

Securing the Next Generation Internet

Sheueling Chang, Hans Eberle, Vipul Gupta, Nils Gura, *Sun Microsystems Laboratories*
 {sheueling.chang, hans.eberle, vipul.gupta, nils.gura}@sun.com

<http://research.sun.com/projects/crypto>

1. Introduction

The Internet today is ...

- a global marketplace for goods and services
- enabled by security mechanisms that ensure *authentication, confidentiality and integrity*
- predominantly secured by the SSL protocol using a combination of *symmetric*- and *public-key* cryptography

but ...

- many new devices connecting to the Internet have limited capabilities (e.g. sensors, appliances)
- new applications (e.g. patient monitoring, building automation) will increase the number of transactions requiring security
- the future will demand higher levels of security (e.g. 128-bit AES, 2048-bit RSA)

The next generation Internet will need stronger, more efficient cryptography.

2. Elliptic Curve Cryptography (ECC)

- Public-key cryptosystem offering the highest security strength per bit. Uses smaller keys for equivalent security.
- Results in faster computations and savings in memory, power and bandwidth (especially important in constrained environments).
- Performance advantage increases as security needs increase over time
- Endorsed/standardized by NIST, ANSI, IEEE, IETF.

Sym-metric	RSA/DH/DSA	ECC	Size	MIPS Yrs to attack	Protection Lifetime
80	1,024	160	6:1	10 ¹²	Until 2010
112	2,048	224	9:1	10 ²⁴	Until 2030
128	3,072	256	12:1	10 ²⁸	Beyond 2030
192	7,680	384	20:1	10 ⁴⁷	
256	15,360	521	30:1	10 ⁶⁶	

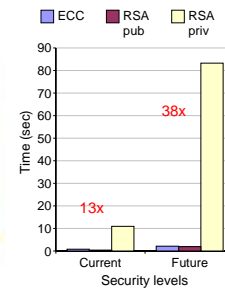
3. ECC on Small Devices

Algorithm	Time* (s)	Data bytes	Code bytes
ECC secp160r1	0.81	282	3682
ECC secp224r1	2.19	422	4812
RSA 1024 (pub**)	0.43	542	1073
RSA 1024 (priv)	10.99	930	6292
RSA-2048 (pub**)	1.94	1332	2854
RSA-2048 (priv)	83.26	1852	7736

*8MHz Atmel Atmega ** e-65537

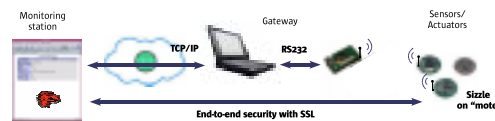


Berkeley/Crossbow "mote"
 (8-bit, 4MHz Atmel ATmega 128 processor, 128KB FLASH, 4KB SRAM, 4KB EEPROM)



Large keys are a big problem for small devices

4. Sizzle (Slim SSL): Standards-based security for the "embedded" Internet

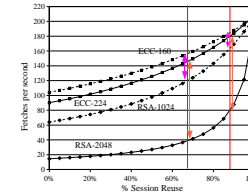


- Sizzle: Small HTTPS stack for embedded systems
- Smallest known secure web server: 2.9KB RAM, 65KB Flash, ~5s full handshake

By using ECC, Sizzle lowers the barrier for connecting interesting new devices to the Internet without sacrificing security

5. ECC in Secure Web Transactions

Apache SSL benchmark*:
 ECC server achieves **higher secure transaction rate**
 current key sizes: **1.1-1.3x**
 future key sizes: **2.2-3.8x**



*Apache 2 with OpenSSL, 900MHz UltraSPARC III CPU, 30KB file size, 66%-87.5% session reuse



6. Summary

- Elliptic Curve Cryptography (ECC) brings the powerful advantages of public-key cryptosystems to constrained environments where traditional mechanisms (e.g. RSA) are simply impractical.
- There are significant performance benefits to using ECC in secure web transactions.
- We have contributed this technology to OpenSSL, Apache, Mozilla and other components of the Internet's security infrastructure with the aim of jumpstarting its widespread adoption.

