

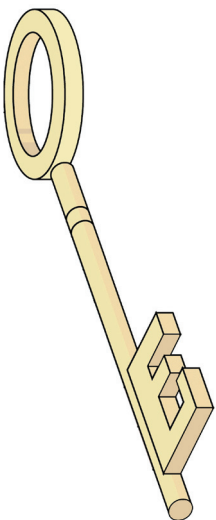
Elliptic Curve Cryptography: The Next Generation of Internet Security



Commercial transactions conducted over the Internet, known as e-commerce, play an important role in the global economy, and their importance is increasing every year. The Census Bureau of the US Department of Commerce estimates that in the United States alone, retail e-commerce sales for the second quarter of 2003 amounted to more than \$12 billion, an increase of almost 28% from the second quarter of 2002.

E-commerce would be impossible without protocols to ensure the privacy and security of online transactions. The Secure Sockets Layer (SSL) protocol is by far the dominant protocol for handling secure transactions over the Internet. SSL supports secure transactions at the Web servers that host e-commerce transactions (that is, on the *server side*) as well as in the Web browsers, applications, and appliances that access those servers (that is, on the *client side*).

The use of SSL unfortunately imposes a significant performance penalty on Web servers. Various studies have reported secure Web servers running three to nine times slower compared to regular Web servers on the same hardware platform. Slow response time is a major cause of frustration for online shoppers and often leads them to abandon their electronic shopping carts during checkout. According to Zona research, the potential revenue loss from e-commerce transactions aborted due to Web performance issues exceeds several billion dollars worldwide.



Until now, service providers have managed to cope with the high cost of providing secure connections by adding more and more powerful hardware, and by limiting, for example, secure connections to logins and to financial transactions. But the following trends will make it even more important to be able to process secure transactions efficiently:

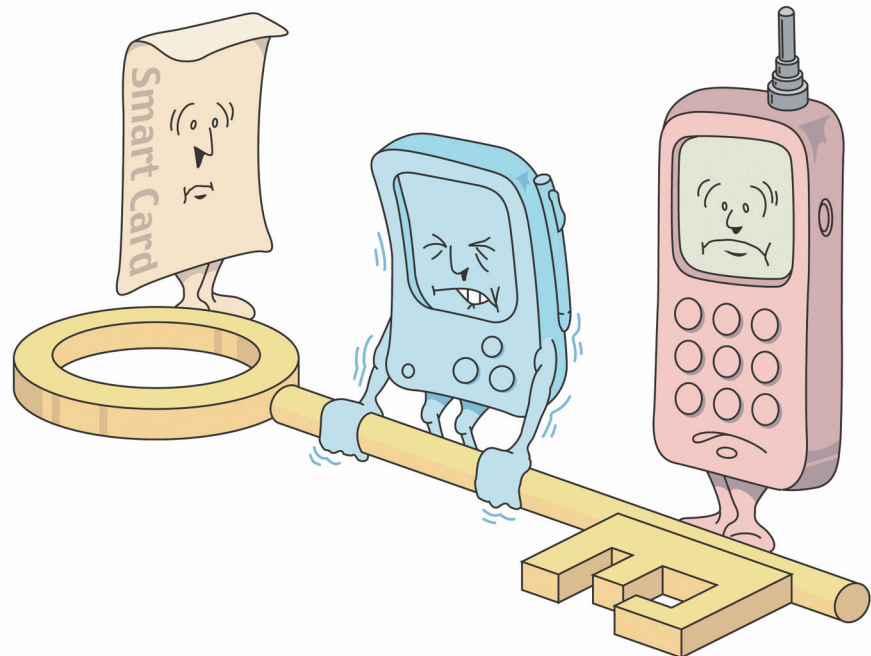
- **More and smaller connected devices:** PDAs, cell phones, and newer devices – home appliances, scientific instruments, onboard automotive computers, smart cards, and even medical devices such as pacemakers – are using networking technology to facilitate data collection and remote control functions. Many of these devices require secure connections to ensure that the information they provide remains confidential, and that only those authorized to control these devices can do so. The volume of secure connections these devices will demand is only part of the story. Many of these devices are much smaller than traditional computers, and their limited computational resources – power and memory – are insufficient to provide adequate levels of security using the cryptographic technology available in current implementations of SSL.

- **Transaction volume:** The volume of online commercial transactions is projected to double every few years, driving up the number of costly secure connections and increasing the load on enterprise servers.

- **Need for more privacy:** Consumers are starting to express the desire for more privacy in all of their online activities. Many people feel that protecting credit card information from electronic eavesdroppers is not enough – that their browsing habits, the books they order, and perhaps most important their email, should be nobody's business but their own. Offering secure connections to Web surfers to ensure their browsing and communications privacy would, of course, dramatically

can increase the security level of their SSL connection by increasing the size of keys used for encryption in SSL. Currently 1024-bit RSA keys are standard, but it is expected that this size will increase to 2048 bits by the end of the decade. Such a large key size puts a severe load on both clients and servers, and the problem is particularly acute for small, networked devices that do not have the capacity to handle such large key sizes.

For these reasons, a team of



Very Large Keys are a Problem for Very Small Devices

increase the server-side cost of supporting the increased processing load.

- **Demand for increased security:** The performance of personal computers doubles every two years. Increasing CPU speeds, the ability to network, and the sheer increase in the number of computers worldwide has given potential attackers more resources than ever before. Online merchants

scientists and engineers at Sun Microsystems Laboratories has been working with standards bodies to develop and integrate a more efficient cryptographic technology into the SSL protocol.

Public-Key Cryptography in SSL

SSL provides a simple and elegant mechanism for two parties, without prior knowledge of one another, to establish a secure connection over an

open and public network such as the Internet. The secure connection protects the confidentiality of the information in transit. In addition, SSL contains options for verifying the identity of each party and ensuring that the information is not modified in transit.

The SSL protocol uses two kinds of cryptographic tools for these security services: symmetric-key cryptography and public-key cryptography. The remainder of this discussion focuses on public-key technology since it is the main bottleneck in SSL processing.

RSA is the main public-key technology used with SSL today but Elliptic Curve Cryptography (ECC) is emerging as an attractive alternative. ECC was invented in 1985 by Victor Miller and Neal Koblitz and has evolved into a mature public-key technology. For example, the National Institute of Standards and Technology (NIST) recently approved ECC for use by the U.S. Government. Several standards organizations, including IEEE, ANSI, OMA (Open Mobile Alliance) and the IETF (Internet Engineering Task Force), have ongoing efforts to include ECC as a required or recommended security mechanism.

At the foundation of every public-key technology is a hard mathematical problem that is computationally intractable. The relative difficulty of solving that problem determines the security strength of the corresponding technology.

Since the fastest known algorithms to attack ECC run more slowly than the fastest known algorithms to attack RSA, ECC can offer equivalent security with substantially smaller keys and much higher performance.

For example, a 160-bit ECC key provides the same level of security as a 1024-bit RSA key at 4 times the RSA performance and a 224-bit ECC key provides the security equivalent to a 2048-bit RSA key at 14 times the RSA performance on large servers with 64-bit processors. For small 8-bit processors, ECC even offers a performance advantage of up to two orders of magnitude. Smaller keys result in faster computations, lower power consumption, and memory and bandwidth savings. These characteristics make ECC especially appealing for small client devices as well as alleviating the computational burden on secure Web servers.

How Has Sun Helped to Promote the Adoption of ECC?

The Next Generation Cryptography project at Sun Laboratories is investigating cryptographic technologies for the next generation of Internet security. This team is staffed by engineers Hans Eberle, Vipul Gupta and Nils Gura, and led by Sheueling Chang Shantz, Sun's first woman distinguished engineer.

Introducing any new technology in a networked environment is a challenging task. It requires both servers and client devices to adopt the technology so that both sides can successfully communicate. For this reason, the group at Sun Labs is placing a great deal of emphasis on seeding industry adoption of ECC. It is doing so by promoting standardization of ECC in the SSL protocol and contributing ECC code to the two most popular open source security libraries. To date, the team's efforts include:

- Contribution of ECC technology to OpenSSL. This allows the Apache Web servers, which has a 60% market share, to communicate securely and efficiently with light-weight devices using ECC technology.
- Addition of ECC support to Netscape Security Services (NSS), which powers the Mozilla/Netscape browsers and the Sun™ ONE Web, directory, and messaging servers.
- Ongoing work with standards bodies and co-authoring the IETF Internet-draft to specify the use of ECC technology in the SSL protocol.

Sun's Open Source contributions include a full-strength, general purpose ECC library which is highly modular and usable for other protocols besides SSL. This cross-platform code is available under a liberal Open Source license which allows free use for commercial and non-commercial purposes; thus affording the developers and small device vendors the opportunity to incorporate this next generation cryptographic technology into innovative new security-enabled products. Sun is seeding the adoption of key technologies critical to the security needs of the wireless mobile industry, and the coming wave of small devices reachable over the Internet.

More information and links to the latest version of the OpenSSL and Mozilla/NSS code containing ECC technology can be found on the Sun Labs Next Generation Crypto Project website at <http://research.sun.com/projects/crypto>.

*Since its inception in 1982, a singular vision
- The Network is The Computer -
has propelled Sun Microsystems, Inc. (Nasdaq: SUNW)
to its position as a leading provider of industrial-strength
hardware, software, and services that make the Net work.*

*Sun can be found in more than 100 countries
and on the world wide Web.*

Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA Phone 800 786-7638 or +1 512 434-1577 Web sun.com



Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India-Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-597-8111, Ireland +353-1-9055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-465774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand-Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China-Beijing +86-10-6803-5588; Chengdu +86-28-619-9333; Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland-German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800

SUN™ THE NETWORK IS THE COMPUTER © 2002 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Sun Enterprise and Java are trademarks, registered trademarks or service marks of Sun Microsystems, Inc. in the United States and other countries. Printed in USA 0/00 000-0000-00 INS, Success Story, xx0000-0