Secure Sockets Layer and the SSLiverse

February 25, 2011
George Macon
Communications Systems Center
School of Electrical and Computer Engineering
SSL/TLS Overview

- SSL/TLS establishes a secure tunnel for data transfer.
- Current versions in use are SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.
- TLS 1.2 is defined in RFC 5246.
- X.509 certificates are used to authenticate the peers.
- Certificates are issued by commercial Certificate Authorities (CAs).
- The root CA certificates are included with browsers when they are published.
Certificates for TLS

- There are many CAs trusted by browsers.
- All CAs have traditionally gotten equal treatment.
- This means that a certificate can be trusted to have been validated to the least stringent requirements of all CAs.
- Domain Validation (DV)
- Organization Validation (OV)
- Individual Validation (IV)
- Extended Validation (EV)
An OV Certificate and Browser Presentation

Certificate:

Data:

Version: 3 (0x2)

Serial Number:


Signature Algorithm: sha1WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High Assurance Secure Server CA

Validity

Not Before: Dec 3 00:00:00 2009 GMT
Not After: Jan 13 23:59:59 2015 GMT

Subject: C=US/postalCode=94110, ST=California, L=San Francisco/streetAddress=454 Shotwell St, O=Electronic Frontier Foundation, OU=Comodo PremiumSSL Wildcard, CN=*.eff.org

X509v3 extensions:

X509v3 Subject Alternative Name:

DNS:*.eff.org, DNS:eff.org
Extended Validation Certificates

- EV certificates are identified by the presence of “EV Policy OIDs” in the certificatePolicy extension.
- Each CA has its own EV Policy OID.
- Browsers give special treatment to certificates with recognized EV OIDs.
The SSL Observatory

- Electronic Frontier Foundation project
- Scanned entire IPv4 space for hosts that respond on TCP port 443.
- Saved server responses for each host
- [https://www.eff.org/observatory](https://www.eff.org/observatory)
- Talk at Defcon 18: “An Observatory for the SSLiverse”
- They provided a MySQL database dump of all of the certificates.
- I wrote a new parser that uses a more normalized schema.
Certificate Encoding

- Certificates are encoded using a flavor of ASN.1 called Distinguished Encoding Rules (DER).
- Theoretically, any two systems that encode the same certificate should result with byte-identical encodings.
- The rules are not closely followed.
- For example, the uTCTime type specifies ‘YYMMDDHHMMSSZ’ as the format, but some certs use ‘YYMMDDHHMMSS+0000’ instead.
Example of ASN.1 Encoding

0:d=0  hl=4  l=1453  cons: SEQUENCE
4:d=1  hl=4  l=1173  cons: SEQUENCE
  8:d=2  hl=2  l=  3  cons: cont [ 0 ]
 10:d=3  hl=2  l=  1  prim: INTEGER           :02
13:d=2  hl=2  l= 16  prim: INTEGER           :4DD360CBCF2...
31:d=2  hl=2  l= 13  cons: SEQUENCE
33:d=3  hl=2  l=  9  prim: OBJECT     :sha1WithRSAEncryption
44:d=3  hl=2  l=  0  prim: NULL
46:d=2  hl=3  l= 137  cons: SEQUENCE
49:d=3  hl=2  l=  1  cons: SET
51:d=4  hl=2  l=  9  cons: SEQUENCE
53:d=5  hl=2  l=  3  prim: OBJECT            :countryName
58:d=5  hl=2  l=  2  prim: PRINTABLESTRING   :GB
Public Key Algorithms

- RSA: 99.9%
- Other: 0.1%
RSA Modulus Size

Certificates by RSA Modulus Length

Number of Certificates

RSA Modulus Length (bits)
Improper Certificates

- RFC 1918 IP Addresses: 339
- Unqualified Host Names: 28207
- Local Host Names: 34683
Improve EV Certificates

- 28 EV Certificates with RFC 1918 IP addresses or local or unqualified host names
- 178 Certificates with RSA keys shorter than 2048 bits but expire after December 31, 2010
Utility

- Accountability
- Accountability
- Accountability