Symantec's View of the Current State of ECDSA on the Web

Rick Andrews

Senior Technical Director and Distinguished Engineer

Agenda

1	Curves used in current practice
2	Market Penetration
3	Why customers use ECDSA
4	Why customers don’t use ECDSA
5	Impact of new ECC curves

Copyright © 2015 Symantec Corporation

Curves in Current Practice for Web-based TLS

- NSA published Suite B; adopted by NIST
  - https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml
- Only NIST-recommended curves have been used in practice for SSL/TLS certificates
  - IETF published “ECC Cipher Suites for TLS”
    - http://www.ietf.org/rfc/rfc4492.txt
    - Defined Supported Elliptic Curves Extension
  - IETF published “Suite B Certificate and Certificate Revocation List (CRL) Profile”
    - http://tools.ietf.org/html/rfc5759
  - IETF published “Suite B Profile for TLS”
    - http://tools.ietf.org/html/rfc6460
    - Restricts TLS to use P-256, P-384 (not P-521)
- Most roots in browsers’ trust stores are P-384

Copyright © 2015 Symantec Corporation

Browser/OS Support for ECDSA and Roots

- Mozilla Firefox browser (since 3.6.28, NSS 3.11) trusts 11 ECC roots (10 P-384, 1 P-256)
  - https://wiki.mozilla.org/CA:IncludedCAs
  - https://bugzilla.mozilla.org/show_bug.cgi?id=195135
  - Platform independent
- Safari browser depends on platform - Mac OS X (since 10.9.1) and iOS (since 7) trust 13 ECC roots (12 P-384, 1 P-256)
  - http://support.apple.com/kb/HT6005
  - http://support.apple.com/kb/HT5012
- IE (since Vista) / Windows Phone 8 trusts 14 ECC roots (13 P-384, 1 P-256)
  - http://social.technet.microsoft.com/wiki/contents/articles/14215.windows-and-windows-phone-8-ssl-root-certificate-program-member-cas.aspx

Copyright © 2015 Symantec Corporation

Browser/OS Support for ECDSA and Roots

- Android (since 3.x) trusts 6 ECC roots
  - https://bluebox.com/blog/technical/questioning-the-chain-of-trust-investigations-into-the-root-certificates-on-mobile-devices/
- Desktop Chrome and Opera (Chromium) use platform crypto and trusted root store
  - Except on Linux, where the browser includes Mozilla's NSS trust store.
- Blackberry (since 5.0)

Copyright © 2015 Symantec Corporation

Curves Supported in Mozilla NSS

NIST_P192	X9_62_PRIME_192V2	X9_62_CHAR2_TNB239V2	SECG_PRIME_192K1
NIST_P224	X9_62_PRIME_192V3	X9_62_CHAR2_TNB239V3	SECG_PRIME_224K1
NIST_P256	X9_62_PRIME_239V1	X9_62_CHAR2_PNB272W1	SECG_PRIME_256K1
NIST_P384	X9_62_PRIME_239V2	X9_62_CHAR2_PNB304W1	SECG_CHAR2_113R1
NIST_P521	X9_62_PRIME_239V3	X9_62_CHAR2_TNB359V1	SECG_CHAR2_113R2
NIST_K163	X9_62_CHAR2_PNB163V1	X9_62_CHAR2_PNB368W1	SECG_CHAR2_131R1
NIST_B163	X9_62_CHAR2_PNB163V2	X9_62_CHAR2_TNB431R1	SECG_CHAR2_131R2
NIST_K233	X9_62_CHAR2_PNB163V3	SECG_PRIME_112R1	SECG_CHAR2_163R1
NIST_B233	X9_62_CHAR2_PNB176V1	SECG_PRIME_112R2	SECG_CHAR2_193R1
NIST_K283	X9_62_CHAR2_TNB191V1	SECG_PRIME_128R1	SECG_CHAR2_193R2
NIST_B283	X9_62_CHAR2_TNB191V2	SECG_PRIME_128R2	SECG_CHAR2_239K1
NIST_K409	X9_62_CHAR2_TNB191V3	SECG_PRIME_160K1	WTLS_1
NIST_B409	X9_62_CHAR2_PNB208W1	SECG_PRIME_160R1	WTLS_8
NIST_K571	X9_62_CHAR2_TNB239V1	SECG_PRIME_160R2	WTLS_9
NIST_B571			

http://bonsai.mozilla.org/cvsblame.cgi?file=mozilla/security/nss/lib/freebl/ecl/ecl-curve.h&rev=1.7&root=/cvsroot

Unclear if each curve can be used for ECDSA and/or ECDH(E)

Copyright © 2015 Symantec Corporation

Curves Supported in Web Server Software

- Microsoft Windows Server 2008; partial support
  - Can’t generate ECC CSR but can work with imported key and certificate
  - https://msdn.microsoft.com/en-us/library/windows/desktop/bb204775%28v=vs.85%29.aspx
- Apache, nginx with latest OpenSSL
- Oracle JRE/JDK 1.7 or newer
- F5 11.5 or newer
- IBM z/OS V1R13 or newer
- CloudFlare (CDN) supports ECC

Copyright © 2015 Symantec Corporation

Curves Supported in Other Web Software

- OpenSSL (since 1.0)
  - P-224 P-256 P-384 P-521
  - B-233 B-283 B-409 B-571
  - K-233 K-283 K-409 K-571
  - http://csrc.nist.gov/groups/STM/cavp/documents/dss/ecdsahistoricalval.html
- Boring SSL (used in Google Chrome) supports P-224, P-256, P-384, P-521
  - https://boringssl.googlesource.com/boringssl/+/master/crypto/ec/ec.c
- GnuTLS supports P-192, P-224, P-256, P-384 and P-521
  - http://gnutls.org/manual/gnutls.html

Copyright © 2015 Symantec Corporation

Curves Supported in Other Web Software

- Java JCE Providers (since Java 6) must support
  - sect163k1, sect163r1, sect163r2, sect193r1, sect193r2, sect233k1, sect233r1, sect239k1, sect283k1, sect283r1, sect409k1, sect409r1, sect571k1, sect571r1
  - secp160k1, secp160r1, secp160r2, secp192k1, secp192r1, secp224k1, secp224r1, secp256k1, secp256r1, secp384r1, secp521r1
  - From http://docs.oracle.com/javase/7/docs/technotes/guides/security/SunProviders.html and http://www.ietf.org/rfc/rfc4492.txt
- BouncyCastle (since 1.32) supports SEC/NIST curves
  - http://www.bouncycastle.org/releasenotes.html
- Mac OS X and iOS support P-192, P-224, P-256, P-384, P-521
  - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2021.pdf

Copyright © 2015 Symantec Corporation

Certification Authorities that offer ECDSA certs

- Symantec (includes VeriSign/GeoTrust/Thawte roots)
- GlobalSign
- Entrust
- DigiCert
- Comodo (includes USERTrust roots)
- Trend Micro (includes AffirmTrust roots)

- These CAs issue 67% of the world's public SSL certificates, according to Netcraft

Copyright © 2015 Symantec Corporation

Market Penetration

- Rough estimates of the number of deployed ECDSA SSL certificates:
  - Netcraft's scans show 1.96% of all public SSL certificates are ECDSA
    - Data available by subscription only
  - ICSI Certificate Notary says that 2.1% of the certificates it sees are ECDSA
    - http://notary.icsi.berkeley.edu
  - Majority of ECDSA certs are hosted by CloudFlare as part of their Universal SSL initiative
    - https://blog.cloudflare.com/introducing-universal-ssl/
  - Most Symantec ECDSA customers are from the US, but interest is broadly distributed around the world (Europe, Africa, Middle East, Australia, Asia)
- We see some demand in non-Web (device) IoT market

Copyright © 2015 Symantec Corporation

Why Customers Choose ECDSA Certificates

- Forward-thinking – want to experiment with alternatives to RSA
- Symantec's performance analysis showed significant server performance gains for P-256 over RSA 2048
  - https://www.symantec.com/page.jsp?id=elliptic-curve-cryptography
- Research demonstrated significant performance advantage of ECDSA/ECDHE over RSA/DH (PFS for free)
  - http://w2spconf.com/2014/papers/TLS.pdf

Copyright © 2015 Symantec Corporation

What is holding back the market for ECDSA certs?

- Legal/IP concerns were not allayed by the 2003 NSA-Certicom license
- Distrust in Suite B curve choices after Snowden, especially in Europe
- Lack of client support (Windows XP and non-traditional devices like smart TVs and Japanese feature phones)
- RSA isn't broken; risk of trying new algorithm; general lack of awareness
- Lack of dual-stack support in web servers (except Apache – see http://httpd.apache.org/docs/2.4/mod/mod_ssl.html#comment_970)
- Clients supporting ECDHE may not have ECDSA root; difficult for servers to know
- ECDSA root may not be EV-enabled
- Client-side performance penalty (ECDSA slower than RSA for signature verification for commonly-used key sizes)
- "Heard there was some technical problem with ECDSA" – (if a cryptographically secure random integer is not selected, the private key can be determined)

Copyright © 2015 Symantec Corporation

Impact of New Curves

- Impact will likely be muted if IP issues are not cleared up
- CAs need support in their HSMs and software toolkits
- CAs will most likely sign keys from new curves using existing P-256 or P-384 roots, to avoid delay of deploying roots using new curves
  - Signing with existing RSA roots or intermediates carries IP risk, but mitigates root ubiquity issue
- Even though CAs may not initially create intermediate CA certs with new curves, we need to perform Proof of Possession of key. Usually done by checking signature on CSR, requiring support of new key curve in the CA's HSMs and software toolkits.
- Browser and web server vendors must support new curves

Copyright © 2015 Symantec Corporation

Thank you!

Rick Andrews

rick_andrews@symantec.com
650-527-9506

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.