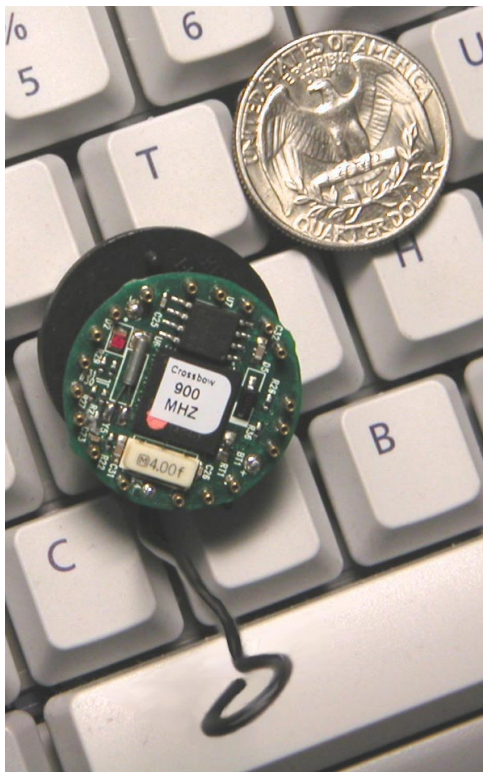


Extending Internet Connectivity to Smart Dust



Researchers at Sun Microsystems Laboratories have created the world's smallest secure web server. This coin-sized server, nicknamed “Sizzle” (for Slim SSL), can be embedded in a wide array of lightweight devices, including home appliances, utility meters, personal medical devices, and industrial sensors for secure monitoring and control across the Internet.



The tiny Sizzle Web server is the size of a coin

Sizzle runs on the Berkeley/Crossbow “motes” — battery-powered, wireless devices equipped with an 8-bit microprocessor, 128KB of FLASH and a mere 4KB of RAM. Although small Web servers have been built before, Sizzle is the first to demonstrate the feasibility of true end-to-end secure communication with such constrained resources.

Sizzle implements the Internet's dominant security protocol, SSL, used to protect sensitive transactions like e-commerce, stock trading and on-line banking. In spite of its small size, Sizzle makes no compromises in security. It uses Elliptic Curve Cryptography (ECC), the next generation public-key technology chosen by the National Security Agency to protect sensitive US Government information. Compared to RSA, the conventional public-key technology used on the Internet today, ECC provides comparable security while using fewer resources. For example, an RSA operation on the mote takes up to 11 seconds while the equivalent ECC operation can be accomplished in under one second. The ECC performance advantage increases to nearly a factor of 40 at the higher key sizes needed by 2010.

By using open standards, Sizzle allows emerging networked devices such as wireless sensors to be connected to the Internet in a seamless fashion with cross-industry multi-vendor interoperability. This Sun Labs technology provides an easy-to-use, highly secure and efficient wireless networking solution for linking factories, manufacturing plants, supply chains, and field operations to a central database.

Wireless Sensors: The Next Wave of the Internet

The evolution of computers from mainframes to laptops was accompanied, and in large part driven, by the continuous trend toward smaller, more powerful, and less expensive computer hardware components. As microprocessors became cheaper and smaller, business and private consumers responded by purchasing millions of them. In recent years, a single development — the introduction of network-enabled cell phones — was responsible for doubling, between 2001 and 2003, the number of devices with access to the World Wide Web.

As impressive as this trend has been to date, the next few years will witness an even more dramatic increase in the number of web-enabled devices. Today more than 3 billion devices have Web access, and that number is expected to grow to 14 billion within the next five years driven primarily by the proliferation of wireless sensors

with ubiquitous Internet connections. These coin-sized devices, with a miniature radio antenna on chip, can gather data by measuring temperature, vibration, or light intensity, and pass along its readings to a hub, where the information is aggregated and sent to a centralized computer for analysis and control decision making.

Industrial, agricultural, environmental, security, and military users are just beginning to recognize how wireless sensor networks can revolutionize their operations. As these devices become available at commodity prices, staggering numbers of wireless sensors will start turning up everywhere imaginable. Some examples of sensor network applications follow.

- **Industrial Applications**—In manufacturing systems, hundreds of tiny wireless sensors remotely monitor temperature, stress, vibration, and other variables on or near failure points, alerting technicians before failures occur and saving costly downtime.
- **Homeland Security Applications** —In shipping containers, wireless sensors alert customs and security officials if a container was opened in transit. At the same time, they perform inventory-control functions such as identifying each item in the shipment and recording the high and low temperatures and humidity levels over the course of the delivery.
- **Military Applications**—Wireless sensors allow technicians to track and locate service vehicles, weapons, munitions, and supplies anywhere in the system. Wireless sensors embedded in equipment and supplies alert personnel when equipment has been exposed to out-of-tolerance environmental conditions or has missed scheduled maintenance, reducing the chance of equipment failure in the field. Wireless sensors scattered from planes or specialized munitions sense motion, vibration, temperature, or magnetic flux to locate enemy combatants on the battlefield. Other sensors help locate the source of incoming small arms fire so that counterattacks can be launched against snipers quickly and precisely.
- **Health care Applications**—In pharmaceutical applications, smart tags track shipments and ensure that counterfeit drugs cannot enter the supply chain. In medical applications, implanted or wearable devices gather patient biometrics for remote medical professionals, and allow medical professionals to adjust their patients' treatment parameters remotely.
- **Agricultural Applications**—Wireless sensors placed in farmland monitor moisture levels so that irrigation can be provided selectively to the areas that need it. These sensors can also monitor soil chemistry, sunlight exposure, and other factors to help farmers improve the yield of their crops. Used in conjunction with electronically actuated gates, farm animals can be automatically identified and collected to receive inoculations or other attention as needed, based on information on each animal stored in a database.
- **Environmental Applications**—Wireless sensors placed on and below the soil and in trees collect very detailed data about the fluctuations in temperature and humidity in different parts of the same ecosystem, to help researchers understand that factors that determine how different species of plants and animals proliferate. Wireless sensors attached to animals track their movements; placed throughout the habitat, they sense the presence of the animals and record information about their habits.

In addition, researchers have designed specialized audio sensors with enough computational capacity to recognize the song patterns of specific bird species or to transmit streaming video of the animal subjects through the wireless network. Wireless sensors monitor temperature and humidity throughout the building, detect motion or body temperature to switch on lights and heat in occupied areas, evaluate sunlight intensity to open and close shades as an aid to energy conservation, and so forth.

These examples, of course, represent only the tip of the iceberg.

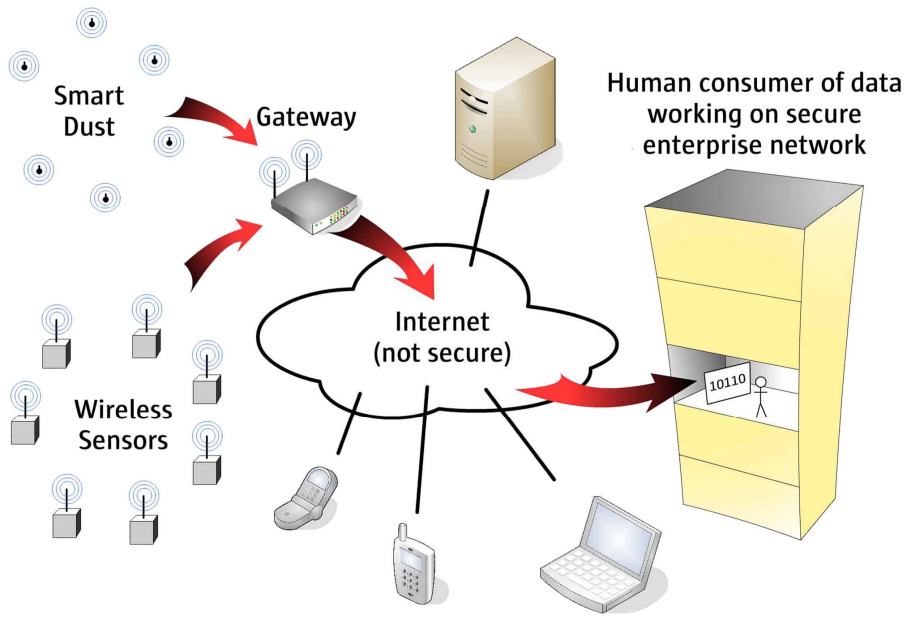
Providing Internet Security for Wireless Sensors

As is the case whenever data is involved, security issues such as privacy, data integrity, authentication, and non-repudiation apply to sensor networks as well as conventional networks. The focus of the work at Sun Labs is on providing “security” for small, inexpensive, resource-constrained devices that offer the greatest opportunities for mass deployment.

The smallest of these devices, often referred to as *smart dust*, have the following characteristics:

- Small and inexpensive (typically 8-bit) microprocessors
- Wireless communications capability
- Extremely low battery power consumption and very limited memory
- Often deployed in remote unsecured locations

The limitations on processing power and memory make complex data processing tasks on these devices difficult and time-consuming. The limitations on electrical power consumption place a high premium on efficiency and economy.



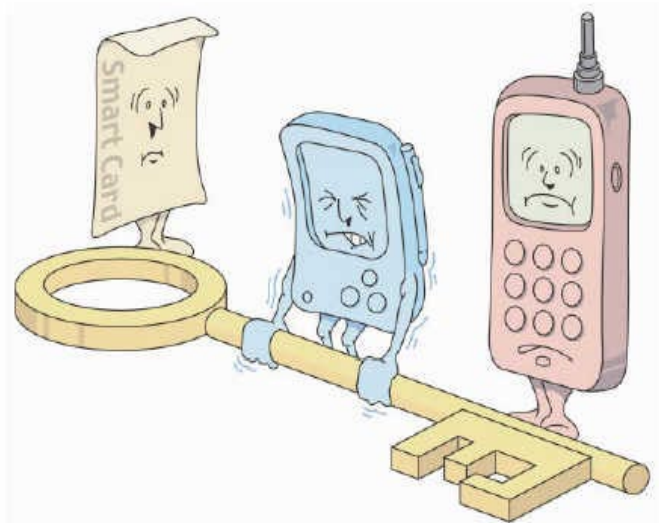
The integration of wireless sensors (as shown on the left) into a larger enterprise network — which already exists in specialized applications today — will become pervasive in the coming years. In order for such data gathering to occur over wireless networks without compromising the integrity of the data, we need end-to-end security.

Extending the Internet to wireless sensors and smart dust

Secure Sockets Layer (SSL) is the most popular security protocol on the Internet today and is a perfect foundation for wireless sensor networks to interoperate in a seamless way with the existing World Wide Web infrastructure and popular Web browsers and servers. SSL combines public-key cryptography for key-distribution/authentication with symmetric-key cryptography for data encryption and integrity.

However, the RSA cryptographic technology used in SSL today requires power and memory resources that many tiny devices simply haven't got. Specifically, the problem is the size of the keys used for encryption in SSL. Currently 1024-bit RSA keys are standard, and this size is expected to 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 tiny devices with small, inexpensive (typically 8-bit) processors, battery-powered operation, and very limited memory.

At Sun Labs, the Next Generation Cryptography Team has been working with standards bodies to develop and integrate a more efficient technology called Elliptic Curve Cryptography (ECC) into the SSL protocol. Invented in 1985 by Victor Miller and Neal Koblitz, ECC has evolved into a mature public-key technology. It offers the same security as RSA, but with substantially smaller key sizes. For example, a 160-bit ECC key provides the same level of security as a 1024-bit RSA key, and a 224-bit ECC key provides the same security as a 2048-bit RSA key. Smaller keys mean faster computation, lower power consumption, and memory and bandwidth savings. For example, on the 8-bit Atmel ATmega128 processor used in many wireless sensor networks, ECC is 13 times faster at the RSA 1024 security level and 38 times faster at the RSA 2048 level.



Large keys are a big problem for small devices.

Sizzle: World's Smallest Secure Web Server

Sun Labs has used Elliptic Curve technology to create the world's smallest secure web server, delivering powerful proof of the capabilities of ECC. This lightweight, wireless, battery-powered, coin sized server is designed to be embedded in a wide array of appliances, utility meters, personal medical devices, and industrial sensors, etc.



“Sizzle” — World's Smallest Secure Web Server

This technology is designed to provide an easy-to-use wireless networking solution for secure monitoring and control across the Internet. It can be used in industrial settings for linking factories, manufacturing plants, supply chains, and field operations to central databases, using the standard web browsers.

Sizzle has already sparked broad interest within the academic community and beyond. According to Prof. David Wagner of U.C. Berkeley, a world-renowned computer security expert, this work represents the “biggest breakthrough in sensor network security in the last year.” A technical paper describing Sizzle has been selected to receive this year's Mark Weiser Best Paper Award at the IEEE Conference on Pervasive Computing and Communications (PerCom2005).

Why is this important? We typically think of Web servers as useful only for serving pages from files but a Web server can be used for monitoring and controlling remote devices. Today, many devices and services can be controlled using Web applications. A small, secure Web server such

as Sizzle embedded in a wireless sensor (or any other device) with Internet connectivity allows the device to be securely monitored and controlled from anywhere in the world.

Seeding Industry Adoption of Elliptic Curve Cryptography

Transforming the lab results and the promise of ECC into tangible benefits for real-world applications is no trivial task. It requires standardization of ECC in Internet security protocols, development of supporting infrastructure like certification authorities and implementation in servers, client devices and various applications. The Sun Labs team has been working diligently to address all of these issues. To date, the team's efforts include:

- Contribution of ECC technology to OpenSSL, which allows Apache Web servers (which currently represent 60% of the Web server market), to communicate securely and efficiently with lightweight devices using ECC technology
- Addition of ECC support to Netscape Security Services (NSS), which powers the Mozilla, Netscape and Firefox web browsers and the Sun Java System Web, Directory, and Messaging Server products
- On-going work with standards bodies and co-authoring the IETF Internet draft to specify the use of ECC technology in the SSL protocol.
- Active engagement with universities, corporations, and military technologists to identify and develop solutions for the challenges that must be addressed before smart sensor networks can achieve their full potential.

To read more about the Next Generation Cryptography project at Sun Labs, go to

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

Sun can be found in more than 100 countries and on the World Wide Web at

<http://www.sun.com>