.au.

Entrust, Inc. has identified www.my.commbank.co
Commonwealth Bank of Australia in Sydney, New S



Safari is using an encrypted connection to www.my.commbank.com.au.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.my.commbank.com.au.

Entrust, Inc. has identified www.my.commbank.com.au as being owned by Commonwealth Bank of Australia in Sydney, New South Wales, AU.

```
Entrust Root Certification Authority - G2
 └ Entrust Certification Authority - L1M
    └ my.commbank.com.au
```

my.commbank.com.au
Issued by: Entrust Certification Authority - L1M
Expires: Saturday 27 July 2024 at 10:11:46 AM Australian Eastern Standard Time
✓ This certificate is valid

Trust

When using this certificate: Use System Defaults ?

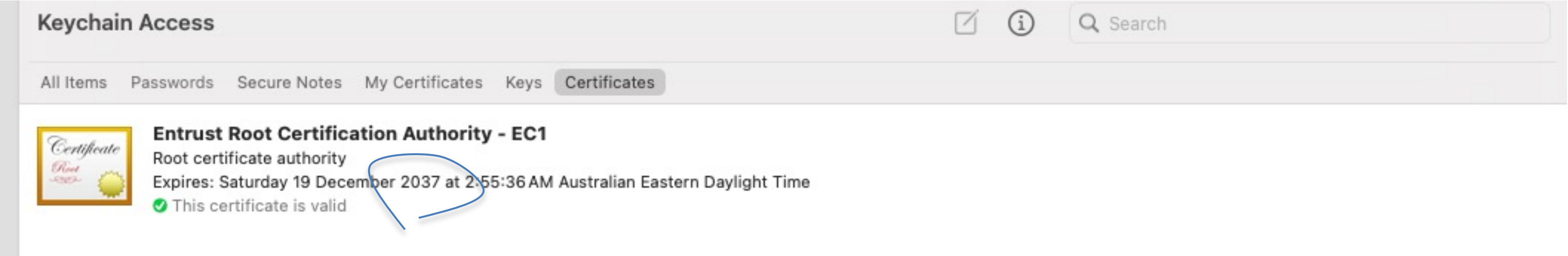
Secure Sockets Layer (SSL)	no value specified
X.509 Basic Policy	no value specified

Details

Subject Name	
Country or Region	AU
State/Province	New South Wales
Locality	Sydney
Inc. Country/Region	AU
Organisation	Commonwealth Bank of Australia
Business Category	Private Organization
Serial Number	48 123 123 124
Common Name	my.commbank.com.au
Issuer Name	
Country or Region	US
Organisation	Entrust, Inc.
Organisational Unit	See www.entrust.net/legal-terms
Organisational Unit	(c) 2014 Entrust, Inc. - for authorized use only
Common Name	Entrust Certification Authority - L1M
Serial Number	7A AD 6D 2C 64 84 F9 0A 53 60 A2 3A B4 41 2D F1
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Monday 3 July 2023 at 10:11:47 AM Australian Eastern Standard Time
Not Valid After	Saturday 27 July 2024 at 10:11:46 AM Australian Eastern Standard Time
Public Key Info	

Trust

My system trusts EVERYTHING that Entrust certifies - and for the next 13 years too!



Entrust Root Certification Authority - EC1
Root certificate authority
Expires: Saturday 19 December 2037 at 2:55:36 AM Australian Eastern Daylight Time
✓ This certificate is valid

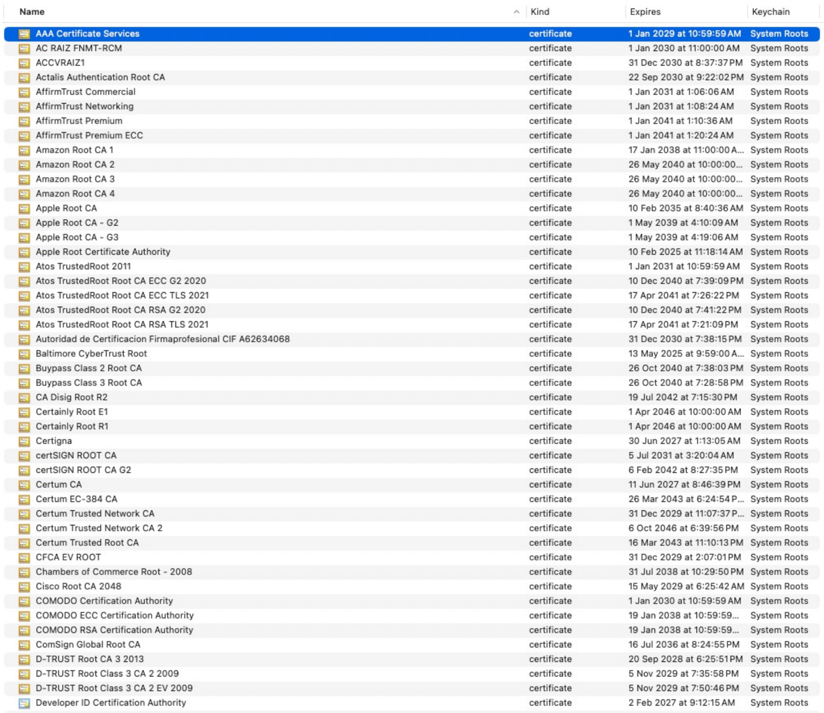
What is assumed here?

- That all of these trusted CAs (and there are a few hundred of them) NEVER EVER lie!
- That the tests applied by the CA in issuing a certificate are robust
- That the CA has not been compromised in any way
- That there is a single unique DNS name space
- The integrity and strength of encryption algorithms

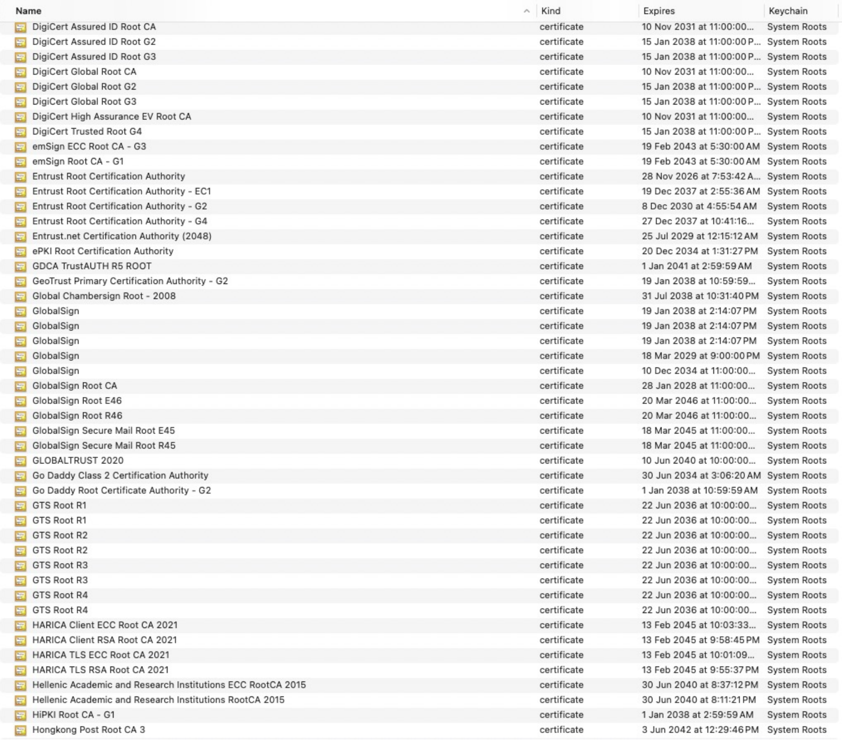
Subverting the Web PKI

- The problem here is that the TLS handshake does not tell the client WHICH CA has certified the server’s public key
- So if I can compromise ANY CA then I can generate certificates for ANY domain name
- And the client can’t tell the difference
- So this system is only as strong as the weakest CA
- So you would think we’d like to limit the number of CAs in this system – yes?

Trust? or Credulity?



Name	Kind	Expires	Keychain
AAA Certificate Services	certificate	1 Jan 2029 at 10:59:59 AM	System Roots
AC RAIZ FNMT-RCM	certificate	1 Jan 2030 at 11:00:00 AM	System Roots
ACCVRAIZ1	certificate	31 Dec 2030 at 8:37:37 PM	System Roots
Actalis Authentication Root CA	certificate	22 Sep 2030 at 9:22:02 PM	System Roots
AffirmTrust Commercial	certificate	1 Jan 2031 at 1:06:06 AM	System Roots
AffirmTrust Networking	certificate	1 Jan 2031 at 1:08:24 AM	System Roots
AffirmTrust Premium	certificate	1 Jan 2041 at 1:10:36 AM	System Roots
AffirmTrust Premium ECC	certificate	1 Jan 2041 at 1:20:24 AM	System Roots
Amazon Root CA 1	certificate	17 Jan 2038 at 11:00:00 A...	System Roots
Amazon Root CA 2	certificate	26 May 2040 at 10:00:00...	System Roots
Amazon Root CA 3	certificate	26 May 2040 at 10:00:00...	System Roots
Amazon Root CA 4	certificate	26 May 2040 at 10:00:00...	System Roots
Apple Root CA	certificate	10 Feb 2035 at 8:40:36 AM	System Roots
Apple Root CA - G2	certificate	1 May 2039 at 4:10:09 AM	System Roots
Apple Root CA - G3	certificate	1 May 2039 at 4:19:06 AM	System Roots
Apple Root Certificate Authority	certificate	10 Feb 2025 at 11:18:14 AM	System Roots
Atos TrustedRoot 2011	certificate	1 Jan 2031 at 10:59:59 AM	System Roots
Atos TrustedRoot Root CA ECC G2 2020	certificate	10 Dec 2040 at 7:39:09 PM	System Roots
Atos TrustedRoot Root CA ECC TLS 2021	certificate	17 Apr 2041 at 7:26:22 PM	System Roots
Atos TrustedRoot Root CA RSA G2 2020	certificate	10 Dec 2040 at 7:41:22 PM	System Roots
Atos TrustedRoot Root CA RSA TLS 2021	certificate	17 Apr 2041 at 7:21:09 PM	System Roots
Autoridad de Certificacion Firmaprofesional CIF A62634068	certificate	31 Dec 2030 at 7:38:15 PM	System Roots
Baltimore CyberTrust Root	certificate	13 May 2025 at 9:59:00 A...	System Roots
Buypass Class 2 Root CA	certificate	26 Oct 2040 at 7:38:03 PM	System Roots
Buypass Class 3 Root CA	certificate	26 Oct 2040 at 7:28:58 PM	System Roots
CA Disig Root R2	certificate	19 Jul 2042 at 7:15:30 PM	System Roots
Certainly Root E1	certificate	1 Apr 2046 at 10:00:00 AM	System Roots
Certainly Root R1	certificate	1 Apr 2046 at 10:00:00 AM	System Roots
Certigna	certificate	30 Jun 2027 at 1:13:05 AM	System Roots
certSIGN ROOT CA	certificate	5 Jul 2031 at 3:20:04 AM	System Roots
certSIGN ROOT CA G2	certificate	6 Feb 2042 at 8:27:35 PM	System Roots
Certum CA	certificate	11 Jun 2027 at 8:46:39 PM	System Roots
Certum EC-384 CA	certificate	26 Mar 2043 at 6:24:54 P...	System Roots
Certum Trusted Network CA	certificate	31 Dec 2029 at 11:07:37 P...	System Roots
Certum Trusted Network CA 2	certificate	6 Oct 2046 at 6:39:56 PM	System Roots
Certum Trusted Root CA	certificate	16 Mar 2043 at 11:10:13 PM	System Roots
CFCA EV ROOT	certificate	31 Dec 2029 at 2:07:01 PM	System Roots
Chambers of Commerce Root - 2008	certificate	31 Jul 2038 at 10:29:50 PM	System Roots
Cisco Root CA 2048	certificate	15 May 2029 at 6:25:42 AM	System Roots
COMODO Certification Authority	certificate	1 Jan 2030 at 10:59:59 AM	System Roots
COMODO ECC Certification Authority	certificate	19 Jan 2038 at 10:59:59...	System Roots
COMODO RSA Certification Authority	certificate	19 Jan 2038 at 10:59:59...	System Roots
ComSign Global Root CA	certificate	16 Jul 2036 at 8:24:55 PM	System Roots
D-TRUST Root CA 3 2013	certificate	20 Sep 2028 at 6:25:51 PM	System Roots
D-TRUST Root Class 3 CA 2 2009	certificate	5 Nov 2029 at 7:35:58 PM	System Roots
D-TRUST Root Class 3 CA 2 EV 2009	certificate	5 Nov 2029 at 7:50:46 PM	System Roots
Developer ID Certification Authority	certificate	2 Feb 2027 at 9:12:15 AM	System Roots

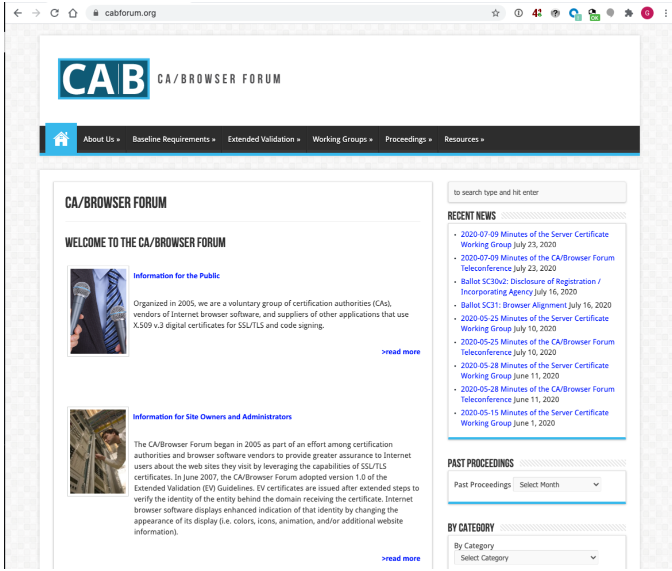


Name	Kind	Expires	Keychain
DigiCert Assured ID Root CA	certificate	10 Nov 2031 at 11:00:00...	System Roots
DigiCert Assured ID Root G2	certificate	15 Jan 2038 at 11:00:00 P...	System Roots
DigiCert Assured ID Root G3	certificate	15 Jan 2038 at 11:00:00 P...	System Roots
DigiCert Global Root CA	certificate	10 Nov 2031 at 11:00:00...	System Roots
DigiCert Global Root G2	certificate	15 Jan 2038 at 11:00:00 P...	System Roots
DigiCert Global Root G3	certificate	15 Jan 2038 at 11:00:00 P...	System Roots
DigiCert High Assurance EV Root CA	certificate	10 Nov 2031 at 11:00:00...	System Roots
DigiCert Trusted Root G4	certificate	15 Jan 2038 at 11:00:00 P...	System Roots
emSign ECC Root CA - G3	certificate	19 Feb 2043 at 5:30:00 AM	System Roots
emSign Root CA - G1	certificate	19 Feb 2043 at 5:30:00 AM	System Roots
Entrust Root Certification Authority	certificate	28 Nov 2026 at 7:53:42 A...	System Roots
Entrust Root Certification Authority - EC1	certificate	19 Dec 2037 at 2:55:36 AM	System Roots
Entrust Root Certification Authority - G2	certificate	8 Dec 2030 at 4:55:54 AM	System Roots
Entrust Root Certification Authority - G4	certificate	27 Dec 2037 at 10:41:16...	System Roots
Entrust.net Certification Authority (2048)	certificate	25 Jul 2029 at 12:15:12 AM	System Roots
ePKI Root Certification Authority	certificate	20 Dec 2034 at 1:31:27 PM	System Roots
GDCA TrustAUTH R5 ROOT	certificate	1 Jan 2041 at 2:59:59 AM	System Roots
GeoTrust Primary Certification Authority - G2	certificate	19 Jan 2038 at 10:59:59...	System Roots
Global Chambersign Root - 2008	certificate	31 Jul 2038 at 10:31:40 PM	System Roots
GlobalSign	certificate	19 Jan 2038 at 2:14:07 PM	System Roots
GlobalSign	certificate	19 Jan 2038 at 2:14:07 PM	System Roots
GlobalSign	certificate	19 Jan 2038 at 2:14:07 PM	System Roots
GlobalSign	certificate	18 Mar 2029 at 9:00:00 PM	System Roots
GlobalSign	certificate	10 Dec 2034 at 11:00:00...	System Roots
GlobalSign Root CA	certificate	28 Jan 2028 at 11:00:00...	System Roots
GlobalSign Root E46	certificate	20 Mar 2046 at 11:00:00...	System Roots
GlobalSign Root R46	certificate	20 Mar 2046 at 11:00:00...	System Roots
GlobalSign Secure Mail Root E45	certificate	18 Mar 2045 at 11:00:00...	System Roots
GlobalSign Secure Mail Root R45	certificate	18 Mar 2045 at 11:00:00...	System Roots
GLOBALTRUST 2020	certificate	10 Jun 2040 at 10:00:00...	System Roots
Go Daddy Class 2 Certification Authority	certificate	30 Jun 2034 at 3:06:20 AM	System Roots
Go Daddy Root Certificate Authority - G2	certificate	1 Jan 2038 at 10:59:59 AM	System Roots
GTS Root R1	certificate	22 Jun 2036 at 10:00:00...	System Roots
GTS Root R1	certificate	22 Jun 2036 at 10:00:00...	System Roots
GTS Root R2	certificate	22 Jun 2036 at 10:00:00...	System Roots
GTS Root R2	certificate	22 Jun 2036 at 10:00:00...	System Roots
GTS Root R3	certificate	22 Jun 2036 at 10:00:00...	System Roots
GTS Root R3	certificate	22 Jun 2036 at 10:00:00...	System Roots
GTS Root R4	certificate	22 Jun 2036 at 10:00:00...	System Roots
GTS Root R4	certificate	22 Jun 2036 at 10:00:00...	System Roots
HARICA Client ECC Root CA 2021	certificate	13 Feb 2045 at 10:03:33...	System Roots
HARICA Client RSA Root CA 2021	certificate	13 Feb 2045 at 9:58:45 PM	System Roots
HARICA TLS ECC Root CA 2021	certificate	13 Feb 2045 at 10:01:09...	System Roots
HARICA TLS RSA Root CA 2021	certificate	13 Feb 2045 at 9:55:37 PM	System Roots
Hellenic Academic and Research Institutions ECC RootCA 2015	certificate	30 Jun 2040 at 8:37:12 PM	System Roots
Hellenic Academic and Research Institutions RootCA 2015	certificate	30 Jun 2040 at 8:11:21 PM	System Roots
HiPKI Root CA - G1	certificate	1 Jan 2038 at 2:59:59 AM	System Roots
Hongkong Post Root CA 3	certificate	3 Jun 2042 at 12:29:46 PM	System Roots

CAs trusted by my computer - and I’m only up to the letter H!

Trust

These Certificate Authorities are listed in my computer's trust set because they claim to operate according to the practices defined by the CAB industry forum (of which they are a member) and they **never** lie!



CA/BROWSER FORUM

WELCOME TO THE CA/BROWSER FORUM

Information for the Public

Organized in 2005, we are a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing.

>read more

Information for Site Owners and Administrators

The CA/Browser Forum began in 2005 as part of an effort among certification authorities and browser software vendors to provide greater assurance to Internet users about the web sites they visit by leveraging the capabilities of SSL/TLS certificates. In June 2007, the CA/Browser Forum adopted version 1.0 of the Extended Validation (EV) Guidelines. EV certificates are issued after extended steps to verify the identity of the entity behind the domain receiving the certificate. Internet browser software displays enhanced indication of that identity by changing the appearance of its display (i.e. colors, icons, animation, and/or additional website information).

>read more

RECENT NEWS

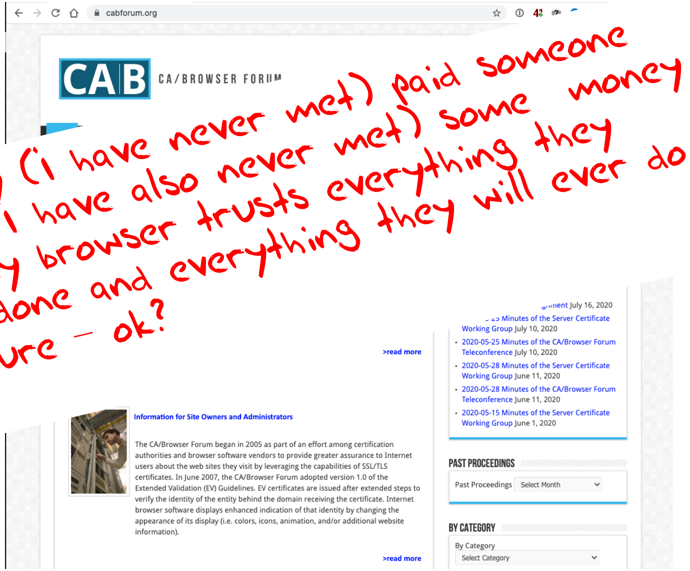
- 2020-07-09 Minutes of the Server Certificate Working Group July 23, 2020
- 2020-07-09 Minutes of the CA/Browser Forum Teleconference July 23, 2020
- Ballot SC30v2: Disclosure of Registration / Incorporating Agency July 16, 2020
- Ballot SC31: Browser Alignment July 16, 2020
- 2020-05-25 Minutes of the Server Certificate Working Group July 10, 2020
- 2020-05-25 Minutes of the CA/Browser Forum Teleconference July 10, 2020
- 2020-05-28 Minutes of the Server Certificate Working Group June 11, 2020
- 2020-05-28 Minutes of the CA/Browser Forum Teleconference June 11, 2020
- 2020-05-15 Minutes of the Server Certificate Working Group June 1, 2020

PAST PROCEEDINGS

BY CATEGORY

Local Trust

These Certificate Authorities are listed in my computer's trust set because they claim to operate according to the practices defined by the CAB industry forum (of which they are a member) and they **never** lie!



...gnment July 16, 2020

- ...-25 Minutes of the Server Certificate Working Group July 10, 2020
- 2020-05-25 Minutes of the CA/Browser Forum Teleconference July 10, 2020
- 2020-05-28 Minutes of the Server Certificate Working Group June 11, 2020
- 2020-05-28 Minutes of the CA/Browser Forum Teleconference June 11, 2020
- 2020-05-15 Minutes of the Server Certificate Working Group June 1, 2020

>read more

Information for Site Owners and Administrators

The CA/Browser Forum began in 2005 as part of an effort among certification authorities and browser software vendors to provide greater assurance to Internet users about the web sites they visit by leveraging the capabilities of SSL/TLS certificates. In June 2007, the CA/Browser Forum adopted version 1.0 of the Extended Validation (EV) Guidelines. EV certificates are issued after extended steps to verify the identity of the entity behind the domain receiving the certificate. Internet browser software displays enhanced indication of that identity by changing the appearance of its display (i.e. colors, icons, animation, and/or additional website information).

>read more

PAST PROCEEDINGS

Past Proceedings: Select Month

BY CATEGORY

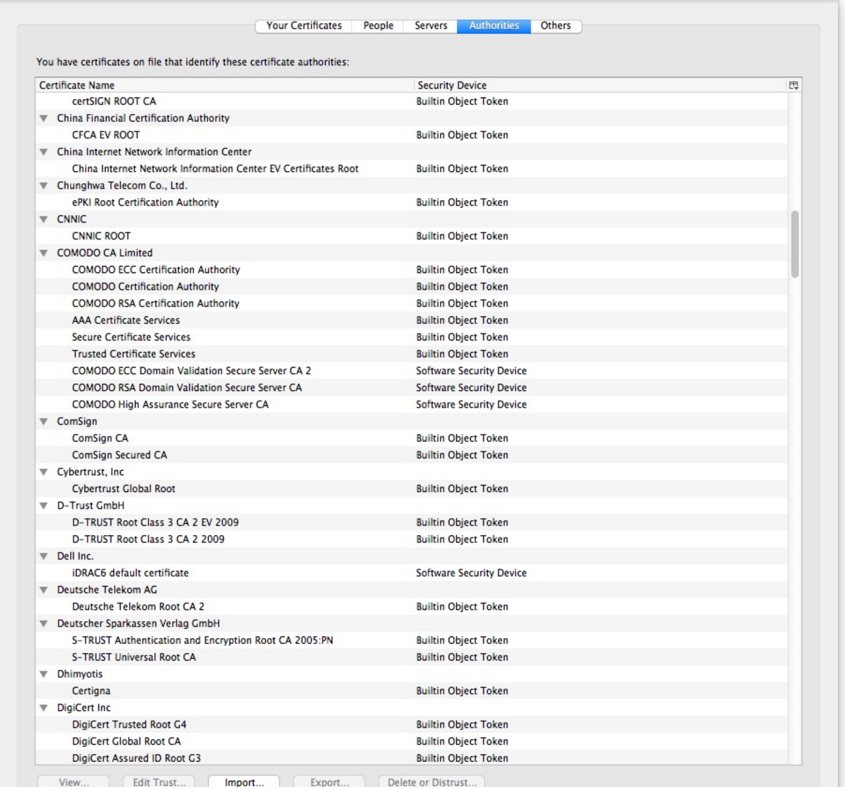
By Category: Select Category

So somebody (I have never met) paid someone
else (whom I have also never met) some money
and then my browser trusts everything they
have ever done and everything they will ever do
in the future – ok?

Local Trust or Local Credulity*?

Wow!

Are they **all** trustable?



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
certSIGN ROOT CA	Builtin Object Token
▼ China Financial Certification Authority	
CFCA EV ROOT	Builtin Object Token
▼ China Internet Network Information Center	
China Internet Network Information Center EV Certificates Root	Builtin Object Token
▼ Chunghwa Telecom Co., Ltd.	
ePKI Root Certification Authority	Builtin Object Token
▼ CNNIC	
CNNIC ROOT	Builtin Object Token
▼ COMODO CA Limited	
COMODO ECC Certification Authority	Builtin Object Token
COMODO Certification Authority	Builtin Object Token
COMODO RSA Certification Authority	Builtin Object Token
AAA Certificate Services	Builtin Object Token
Secure Certificate Services	Builtin Object Token
Trusted Certificate Services	Builtin Object Token
COMODO ECC Domain Validation Secure Server CA 2	Software Security Device
COMODO RSA Domain Validation Secure Server CA	Software Security Device
COMODO High Assurance Secure Server CA	Software Security Device
▼ ComSign	
ComSign CA	Builtin Object Token
ComSign Secured CA	Builtin Object Token
▼ Cybertrust, Inc	
Cybertrust Global Root	Builtin Object Token
▼ D-Trust GmbH	
D-TRUST Root Class 3 CA 2 EV 2009	Builtin Object Token
D-TRUST Root Class 3 CA 2 2009	Builtin Object Token
▼ Dell Inc.	
iDRAC6 default certificate	Software Security Device
▼ Deutsche Telekom AG	
Deutsche Telekom Root CA 2	Builtin Object Token
▼ Deutscher Sparkassen Verlag GmbH	
S-TRUST Authentication and Encryption Root CA 2005:PN	Builtin Object Token
S-TRUST Universal Root CA	Builtin Object Token
▼ Dhimyotis	
Certigna	Builtin Object Token
▼ DigiCert Inc	
DigiCert Trusted Root G4	Builtin Object Token
DigiCert Global Root CA	Builtin Object Token
DigiCert Assured ID Root G3	Builtin Object Token

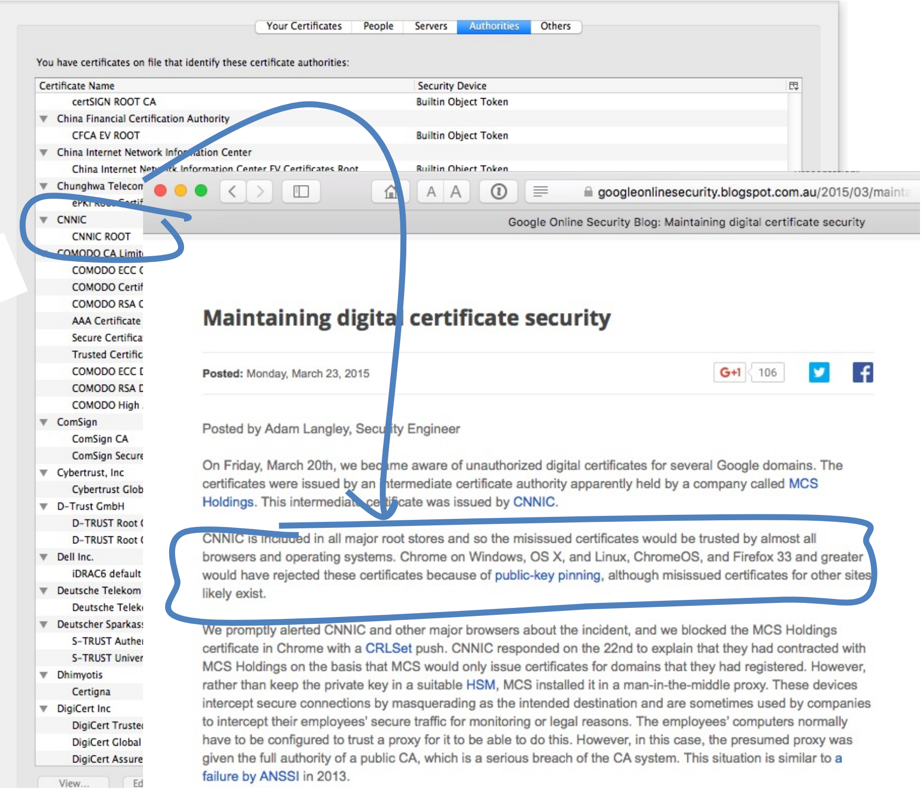
* cre·du·li·ty
/krəˈd(y)o͞olədē/
noun
a tendency to be too ready to believe that something is real or true.

Local Credulity

Wow!

Are they **all** trustable?

Evidently Not!



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
certSIGN ROOT CA	Builtin Object Token
▼ China Financial Certification Authority	
CFCA EV ROOT	Builtin Object Token
▼ China Internet Network Information Center	
China Internet Network Information Center EV Certificates Root	Builtin Object Token
▼ Chunghwa Telecom	
ePKI Root Certif	
▼ CNNIC	
CNNIC ROOT	
▼ COMODO CA Limit	
COMODO ECC C	
COMODO Certif	
COMODO RSA C	
AAA Certificate	
Secure Certifica	
Trusted Certific	
COMODO ECC D	
COMODO RSA D	
COMODO High	
▼ ComSign	
ComSign CA	
ComSign Secure	
▼ Cybertrust, Inc	
Cybertrust Glob	
▼ D-Trust GmbH	
D-TRUST Root C	
D-TRUST Root C	
▼ Dell Inc.	
iDRAC6 default	
▼ Deutsche Telekom	
Deutsche Telek	
▼ Deutscher Sparkas	
S-TRUST Authe	
S-TRUST Univer	
▼ Dhimyotis	
Certigna	
▼ DigiCert Inc	
DigiCert Truste	
DigiCert Global	
DigiCert Assure	

googleonlinesecurity.blogspot.com.au/2015/03/mainta

Google Online Security Blog: Maintaining digital certificate security

Maintaining digital certificate security

Posted: Monday, March 23, 2015

Posted by Adam Langley, Security Engineer

On Friday, March 20th, we became aware of unauthorized digital certificates for several Google domains. The certificates were issued by an intermediate certificate authority apparently held by a company called MCS Holdings. This intermediate certificate was issued by CNNIC.

CNNIC is included in all major root stores and so the misissued certificates would be trusted by almost all browsers and operating systems. Chrome on Windows, OS X, and Linux, ChromeOS, and Firefox 33 and greater would have rejected these certificates because of public-key pinning, although misissued certificates for other sites likely exist.

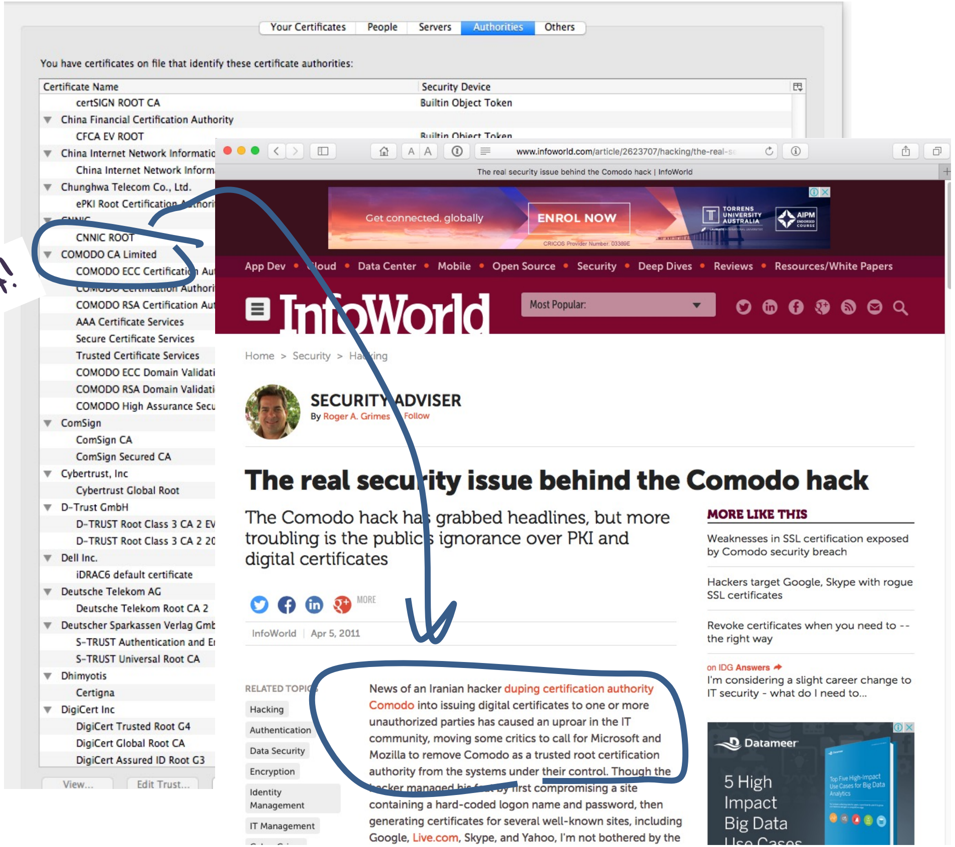
We promptly alerted CNNIC and other major browsers about the incident, and we blocked the MCS Holdings certificate in Chrome with a CRLSet push. CNNIC responded on the 22nd to explain that they had contracted with MCS Holdings on the basis that MCS would only issue certificates for domains that they had registered. However, rather than keep the private key in a suitable HSM, MCS installed it in a man-in-the-middle proxy. These devices intercept secure connections by masquerading as the intended destination and are sometimes used by companies to intercept their employees' secure traffic for monitoring or legal reasons. The employees' computers normally have to be configured to trust a proxy for it to be able to do this. However, in this case, the presumed proxy was given the full authority of a public CA, which is a serious breach of the CA system. This situation is similar to a failure by ANSSI in 2013.

Local Credulity

Wow!

Are they **all** trustable?

Evidently Not!



Your Certificates | People | Servers | Authorities | Others

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
certSIGN ROOT CA	Builtin Object Token
▼ China Financial Certification Authority	
CFCA EV ROOT	Builtin Object Token
▼ China Internet Network Informatio	
China Internet Network Inform	
▼ Chunghwa Telecom Co., Ltd.	
ePKI Root Certification Authori	
▼ CNNIC	
CNNIC ROOT	
▼ COMODO CA Limited	
COMODO ECC Certification Au	
COMODO Certification Authori	
COMODO RSA Certification Aut	
AAA Certificate Services	
Secure Certificate Services	
Trusted Certificate Services	
COMODO ECC Domain Validati	
COMODO RSA Domain Validati	
COMODO High Assurance Secu	
▼ ComSign	
ComSign CA	
ComSign Secured CA	
▼ Cybertrust, Inc	
Cybertrust Global Root	
▼ D-Trust GmbH	
D-TRUST Root Class 3 CA 2 EV	
D-TRUST Root Class 3 CA 2 20	
▼ Dell Inc.	
iDRAC6 default certificate	
▼ Deutsche Telekom AG	
Deutsche Telekom Root CA 2	
▼ Deutscher Sparkassen Verlag Gmb	
S-TRUST Authentication and E	
S-TRUST Universal Root CA	
▼ Dhimyotis	
Certigna	
▼ DigiCert Inc	
DigiCert Trusted Root G4	
DigiCert Global Root CA	
DigiCert Assured ID Root G3	

View... | Edit Trust...

www.infoworld.com/article/2623707/hacking/the-real-s

The real security issue behind the Comodo hack | InfoWorld

App Dev • Cloud • Data Center • Mobile • Open Source • Security • Deep Dives • Reviews • Resources/White Papers

InfoWorld

Most Popular:

Home > Security > Hacking

SECURITY ADVISER

By Roger A. Grimes Follow

The real security issue behind the Comodo hack

The Comodo hack has grabbed headlines, but more troubling is the public's ignorance over PKI and digital certificates

MORE

InfoWorld | Apr 5, 2011

RELATED TOPICS

Hacking

Authentication

Data Security

Encryption

Identity Management

IT Management

News of an Iranian hacker duping certification authority Comodo into issuing digital certificates to one or more unauthorized parties has caused an uproar in the IT community, moving some critics to call for Microsoft and Mozilla to remove Comodo as a trusted root certification authority from the systems under their control. Though the hacker managed his feat by first compromising a site containing a hard-coded logon name and password, then generating certificates for several well-known sites, including Google, Live.com, Skype, and Yahoo, I'm not bothered by the

MORE LIKE THIS

Weaknesses in SSL certification exposed by Comodo security breach

Hackers target Google, Skype with rogue SSL certificates

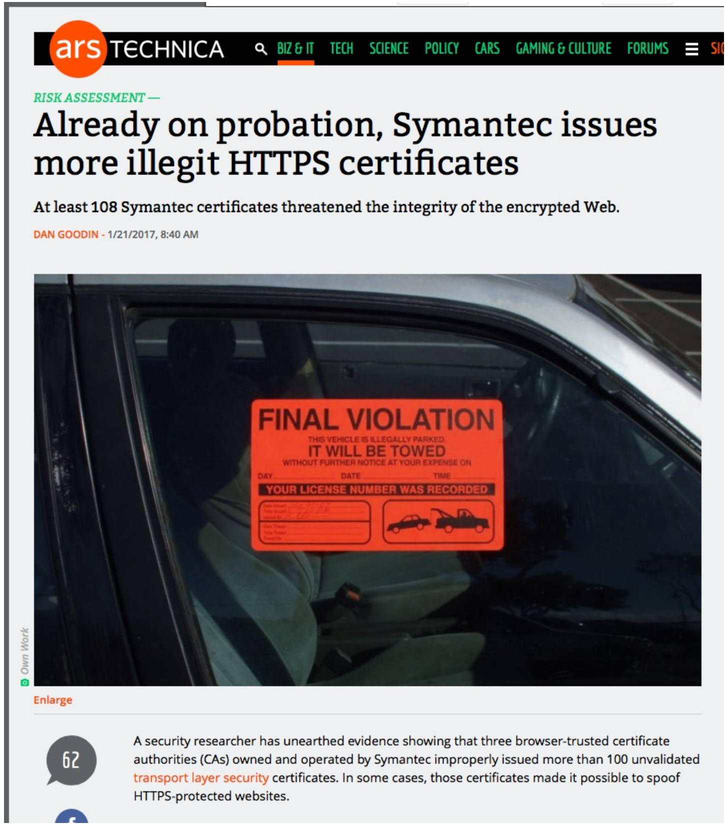
Revoke certificates when you need to -- the right way

on IDG Answers

I'm considering a slight career change to IT security - what do I need to...

Never?

Well, hardly ever



RISK ASSESSMENT —

Already on probation, Symantec issues more illegit HTTPS certificates

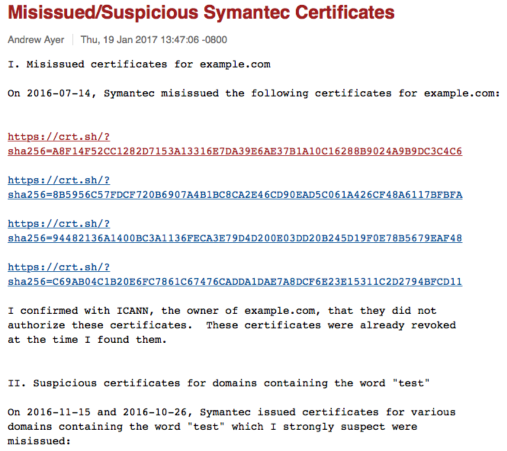
At least 108 Symantec certificates threatened the integrity of the encrypted Web.

DAN GOODIN - 1/21/2017, 8:40 AM

Enlarge

A security researcher has unearthed evidence showing that three browser-trusted certificate authorities (CAs) owned and operated by Symantec improperly issued more than 100 unvalidated transport layer security certificates. In some cases, those certificates made it possible to spoof HTTPS-protected websites.

http://arstechnica.com/security/2017/01/already-on-probation-symantec-issues-more-illegit-https-certificates/

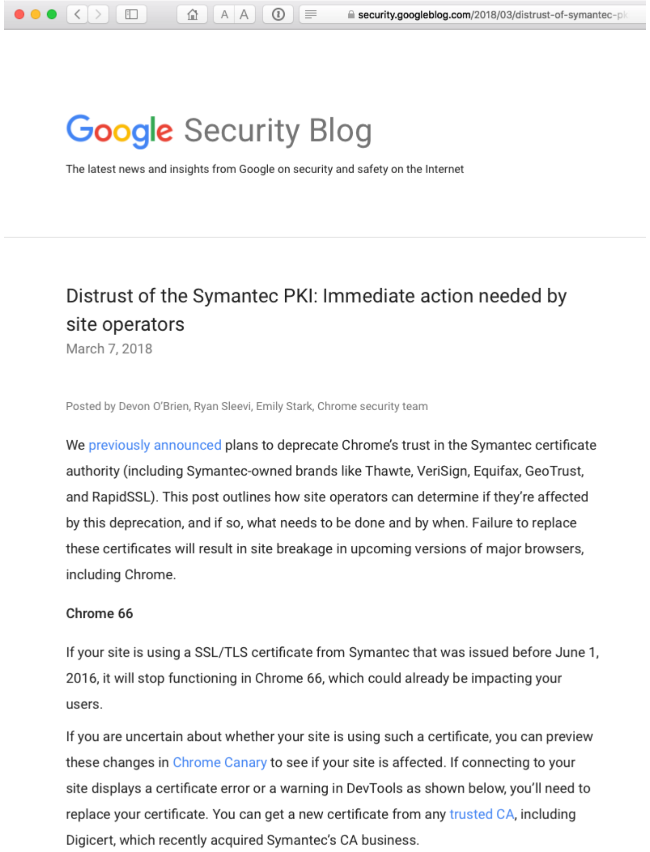


Misissued/Suspicious Symantec Certificates

Andrew Ayer | Thu, 19 Jan 2017 13:47:06 -0800

```
I. Misissued certificates for example.com

On 2016-07-14, Symantec misissued the following certificates for example.com:


https://crt.sh/?
sha256=A8F14F52CC1282D7153A13316E7DA39E6AE37B1A10C16288B9024A9B9DC3C4C6

https://crt.sh/?
sha256=8B5956C57FDCF720B6907A4B1BC8CA2E46CD90EAD5C061A426CF48A6117BFBFA

https://crt.sh/?
sha256=94482136A1400BC3A1136FECA3E79D4D200E03DD20B245D19F0E78B5679EAF48

https://crt.sh/?
sha256=C69AB04C1B20E6FC7861C67476CADDA1DAE7A8DCF6E23E15311C2D2794BFCD11

I confirmed with ICANN, the owner of example.com, that they did not
authorize these certificates.  These certificates were already revoked
at the time I found them.


II. Suspicious certificates for domains containing the word "test"

On 2016-11-15 and 2016-10-26, Symantec issued certificates for various
domains containing the word "test" which I strongly suspect were
misissued:
```

Well, hardly ever



Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Distrust of the Symantec PKI: Immediate action needed by site operators

March 7, 2018

Posted by Devon O'Brien, Ryan Sleevi, Emily Stark, Chrome security team

We previously announced plans to deprecate Chrome's trust in the Symantec certificate authority (including Symantec-owned brands like Thawte, VeriSign, Equifax, GeoTrust, and RapidSSL). This post outlines how site operators can determine if they're affected by this deprecation, and if so, what needs to be done and by when. Failure to replace these certificates will result in site breakage in upcoming versions of major browsers, including Chrome.

Chrome 66

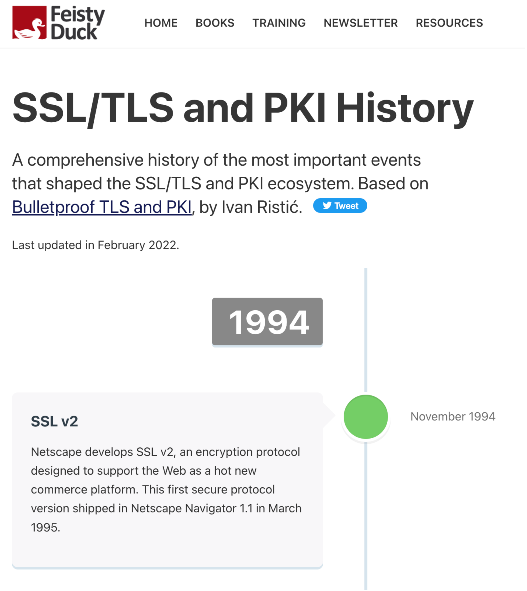
If your site is using a SSL/TLS certificate from Symantec that was issued before June 1, 2016, it will stop functioning in Chrome 66, which could already be impacting your users.

If you are uncertain about whether your site is using such a certificate, you can preview these changes in Chrome Canary to see if your site is affected. If connecting to your site displays a certificate error or a warning in DevTools as shown below, you'll need to replace your certificate. You can get a new certificate from any trusted CA, including Digicert, which recently acquired Symantec's CA business.

These are isolated events

No, they’re not:

https://www.feistyduck.com/ssl-tls-and-pki-history/



SSL/TLS and PKI History

A comprehensive history of the most important events that shaped the SSL/TLS and PKI ecosystem. Based on Bulletproof TLS and PKI, by Ivan Ristić.

Last updated in February 2022.

1994

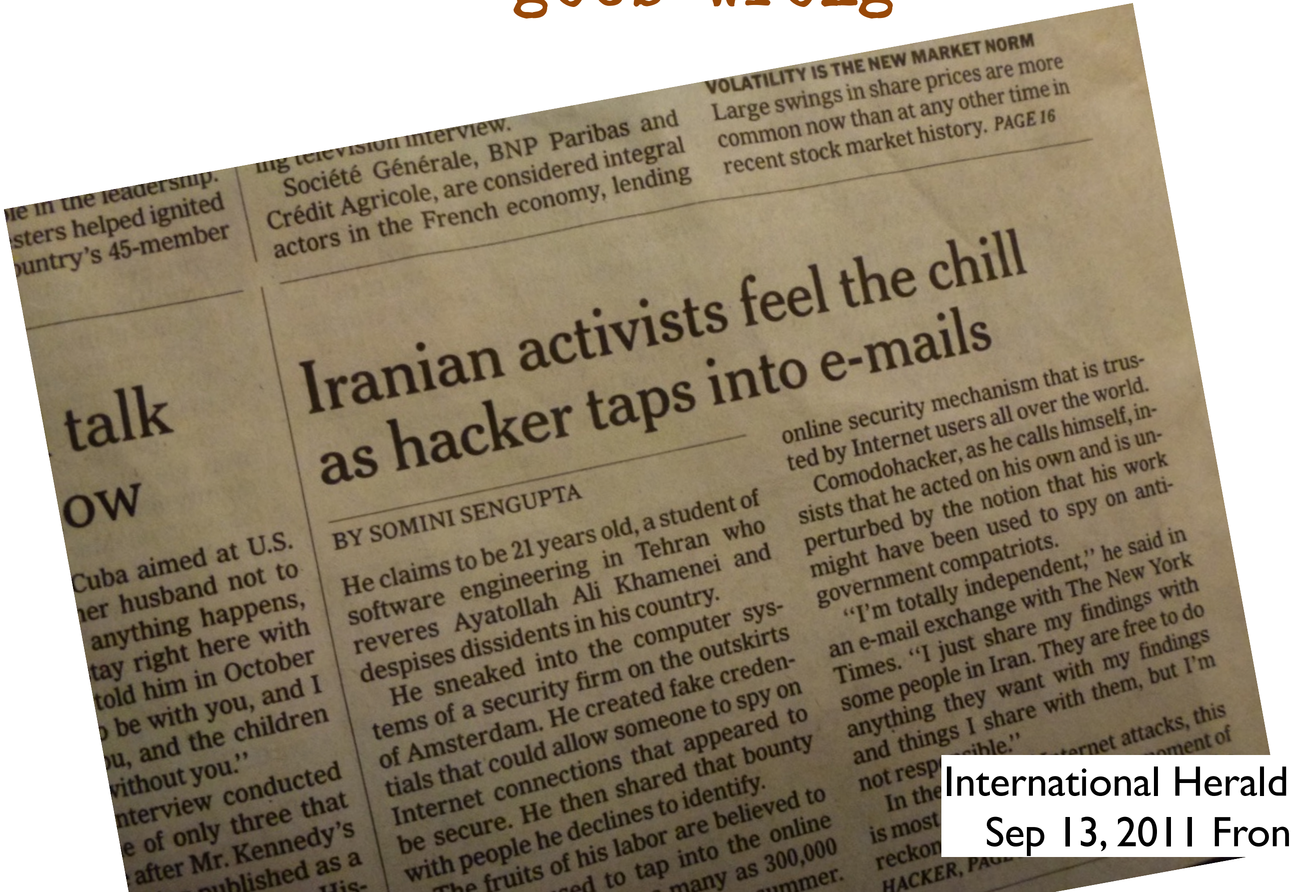
November 1994

SSL v2

Netscape develops SSL v2, an encryption protocol designed to support the Web as a hot new commerce platform. This first secure protocol version shipped in Netscape Navigator 1.1 in March 1995.

With unpleasant consequences when it all goes wrong

With unpleasant consequences when it all goes wrong



le in the leadership.
sters helped ignited
ountry's 45-member

ing television interview.
Société Générale, BNP Paribas and Crédit Agricole, are considered integral actors in the French economy, lending

VOLATILITY IS THE NEW MARKET NORM
Large swings in share prices are more common now than at any other time in recent stock market history. *PAGE 16*

talk
ow

Cuba aimed at U.S.
her husband not to
anything happens,
tay right here with
told him in October
be with you, and I
u, and the children
without you."
nterview conducted
e of only three that
after Mr. Kennedy's
published as a
His-

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 ...ed to tap into the online ... many as 300,000 ...ummer. online security mechanism that is trusted by Internet users all over the world.

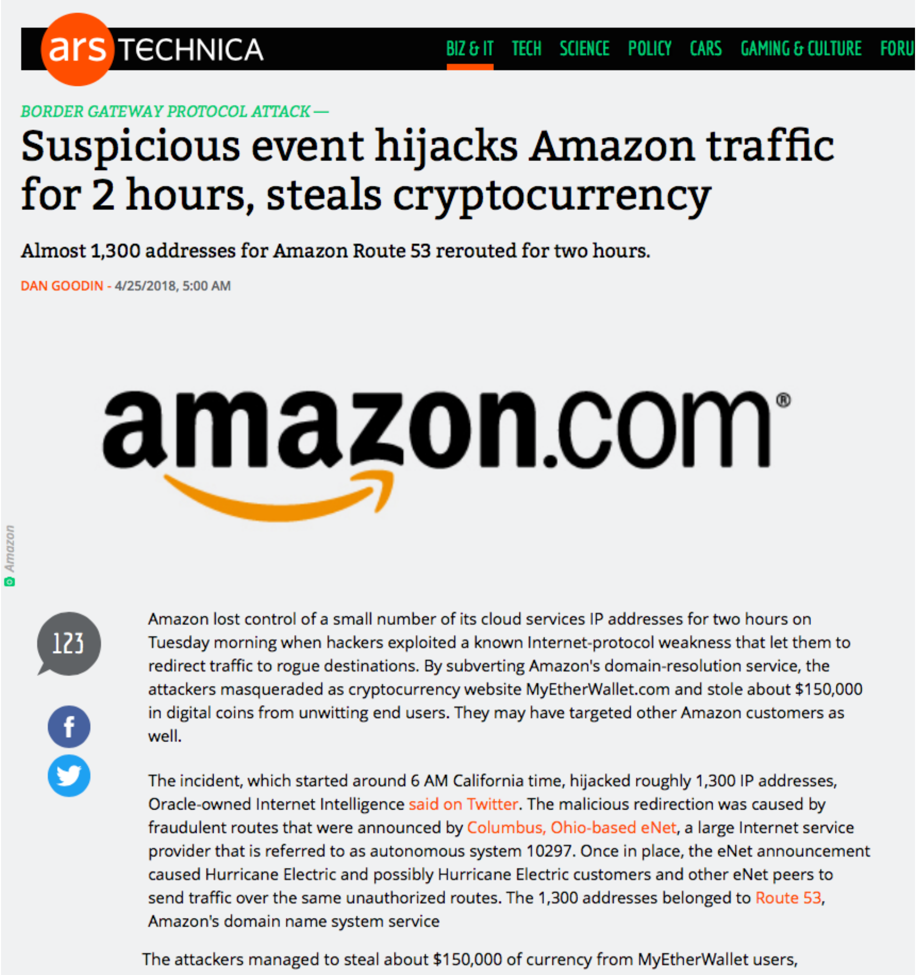
Comodohacker, as he calls himself, insists that he acted on his own and is unperturbed by the notion that his work might have been used to spy on antigovernment compatriots.

"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 resp...sible."

In the ...ternet attacks, this is most ...ment of reckon...

HACKER, PA...

International Herald Tribune
Sep 13, 2011 Front Page



BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/25/2018, 5:00 AM

Amazon lost control of a small number of its cloud services IP addresses for two hours on Tuesday morning when hackers exploited a known Internet-protocol weakness that let them to redirect traffic to rogue destinations. By subverting Amazon's domain-resolution service, the attackers masqueraded as cryptocurrency website MyEtherWallet.com and stole about $150,000 in digital coins from unwitting end users. They may have targeted other Amazon customers as well.

The incident, which started around 6 AM California time, hijacked roughly 1,300 IP addresses, Oracle-owned Internet Intelligence said on Twitter. The malicious redirection was caused by fraudulent routes that were announced by Columbus, Ohio-based eNet, a large Internet service provider that is referred to as autonomous system 10297. Once in place, the eNet announcement caused Hurricane Electric and possibly Hurricane Electric customers and other eNet peers to send traffic over the same unauthorized routes. The 1,300 addresses belonged to Route 53, Amazon's domain name system service

The attackers managed to steal about $150,000 of currency from MyEtherWallet users,

What's going wrong here?

What's going wrong here?

- There is no incentive for quality in the CA marketplace
- Why pay more for any certificate when the entire CA structure is only as strong as the weakest CA
- And your browser trusts a LOT of CAs!
  - About 60 – 100 CA's
  - About 1,500 Subordinate RA's
  - Operated by 650 different organisations

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

In a Commercial Environment

Where CA's compete with each other for market share

And quality offers no protection

Then what 'wins' in the market?

Sustainable
Resilient
Secure
Privacy
Trusted
Cheap!

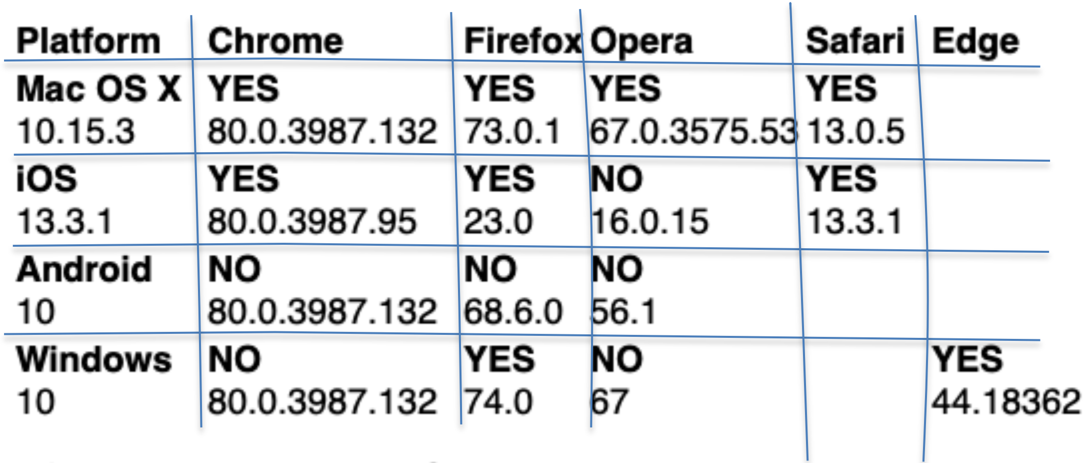
But it's all OK

Really.

- Because ‘bad’ certificates can be revoked
- And browsers **always** check revocation status of certificates before they trust them

Always?

Ok - Not Always.
Some do.
Sometimes.



Platform	Chrome	Firefox	Opera	Safari	Edge
Mac OS X 10.15.3	YES 80.0.3987.132	YES 73.0.1	YES 67.0.3575.53	YES 13.0.5	
iOS 13.3.1	YES 80.0.3987.95	YES 23.0	NO 16.0.15	YES 13.3.1	
Android 10	NO 80.0.3987.132	NO 68.6.0	NO 56.1		
Windows 10	NO 80.0.3987.132	YES 74.0	NO 67		YES 44.18362

Table 1 – Browser Revocation Status

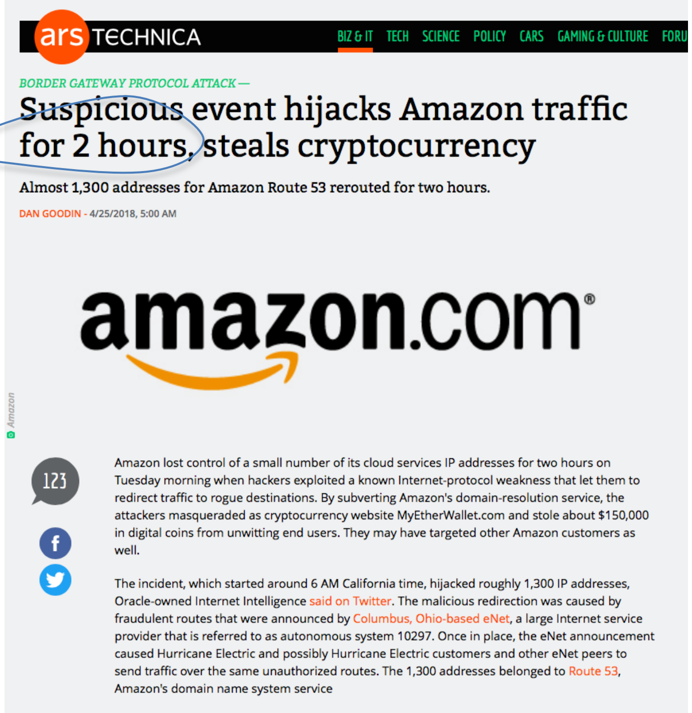
https://www.potaroo.net/ispcol/2020-03/revocation.html

So, we can't count on revocation

- If we can’t revoke certificates, then we need to reduce certificate lifetimes

So, we can't count on revocation

- If we can't revoke certificates then we need to reduce certificate lifetimes
- What's a "safe" certificate lifetime?



BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/25/2018, 5:00 AM

Amazon lost control of a small number of its cloud services IP addresses for two hours on Tuesday morning when hackers exploited a known Internet-protocol weakness that let them to redirect traffic to rogue destinations. By subverting Amazon's domain-resolution service, the attackers masqueraded as cryptocurrency website MyEtherWallet.com and stole about $150,000 in digital coins from unwitting end users. They may have targeted other Amazon customers as well.

The incident, which started around 6 AM California time, hijacked roughly 1,300 IP addresses, Oracle-owned Internet Intelligence said on Twitter. The malicious redirection was caused by fraudulent routes that were announced by Columbus, Ohio-based eNet, a large Internet service provider that is referred to as autonomous system 10297. Once in place, the eNet announcement caused Hurricane Electric and possibly Hurricane Electric customers and other eNet peers to send traffic over the same unauthorized routes. The 1,300 addresses belonged to Route 53, Amazon's domain name system service

So, we can't count on revocation

- If we can’t revoke certificates then we need to reduce certificate lifetimes
- What’s a “safe” certificate lifetime?
- If we want 2 hours or less, then we need to think hard about how to achieve this

Why is this so hard?

Why is this so hard?

We have different goals

- Some people want to provide strong hierarchical controls on the certificates and keys because it entrenches their role in providing services
- Some want to do it because it gives them a point of control to intrude into the conversations of their citizens
- Others want to exploit weaknesses in the system to leverage a competitive advantage
- Some people think users prefer faster application startup, even if faster startup admits security weaknesses
- Others think users are willing to pay a time penalty for better authentication controls

Why is this so hard?

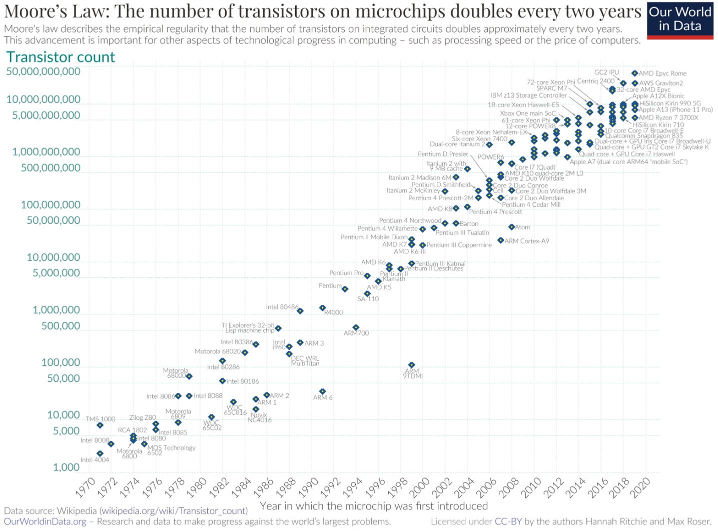
Because there are so many moving parts?

- In a system that is constructed upon the efforts of multiple systems and multiple providers we are relying on someone in charge to orchestrate the components to as working whole

Saturn V Launch Vehicle
Three stage rocket, each built by a different contractor
Each of whom used multiple subcontractors
3 million components
Each supplied by the lowest bidder!

Will it get more expensive?

- So far Moore’s Law has absorbed the incremental cost of crypto
- As we get to 3nm tracks on chips further reductions in size and unit cost are proving to be a major challenge for silicon engineers
- Which implies that robust crypto may become more expensive to use
- Who is going to pay the incremental cost of highly robust crypto?



Moore’s Law: The number of transistors on microchips doubles every two years

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.

Data source: Wikipedia (wikipedia.org/wiki/Transistor_count)

OurWorldinData.org – Research and data to make progress against the world’s largest problems.

Licensed under CC-BY by the authors Hannah Ritchie and Max Roser.

Silicon Chip transistor counts

It's a tough problem…

The Economist

The Pearl river delta: a special report

Hospitals of the future

Jacob Zuma must go

Parking, wrong on so many levels

APRIL 8TH–14TH 2017

Why computers will never be safe

Computers will never be secure. To manage the risks, look to economics rather than technology

A rather bleak prognosis from the Economist – don't look for technology to improve this rather disturbing situation!

They suggest looking at economics and markets to try and address this problem

The problem with this suggestion is that there is no natural market that provides incentive for highly robust and secure technologies. The major market incentives are based on driving down unit costs of service delivery, and security is an obvious point of avoidable cost

The Economics of Security

- Effective security for services and infrastructure is a market failure in the IT industry
- Consumers are unwilling to pay a major price premium for a highly robust service
- Service providers do not have any market-based incentive to add robust security to their products and offerings
- The reason why the public sector is undertaking investment in cyber defence measures is that the private sector is not naturally motivated to do so!

The Economics of Security

- Domain Name certificates have only taken off when the cost of obtaining them has dropped to zero, and the demonstration of proof of control is cursory
- And in a demonstration that Gresham's Law applies equally well in security, the low-quality cheap certificate product has driven out other forms of extended validation certification

Trust and Internet Fragmentation

- Trust is typically based upon the roles of mutually trusted intermediaries
- For this to work as intended, we all need to share a single context:
  - A single rooted name system without local additions or removals
  - A single coherent address system
  - Applications making consistent use of this underlying common name, address and routing infrastructure
- Fragmentation shatters this assumption, allowing ambiguity to undermine trust by altering the context of the use of a named resource across instances of the use of a network resource

Why is this so hard?

Because we are relying on the market to provide coherence and consistency of orchestration across providers?

- And perhaps that’s the key point here
- Loosely coupled fragmented systems will always present windows of vulnerability
  - Routing integrity
  - Name registration
  - Name certification
  - Service control
- Effective defence involves not only component defence but also in defending the points of interaction between components
- And we find this very hard to achieve when the market itself is the orchestration agent

Is this another of those massive challenges of our time?

We just don’t have the mechanisms to enforce outcomes across the global Internet

We can’t regulate behaviours of the platforms, their distributors, nor their operators

We can’t regulate trust!

What a dysfunctional mess we've created!

Users and Trust

- Users just want to be able to trust that the websites and services that they connect to and share their credentials, passwords and content with are truly the ones they expected to be using without first studying for a PhD in Network Operational Security
- Somehow, we’re missing that simple objective and we’ve interposed complexity and adornment that have taken on a life of their own and are in fact eroding trust
- And that’s bad!
- **If we can’t trust our communications infrastructure, then we don’t have a useful communications infrastructure.**

Questions?