

HACK THIS

AS HACKERS MOVE
DOWN THE FOOD
CHAIN FROM
DESKTOPS TO
EMBEDDED
SYSTEMS,
HARDWARE-
AND SOFTWARE-
SECURITY DECISIONS
DOMINATE THE
DESIGN PROCESS.



By Warren Webb, Technical Editor

FIVE YEARS AGO, billions of embedded systems moved into the spotlight as pundits predicted Y2K failures that would disrupt manufacturing, power distribution, transportation, communications, water purification, cash dispensing, and weapon systems, among a multitude of other disasters. Governments and private com-

panies around the globe spent thousands of man-hours and billions of dollars to analyze and update embedded firmware to successfully avert potential catastrophe. These same embedded devices now face new enemies from the growing number of hackers and terrorists attempting to create similar disruptions, force unplanned operation, or extract private information. This new reality places security concerns at the top of the priority list for any new embedded-system design.

By virtue of their application, embedded devices have a much higher reliability expectation than most of the other computing systems that we deal with on a daily basis. Thousands of users every day shut down or reboot desktop computers to deal with errant programs or malicious viruses. Yet, you cannot stop or reboot many embedded devices, such as those in critical systems, without risking loss of life, property, or information. The desktop-software scenario of waiting for a failure or breach to occur and then devising a patch to bypass it is unacceptable in the embedded world. As hackers hone

their attacks against all forms of computer-based systems, device developers must respond with hardware- and software-security measures to prevent or contain any destructive invasion.

Although you can incorporate multiple layers of protection, no system or product is ever 100% secure. Most experts agree that a system is secure when the amount of time and money necessary to compromise the product exceeds the value of the information the hacker extracts. We must assume that, with enough resources, a hacker can break into any system. Because it is almost impossible to add security to an existing product, it must be a prime design goal from conception through production, deployment, and end-of-life disposal. NIST (National Institute of Standards and Technology) special publication 800-27 provides a number of security-related design principles to consider during each phase of a product's life cycle (**Reference 1**). These principles include defining a security policy, designing the product, handling upgrades, dealing with changing threats, incorporating new technology, establishing multiple security layers, and training programmers to deliver secure software.

At a glance.....**28**

Security benchmarks
check processor
performance**30**

For more information**32**

Illustration by Eric Mueller

One of the first security questions is to determine what information you need to protect so that you can select an appropriate safeguard. It is important to differentiate between the public and the private data that an embedded device stores or displays because you may be able to reduce or even eliminate the sensitive data to minimize the security effort. In addition to the obvious company and personal private data, your device may need to protect copyrighted material, such as books, music, or videos, with some type of digital-rights-management scheme. The details of your proprietary product design may also provide valuable information to outsiders or competitors.

WHO'S AT THE DOOR?

Next, you should determine your possible attackers and their level of sophistication. You may be able to protect music data from curious hobbyists with a simple password; however, if your device opens the vault door at Fort Knox, then you can expect attackers with experience, money, and determination to test your security features. Terrorist organizations want to bypass security provisions to endanger lives and create uncertainty. Foreign governments may fund attackers searching for data sensitive to our national security. If the data you are protecting involves finances, you can expect criminal elements to attempt to break your security. Finally, consider industrial espionage in which unscrupulous competitors can profit by reducing or eliminating product-design costs.

If a device stores sensitive or private data, your design must provide protection during normal operation, during attack through a network connection, or during electronic probing in the attacker's laboratory. Embedded devices, especially portable products, face many more security threats than a typical desktop system. Hackers may use sensitive test equipment to steal, disassemble, and probe small devices to extract data. They can remove memory elements from the product to extract their contents. Likewise, they may use debugging ports and software to read sensitive data or force unintended operation. Attackers may measure electromagnetic radiation or power consumption to gain clues about concealed information. Another trick forces the system to operate outside its design parameters by introducing ex-

AT A GLANCE

- ▶ Unlike the desktop-software-security policy of patch after failure, embedded products must continue operation in spite of security threats.
- ▶ Embedded-device security threats force designers to include physical packaging protection in addition to traditional software safeguards.
- ▶ The abundance of embedded-system architectures provides multiple attack opportunities and prevents the development of an industrywide security protection scheme.
- ▶ Specialized, embedded, secure storage silicon and coprocessors offload security authentication and encryption tasks to dedicated hardware.

treme temperatures, voltage excursions, and clock variations to expose aberrant behavior.

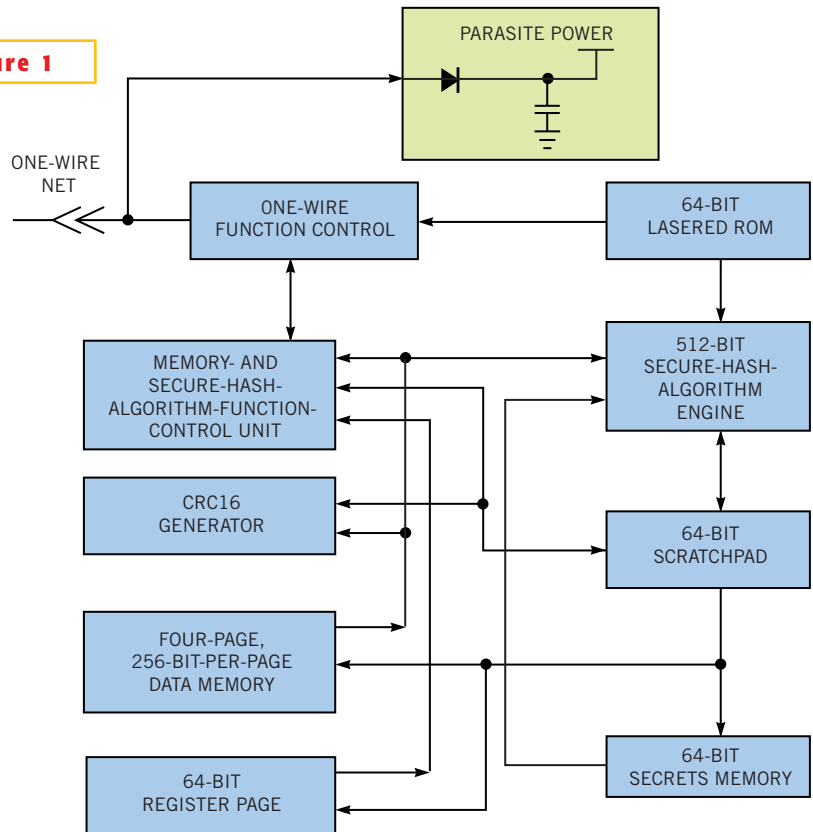
Because of the additional threats to

portable equipment, designers should incorporate physical deterrents to safeguard sensitive information. A hardened enclosure requiring specialized equipment to open may deter some attacks. Sensors can signal the software when an attack is under way. As a minimum, enclosure designs should provide visible evidence of tampering with seals or tapes that hackers destroy when they open the product. Concerning internal design, developers should design pc boards with security in mind. For example, BGA packages with critical signals hidden on internal board layers make it more difficult to probe and reverse-engineer them. Although hackers can remove some formulations with acid, designers can use epoxies and conformal coatings to protect all or part of a product's sensitive internal circuitry.

MEMORY LOSS

Memory devices are the favorite targets of internal attacks because they hold both the product's firmware and its sensitive data. Many devices can be read while in circuit and may provide tempo-

Figure 1



The Dallas Semiconductor DS2432 provides 1128 bits of 5V EEPROM partitioned into four pages of 256 bits, a 64-bit write-only secret, and as many as five general-purpose read/write registers.

rary plain text data during operation. If your device has a tamper sensor, you can incorporate hardware or software resources to rapidly erase sensitive data. Several vendors offer secure-memory devices to protect internal data. For example, the Dallas Semiconductor DS2432 combines 1024 bits of EEPROM with a 64-bit secret and 512-bit secure-hash-algorithm engine to provide low-cost, authentication-based security (Figure 1). The DS2432 sells for \$2.03 (1000).

On the software side, embedded products offer hackers a multitude of opportunities. Unlike desktop products, embedded products employ dozens of software architectures and operating systems that provide various levels of security, depending on each vendor's expertise. In an effort to establish standards for system security, the United States, Canada, and several European nations created the Common Criteria for Information Technology Security Evaluation, or Common Criteria. The Common Criteria structure allows consumers, developers, and evaluators to specify the security functions of a product in standard protection profiles and EALs (evaluation-assurance levels). Although no operating system has yet attained the highest EAL-7 certification, several development programs are under way. For example, LynuxWorks is working on a small runtime-kernel modification to its LynxOS-178 operating system that it ex-

pects to formally verify and test at the highest level. The exhaustive mathematical analysis necessary for an EAL-7 level certification limits the length of such software to a maximum of 6000 to 7000 lines of code.

Another embedded software-security standard, MILS (Multiple Independent Levels of Security), requires a partitioned real-time operating system that users can certify as secure by using rigorous tests. Memory protection and guaranteed resource availability allow you to manage secure and nonsecure data on one processor. The MILS

architecture allows the creation of mathematically verified, always-invoked, and tamperproof application code with security features that would-be hackers cannot bypass. Green Hills Software, LynuxWorks, and Wind River Software are among vendors working on MILS-compliant RTOSs for military and defense systems.

Before users can interact with a secure embedded system, they must undergo an authentication process to verify their identity. Authentication scenarios may include combinations of a secret password; a physiological trait, such as a fingerprint; or a security device, such as a smart card or key. Hackers have successfully obtained passwords by visually

or electronically capturing keystrokes or simply asking for them through a variety of subterfuges. Often, hackers can use widely available packet-capture programs to read clear text passwords as they travel unencrypted over local wired or wireless networks. Because it is fairly easy to compromise a password, security-conscious vendors are requiring two- or three-stage authentication. RSA Security's SecurID is one of the most popular two-stage authentication systems, and many organizations use it for identifying remote users. The token fits on a key chain and generates a new six-digit security code every minute (Figure 2). Users must enter their private PIN and the code displayed on the token to gain access.

NETWORK ENCRYPTION

When designers must connect an embedded system to a network or the Internet, they turn to encryption to safeguard their data. Effective encryption schemes

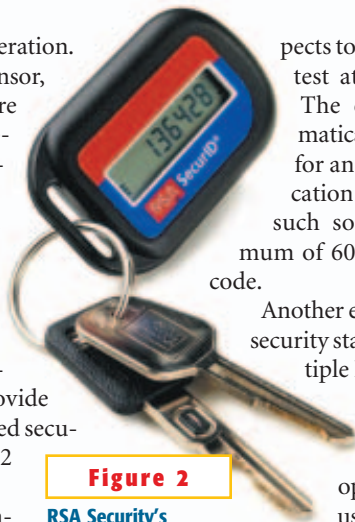


Figure 2

RSA Security's SecurID two-stage authentication system generates a new synchronized, six-digit, security code every minute to thwart password theft.



Figure 3

The IBM embedded security subsystem stores encryption keys for secure data and digital signatures for authentication and user identification.

SECURITY BENCHMARKS CHECK PROCESSOR PERFORMANCE

The EEMBC (Embedded Microprocessor Benchmark Consortium) has recently released a series of benchmarks to test a processor's ability to handle security as a stand-alone processor or as one that integrates a hardware accelerator. These new digital-entertainment benchmarks include MP3, MPEG-2/4 encoding and decoding, and the AES (Advanced Encryption Standard), DES (Data

Encryption Standard), and RSA (Rivest, Shamir, and Adleman) cryptography algorithms. The developers of the AES benchmark based it on Rijndael ANSI C Reference Code for AES Encryption/Decryption Version 2, with enhancements to pass the US Government-mandated FIPS (Federal Information Processing Standard) tests. The RSA and DES benchmarks use a version of Eric Young's SSLeay library

(Secure Socket Layer) for embedded execution. The DES benchmark processes both 3DES (Triple DES), and NCBC (nested-cipher-blocking-chaining) DES-key generation, encryption, and decryption. The RSA benchmark processes the public-encryption and private-key decryption of PKCS (Public Key Cryptography Standards) Version 1.5 and OAEP (Optimal Asymmetric Encryption Padding) padded

keys. The cost to join the consortium and gain access to this collection of benchmarks is \$12,000.

REFERENCE

1. National Institute of Standards and Technology, "Engineering Principles for Information Technology Security," <http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf>.

work equally well over wired, wireless, or power-line communications systems. The two basic types of encryption algorithms in use today both rely on a secret key, plus an encoding sequence to transform plain text into cipher text and vice versa. With the symmetric-encryption algorithm, the sender and the receiver use the same key to encrypt and decipher a message. Asymmetric encryption uses two keys—one for encryption and another for decryption. Public-key cryptography is a popular form of asymmetric encryption in which one of the keys is available publicly, and the other is secret. Key distribution and secrecy are fundamental problems in cryptographic-security systems. Given enough time and computing power, a hacker can decode any encrypted data without the key; however, designers can consider an algorithm secure if the decoding cost or time exceeds the value or useful life of the data. Any computer system, including an embedded product, can generate key pairs and submit the public key to a certificate authority, such as VeriSign, for validation. Secure systems maintain a local list of certificates to verify incoming messages and encrypt outgoing data. After the authority verifies the identity of the applicant, it issues a certificate containing the public key, the period of validity, and digital-signature data.

Compaq, Hewlett-Packard, IBM, Intel, and Microsoft in 1999 formed the TCPA (Trusted Computing Platform Alliance) to create open industry standards for interoperable hardware and software.

Figure 4



The Targus Authenticator PC card fingerprint reader offers biometric-access control for secure embedded devices.

The alliance defined and developed the concept of trusted computing as a security standard. The recently approved TCG (Trusted Computing Group) Standard 1.2 limits access to protected data, authenticates the identity of computers, and manages user privacy. An embedded TCP (Trusted Platform Module) enables these functions by monitoring the boot process to create hash values or checksums for the important elements, such as the BIOS, device drivers, and operating-system loaders. The TPM stores these values and compares them with the reference values that define the trustworthy status of the platform. The TPM also provides public/private-key RSA encryption and decryption along with a tamperproof on-chip memory for keys and passwords. Atmel's recently introduced AT97SC3202 TPM supports the TCG 1.2 standard, comes in a 28-lead TSSOP package, and sells for \$4 (10,000).

The IBM embedded-security subsys-

FOR MORE INFORMATION...

For more information on products such as those discussed in this article, contact any of the following manufacturers directly, and please let them know you read about their products in *EDN*.

AMD

www.amd.com

Atmel

www.atmel.com

Compaq

www.compaq.com

Embedded Microprocessor Benchmark Consortium (EEMBC)

www.eembc.com

Green Hills Software

www.ghs.com

Hewlett-Packard

www.hp.com

IBM

www.ibm.com

Intel

www.intel.com

LinuxWorks

www.linuxworks.com

Maxim/Dallas Semiconductor

www.maxim-ic.com

Microsoft

www.microsoft.com

National Institute of Standards and Technology (NIST)

www.nist.gov

RSA Security

www.rsasecurity.com

Targus

www.targus.com

The Common Criteria Project

www.commoncriteria.portal.org

The Trusted Computing Group

www.trustedcomputing.group.org

Verisign

www.verisign.com

Wind River Systems

www.windriver.com

tem is another TCG-compliant, chip-based device to protect data (Figure 3). The hardware portion works with IBM client software to provide an integrated security device that protects critical information, including encryption keys for privacy and digital signatures for authentication or user identification. The client software can also act as an interface between security-aware applications and the security chip itself to provide support for peripheral security-access-control devices. The Targus PC card fingerprint reader is an example of biometric access-control device that works with the embedded-security subsystem (Figure 4).

BROWSER SECURITY

The most common security protocol for TCP/IP (Transfer Control Protocol/Internet Protocol) network traffic is the SSL (Secure Sockets Layer), which provides data encryption, server authentication,

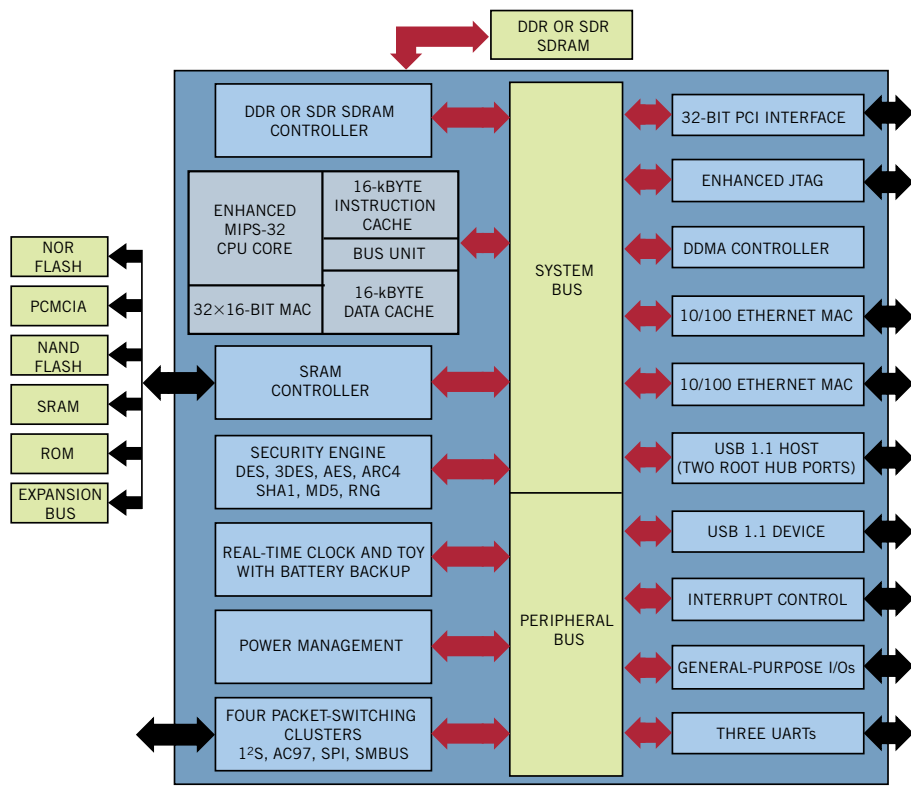
message integrity, and optional client authentication. SSL comes in 40- and 128-bit versions, which refer to the length of the session key that the encrypted transactions generate. The longer the key, the more secure the encrypted data. Most current desktop browser versions now encrypt transactions in 128-bit sessions. IPSec (Internet Protocol Security), another encryption standard, implements security at the network layer and allows you to transparently encrypt network traffic. You can install IPSec in a gateway computer to secure all traffic passing onto the Internet without adding overhead to individual network nodes. Like most other security protocols, IPSec includes provisions for both key and message exchange. VPNs (virtual private networks) use IPSec to create a secure network over the Internet.



With increasing data rates, embedded processors are straining to run security software, such as encryption algorithms, along with the primary application routines. Although benchmarks are available to test the security capabilities of any processor, several specialized processors transfer some of the encryption operations from the main processor to an integral auxiliary unit (see sidebar “Security benchmarks check processor performance”).

The recently introduced Au1550 security network processor from AMD, for example, includes an integrated security engine that implements the IPSec VPN-packet protocol (Figure 5). By accelerating the IPSec packet-processing task in hardware, the Au1550 offers security functions without burdening the main application software. The Au1550 sells for \$21.26 (high volumes) for the 333-MHz version and \$33.75 for the 500-MHz version. Similarly, Motorola has added integrated security engines to its popular PowerQuic processors. The MPC885, MPC8272, and MPC8349E families eliminate encryption bottlenecks in applications that support IPSec, SSL, and other security protocols.

Security concerns and precautions have changed the basic design guidelines for embedded products. The smallest circuitry, the tightest code, or even the longest MTBF (mean time between failures) are no longer the criteria for measuring clever designs. Modern embedded products must provide predictable and secure performance during not only normal operation, but also under attack. In the future, you can expect embedded-product-development budgets to increase to provide the packaging, processing performance, and secure firmware necessary to combat mounting security threats. □



NOTES:
 AES=ADVANCED ENCRYPTION STANDARD.
 AR4=ALLEGED RC4.
 ARC4=ADDRESS RESOLUTION CLIENT 4.
 DDMA=DESCRIPTOR-BASED DMA.
 DES=DATA ENCRYPTION STANDARD.
 MAC=MEDIA-ACCESS CONTROLLER.
 MD5=MESSAGE DIGEST 5
 RNG=RANDOM-NUMBER GENERATOR.
 SHA1=SECURE HASH ALGORITHM.
 3DES=TRIPLE DATA ENCRYPTION STANDARD.
 TOY=TIME OF YEAR.

Figure 5

The AMD Au1550 security network processor integrates an IPSec VPN packet protocol engine to offload the main application software.

TALK TO US
 Post comments via TalkBack at the online version of this article at www.edn.com.