Browser-based Secure Interaction with Sensor Devices

Vipul Gupta, Michael Wurm*
Sun Microsystems Laboratories
16 Network Circle, UMPK16-159
Menlo Park, CA 94025
vipul.gupta@sun.com, mwurm@sime.com
http://research.sun.com/projects/crypto

Abstract

Industrial, agricultural, health care, environmental, and military users, among many others, are just beginning to recognize how wireless sensor devices, like the ”motes”, can revolutionize their operations. As these devices become available at commodity prices, they will start turning up in staggering numbers everywhere imaginable. Due to cost and size constraints, these devices have limited memory, lack a display or input mechanism for direct user interaction and are equipped with processors far less capable than those found in PCs or PDAs. Furthermore, as these devices proliferate, increasing numbers of their users will be unskilled in managing and administrating computers. These factors make it especially challenging to support secure, user- friendly interaction with sensor devices.

Our demonstration shows a tiny secure web server (capable of SSL) embedded within sensor devices allowing them to be securely controlled and monitored via a standard web browser like Internet Explorer or Safari. We demonstrate our ability to restrict certain control and monitoring operations to authorized users and to configure sensor devices to send automatic notification, via SMS for example, upon detecting sensor readings outside a user-specified range.

Prior security research deemed public-key cryptography and, therefore, Internet standards like SSL that rely on it, infeasible on such devices. Our research group recently showed that Elliptic Curve Cryptography, a resource efficient alternative to RSA[1], not only makes public-key cryptography feasible on the Mica2dot and Mica2 mote devices, it also allows one to create an ECC enabled secure web server [1]. Unfortunately, most web browsers deployed today only support RSA. This demonstration shows that the Telos mote, the newest device in the mote family, has enough additional processing power and RAM[2] to make RSA-based SSL not only feasible but fairly efficient. With our highly optimized implementation, a full RSA handshake takes less than 6 seconds and the use of features like session reuse and persistent HTTPS makes subsequent interactions extremely quick, *e.g.* the time from sending an HTTPS request to receiving 1KB of application data in an HTTPS response is less than half a second.

Our architecture uses a PC connected to a MicaZ mote as a gateway to bridge the TCP/IP and IEEE 802.15.4 networks. The TCP/IP connection terminates at the gateway and is translated into an application specific wireless protocol which allows for reliable communication between the gateway and multiple sensors. However the security offered by SSL is end-to-end – from the browser to the mote.

References

[1] V. Gupta *et al.*, ”Sizzle: A standards-based end-to-end security architecture for the embedded Internet”, IEEE PerCom 2005, Mar, 2005.

*This work was performed while the author was on a student internship from the Graz University of Technology, Austria

[1] RSA is the most commonly used public-key cryptosystem used on the Internet today.

[2] The Telos has 10KB of RAM while the Mica2, Mica2dot have only 4KB. The Telos uses a 16-bit MSP430 processor whereas the Mica family of devices uses an 8-bit Atmel ATmega processor. The Telos also happens to be more energy efficient.