SAC057 / non-FQDN Certs

Fun with TLDs...

Patrik Fältström & Warren Kumari
(RIPE DUBLIN, 2013-05)
Internal Server Names

- Designed for “internal only” type applications.
  - Often used by Microsoft Exchange, Active Directory.
- Doesn’t end in a TLD
  - can’t be used on the Internet
  - nowhere to send the validation email
Certificate request

Certificate Request:

Data:

Version: 0 (0x0)

Subject: C=US, ST=VA, L=Dulles,
O=Dulles Steel and Forge Supplies,
OU=IT - Internal WWW Site.,
CN=www.site/emailAddress=warren@kumari.net

Subject Public Key Info:

Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:da:ef:bd:d0:ee:db:...

....
Helpful...

Thanks!
Issued Certificate

Data:
Version: 3 (0x2)
Serial Number:
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=Arizona, L=Scottsdale,
O=GoDaddy.com, Inc., OU=http://certificates.godaddy.com/repository, CN=Go Daddy Secure Certification Authority/serialNumber=07969287
Validity
Not Before: Oct 2 23:56:35 2012 GMT
Not After : Oct 2 23:56:35 2013 GMT
Subject: O=www.site, OU=Domain Control Validated,
CN=www.site
X509v3 Subject Alternative Name:
DNS:www.site, DNS:site
Testing

- Setup a fake root
- Delegated .site to myself
- Setup a webservice, serving the cert
It works!

This is the default web page for this site.

The web server software is running but no content has been added, yet.

Safari is using an encrypted connection to www.site.

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

Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
www.site

www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time

Trust
Details

This certificate is valid

Hide Certificate OK
It works!

This is the default web page for this server.
The web server software is running but no content has been uploaded yet.
Investigations by SSAC

- SSAC formed a work party
- Researched prevalence of non-FQDN certs
  - Using the EFF SSL Observatory data
  - At least 157 CAs have issued such certs
  - Lower bounds estimate
- CA/B Forum is aware of the issue
  - 3 year from signing to revocation

Conclusion:
- ICANN must immediately do something
ICANN Actions

- ICANN Security Team took the lead
- “Coordinated Vulnerability Disclosure”
- Contacted CA/B Forum Chair Jan 23
- Briefed CA/B Forum Feb 5
- Ballot 96 at CA/B Forum passed Feb 26
  - 30 / 120 day period (instead of 3 years)
- SAC057 published Mar 15
  - Outreach, outreach and more outreach
Solved? Nope...

- Not all CAs are members of the CA/B Forum
  - So not bound by these agreements
  - But generally trustworthy / follow guidelines
- Revocation ineffective*
  - Blocking CRL / OSCP / air-gapped networks

* : [http://www.imperialviolet.org/2011/03/18/revocation.html](http://www.imperialviolet.org/2011/03/18/revocation.html)
Questions?