DANE: TLS Domain Name Authentication using the DNS Itself

Richard Barnes
BBN
<rlb@ipv.sx>
Security == Domain Names == PKI

• Basically all major security protocols rely on authenticating host names with certificates
  – TLS, IPsec
  – HTTPS, SIPS, SMTP/IMAPS, etc.

• EV certificates provide additional assurances, especially when user interaction is possible

• 95% of CA-issued certificates are DV
  – 35,661 EV vs. 603,481 DV [NetCraft, Jan 2011]
Scoping and Authority

• Current CA system is fundamentally unsuited for authenticating domain names
  – Anyone can vouch for anything
  – DigiNotar can vouch for Google
  – Nobody is authoritative for anything

• Patch on patch on patch
  – Pinning, CAA, Transparency, ...

PKIX

Verisign Class 3 Primary Public Certification Authority
(key: AF 24 08 08 ...)

Verisign Class 3 Extended Validation SSL SGC CA
(key: BD 56 88 BA ...)

www.nist.gov
(key: C9 83 13 87...)

Constraining the PKI

• Hierarchy with name constraints
  – CA == domain holder
• Why hasn’t this happened yet?
  – Support for name constraints
  – Economic reasons
  – Political reasons
The hierarchy you’re looking for

- **Name constraints are central to DNSSEC**
  - Keys are always scoped
- **Econ/Politics might be easier**
  - Root signed since 2010
  - Many TLD ops deploying
  - Some hosting providers
- **What goes at the end of the chain?**
- **Interaction with PKI?**
TLSA Records

• **RFC 6698**: TLS association records (TLSA)
  – TLS connects to a name
  – TLSA associates certificates to a name

• Types of association:
  – Type 0: CA constraint
  – Type 1: Certificate constraint
  – Type 2: TA assertion
  – Type 3: Certificate assertion
Type 0/1: Constraints

**TLSA Type 0: CA Constraint**

- . DNSKEY (key: ...)
- gov. DNSKEY (key: ...)
- nist.gov. DNSKEY (key: ...)
- www.nist.gov. DNSKEY (key: ...)

**PKIX**

- Verisign Class 3 Primary Public Certification Authority (key: AF 24 08 08 ...)
- Verisign Class 3 Extended Validation SSL SGC CA (key: BD 56 88 BA ...)

**TLSA Type 1: Cert Constraint**

- . DNSKEY (key: ...)
- gov. DNSKEY (key: ...)
- nist.gov. DNSKEY (key: ...)
- www.nist.gov. DNSKEY (key: ...)

_rrsig_443._tcp.www.nist.gov. TLSA
Only trust the CA with key BD 56 88 BA ...

_rrsig_443._tcp.www.nist.gov. TLSA
Only trust the cert with key C9 83 13 87 ...
Type 2/3: Assertions

**TLSA Type 2: TA Assertion**
- .DNSKEY (key: ...)
- gov. DNSKEY (key: ...)
- nist.gov. DNSKEY (key: ...)
- www.nist.gov. DNSKEY (key: ...)

_NIST CA_ (key: 62 65 D0 1B ...)

**PKIX**

Verisign Class 3 Primary Public Certification Authority (key: AF 24 08 08 ...)

Verisign Class 3 Extended Validation SSL SGC CA (key: BD 56 88 BA ...)

_NIST CA_ (key: 62 65 D0 1B ...)

**TLSA Type 3: Cert Assertion**
- .DNSKEY (key: ...)
- gov. DNSKEY (key: ...)
- nist.gov. DNSKEY (key: ...)
- www.nist.gov. DNSKEY (key: ...)

_NIST CA_ (key: 62 65 D0 1B ...)

_NIST CA_ (key: C9 83 13 87 ...)

_Hypertext:_
- Only **Trust** the CA with key 62 65 D0 1B ...
- Only **Trust** the cert with key C9 83 13 87 ...
Truth in Advertising

DANE DOES
- Provide scoping of authority
- Make CAs untrusted for domain name validation
  - Secondary check, in addition to X.509 verification
  - Mitigates misissue

DANE DOES NOT
- Attest to other identity than domain name
- Remove authority risk completely
  - CAs → DNS operators

HOWEVER
- Type 0/1 with EV
- DNS operator could probably get a cert anyway
Deployment

• Before you get DANE, you need DNSSEC
  – Parent issues
  – Resolver issues
  – Client support issues

• **Browser extensions** with DNSSEC libraries

• **DNSSEC “stapling”**: Provide all necessary DNS records in TLS handshake
Future Work

• SRV / MX: How to deal with delegation
  – My mail domain is ipv.sx
  – ipv.sx IN MX mail01.l.google.com
  – Where do I look for TLSA records?
  – What if the delegation is not secure?

• S/MIME: How to find certs for email address
  – alice@example.com
  – alice._at.example.com IN TLSA?
Summary

• Authenticating domain names is important
• X.509 is not great for domain names
  – Especially as currently deployed
• DANE uses security in the DNS to secure domain names in applications
  – Constraints + assertions
• Deployment bound on DNSSEC, but starting...
Thanks!

Richard Barnes
BBN
<rlb@ipv.sx>