



# A

BY WARREN WEBB • TECHNICAL EDITOR

s embedded devices permeate society and assume ever more important roles, the consequences of security failures are potentially catastrophic. Embedded devices provide unattended operation for thousands of mission-critical or safety-related systems in sectors such as manufacturing, health care, transportation, finance, and the military. Although we rely on these embedded systems without giving them a second thought, any one could be the potential target of casual hackers, organized crime, terrorists, or even adversary governments. The responsibility to protect against these attacks falls squarely on the shoulders of the system designer, who must secure not only the data that passes through or is stored on his embedded device, but also the intellectual property of the product itself.

Historically, designers physically protected and isolated embedded devices to achieve reasonable data security. Today, widespread interconnectivity may expose a critical embedded system to data extraction or process manipulation from anywhere in the world.

Unlike desktop systems, an embedded product must incorporate all security measures before its deployment. Embedded-system designers cannot wait for a breach and then devise a patch to cover security flaws. Users expect embedded products to perform a function for years without modification, and you can't stop or

reboot many devices without risking loss of life, property, or critical information.

Security must be a prime design consideration from conception through production, deployment, and end-of-life disposal, because it is almost impossible to add to products currently in the field. The NIST (National Institute of Standards and Technology) provides designers with a number of security-related publications at its CSRC (Computer Security Resource Center). These documents outline life-cycle design principles to consider, such as security-policy definition, product design, threat identification, technological options, and programmer education. For example, the first challenge is to identify what data or proprietary information requires protection before selecting safeguards. It may be possible to reduce or even eliminate sensitive data to minimize the security effort. Next, you should

SECURITY  
REQUIREMENTS  
NOW TOP  
THE EMBEDDED-  
SYSTEM DESIGNER'S  
CHECKLIST AS  
NETWORKED  
DEVICES MULTIPLY  
AND HACKERS  
OPTIMIZE  
THEIR ATTACK  
TECHNIQUES.

# HACK- PROOF DESIGN



## AT A GLANCE

Threats to portable devices force designers to include physical packaging protection in addition to traditional software safeguards.

Unlike the desktop-software practice of patch after failure, embedded products must continue operation in spite of security threats.

Widely available cryptography algorithms and secure protocols offer embedded-system designers the best security protection for Internet-connected devices.

New pay-as-you-go business models rely on secure hardware and software architectures to allow customers to pay for pricey systems as they use them.

determine your possible attackers and their level of sophistication. A simple password may stop a curious amateur, but determined intruders require multiple levels of security.

## SEPARATE AND SECURE

An obvious security measure is to physically isolate networked systems from outside influence. If you can collocate the embedded system and server on the same network segment without Internet access, most security problems disappear. Isolation is especially effective in highly critical applications, such as controlling a factory, where disruption would be costly. Minimizing the connection time to the Internet can also thwart many hacking attempts. A short-term connection to exchange data at random times prevents search robots from identifying your system. However, if your embedded system is a target of a hacker, short connections will only delay unauthorized access.

Attackers can steal embedded devices, especially portable products, disassemble them, and probe them with sensitive test equipment to extract data. They can remove memory elements from the products to possibly extract their contents. Likewise, they can use

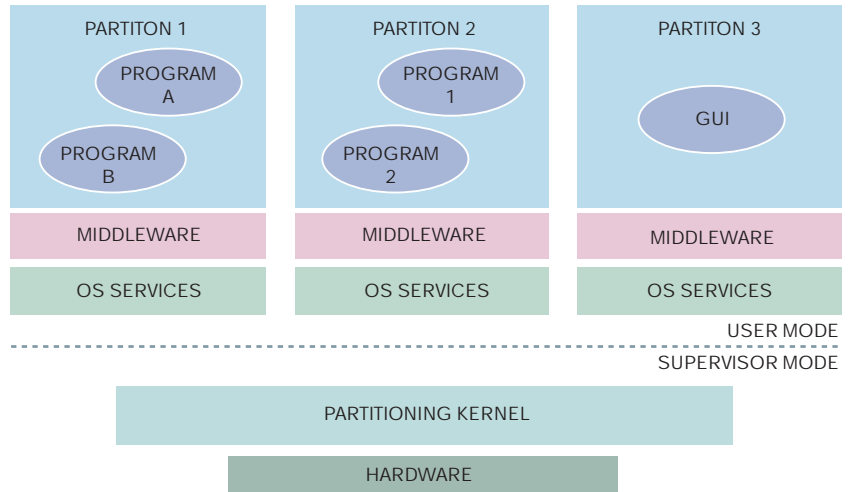


Figure 1 The MILS (Multiple Independent Levels of Security) architecture isolates kernel, middleware, and application components (courtesy LynuxWorks).

active debugging ports and software to read sensitive data or force unintended operation. Attackers may even monitor electromagnetic radiation or force the system to operate outside its design parameters, with extreme temperatures, voltage excursions, and clock variations, to gain information.

Equipment designers should also incorporate physical deterrents to safeguard sensitive or proprietary informa-

tion. A hardened enclosure requiring specialized equipment to open may deter some attacks. Internally, designers should engineer pc boards with security in mind. For example, BGA packages with critical signals hidden on internal board layers complicate probing and reverse-engineering. Although you can remove some formulations with acid, epoxies and conformal coatings also provide protection to all or part of a

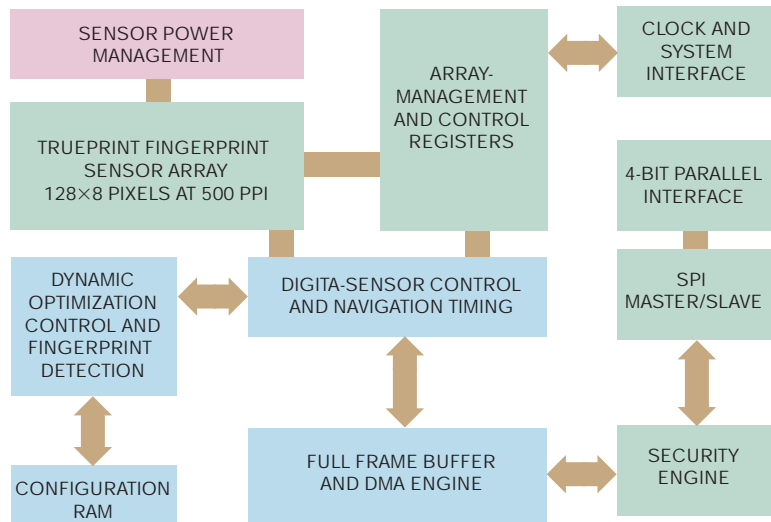


Figure 2 With a 12x5-mm footprint, the EntréPad 1510 slide sensor from AuthenTec enables secure fingerprint authentication on portable devices.



product's sensitive internal circuitry.

To establish standards for system security, the United States, Canada, and several European nations created the "Common Criteria for Information Technolo-

gy Security Evaluation" usually referred to as "the Common Criteria." The Common Criteria Web site includes a developer section with guidelines and complete documentation. 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). Another embedded-

## SAFEGUARDING KEYS

*By Kris Ardis, Dallas Semiconductor/Maxim*

When most people think about security, they first think of encryption. An embedded system that sends and receives only triple-DES (Data Encrypted Standard)-encrypted commands might seem difficult to crack. However, imagine a house that has the most advanced door locks and an electronic security system; it would also be difficult to crack. An enterprising thief would not try to circumvent the house's protection but instead would attempt to steal the keys or coerce the security code from the homeowner. Embedded systems are prone to the same weakness: All the encryption in the world is futile if someone steals the encryption key.

Proper key protection starts with where you store the keys. The safest place is in the same place you will use them. Embedded systems, therefore, need to store encryption keys inside a microcontroller and never allow the keys to leave. If you store the key in an external memory, such as a serial EEPROM or an external RAM, the microcontroller would need to fetch the key before using it. When the external memory transmits the key to the microcontroller, it transmits it in the clear,

allowing anyone with an oscilloscope or a logic analyzer to discover the key data.

On-chip EEPROM or flash may also be inadequate protection. A determined attacker could remove the microcontroller's plastic packaging and use a microprobe to inspect the memory cells. In high-security applications, losing the key would be catastrophic. An attacker would have unimpeded access to financial networks or could create undetectable fake-ID cards.

High-security applications present unique challenges for IC designers. Secure microcontrollers, such as Dallas Semiconductor's DS5250, address this design challenge by providing battery-backed, nonvolatile SRAM for on-chip key storage. This custom-designed memory can link to several tamper-detection circuits, both on- and off-chip, and instantly erase when the situation meets one of several tampering criteria. Some on-chip sensors, such as temperature and voltage detectors, respond to fault-injection attacks. Such attacks occur when the secure microcontroller is operating outside its maximum

operating range, attempting to make cryptographic operations fail so that the device leaks key data. Another kind of on-chip sensor detects microprobing attacks. A silicon mesh in the top layer of the chip initiates a "tamper destruct" if someone shorts or breaks its sub-micron traces. Secure microcontrollers also include self-destruct input pins that external mechanisms, such as microswitches, light sensors, and pressure sensors, can trigger.

Although physical protection of the key is critical, so is logical protection. Secure microcontrollers offer encryption accelerators that can quickly and securely execute standard algorithms. Public-key operations such as RSA (Rivest, Shamir, and Adleman) execute in milliseconds, and symmetric algorithms such as triple DES run in microseconds. Hardware accelerators are more resistant to timing attacks than software algorithms, because they complete in the same number of machine cycles regardless of the actual values of the keys or the data. Secure microcontrollers also incorporate hardware random-number generators that vary in behavior over

voltage, temperature, and process variations, making it impossible for an attacker to guess the value of generated keys or blinding values.

Encrypted program memories provide further logical protection for the applications running on secure microcontrollers. When you first initialize the system, the secure microcontroller uses the on-chip random-number generator to create a unique key, which the system uses to encrypt the program space. When the device executes, the system decrypts the encrypted instructions and places them in an on-chip cache in real time. This method not only protects intellectual property and thwarts reverse-engineering, but also prevents an attacker from executing malicious code.

Applications concerned with security have unique challenges to meet. By designing secure microcontrollers with physical and logical security in mind, you can create the safest foundation for applications that must protect secret keys.

---

#### AUTHOR'S BIOGRAPHY

*Kris Ardis is a product manager for secure microcontrollers at Dallas Semiconductor/Maxim.*



software security standard, MILS (Multiple Independent Levels of Security), requires a partitioned real-time operating system that you can certify with rigorous tests (Figure 1). Memory protection and guaranteed resource availability allow you to manage secure and nonsecure data on a single processor. The MILS architecture allows designers to create application code with tamperproof security features that you cannot bypass, that you can verify mathematically, and that the system always invokes.

Before a user can interact with a secure embedded system, he must undergo an authentication process to verify his 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. For example, the EntréPad 1510 slide sensor from AuthenTec enables fingerprint authentication for portable devices such as cell phones. Contained in a 12×5-mm, 40-pin BGA package, the sensor includes a dense 128×8-pixel-detection matrix along with pattern-matching firmware (Figure 2). Hackers have been successful in obtaining passwords by visually or electronically capturing keystrokes or simply asking for them through a variety of subterfuges. Often, passwords pass over local wired or wireless networks in the clear or unencrypted, and attackers can capture them with simple packet-capture programs widely available on the Internet.

## CODE AND DECODE

When an embedded system must connect to a network or the Internet, designers turn to encryption to safeguard their data. Effective encryption schemes work equally well over wired, wireless, or power-line communications systems. Two basic types of encryption algorithms are in use today, both relying on a secret key plus an encoding sequence to transform plain text into cipher text and vice versa. With symmetric encryption, the sender and 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 that makes one of the keys available publicly and keeps



Figure 3 The Spartan P630 targets military-manpack applications with a hardened, sealed enclosure and software for preboot access control and data encryption.

the other secret. Key distribution and secrecy are fundamental problems in cryptographic security systems (see sidebar “Safeguarding keys”).

The most widely used security protocol for TCP/IP network traffic is the SSL (Secure Sockets Layer), which provides data encryption, server authentication, message integrity, and optional client authentication. SSL comes in 128- and 256-bit versions whose names refer to the length of the session key that encrypted transactions generate. The longer the key, the more secure the encrypted data. IPSec (Internet Protocol Security), another

encryption standard, implements security at the network layer and allows the system 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. Virtual private networks use IPSec to create secure networks over the Internet.

Targeting military-manpack applications in which security is paramount, General Micro Systems recently introduced a secure portable PC with a 6.5×3×0.5-in. main-board footprint (Figure 3). The Spartan P630 is a hardened PC featuring a 1.4-GHz Pentium-M processor, as much as 2 Mbytes of L2 cache, an embedded GPS (global-positioning-system) receiver, and 802.11b/g wireless communications in a pocket-sized form factor. The company can configure the device with as much as 2 Gbytes of ECC memory, 16 Gbytes of bootable flash, as much as 60 Gbytes of hard-disk drive, and an LCD/touchscreen in a hardened, sealed enclosure. To ensure secure operation, Spartan includes software for preboot access control and data encryption along with automatic file deletion if someone compromises the system. Spartan also features a six-hour bat-



Figure 4 Security features allow Pure Digital to profitably offer customers a one-time-use video camcorder for less than \$40.



tery life and is available in a conduction-cooled version operating at  $-40$  to  $+85^{\circ}\text{C}$  or a standard convection-cooled version with a  $0$  to  $55^{\circ}\text{C}$  temperature range. Packaging options include a titanium-aluminum enclosure for rugged applications. Software support for the P630 is available under Windows XP, Linux, QNX, and VxWorks. Prices for the conduction-cooled version start at \$3400 (100).

### SECURE BUSINESS

With improving security, device manufacturers are experimenting with business models to attract more customers. In the pay-as-you-go scenario, customers receive a fully functional device and promise to pay for it as they use it or over the life of a subscription plan. If the customer fails to make a payment, the vendor can disable the device by withholding network-activation codes. A strong security model then prevents the customer from bypassing activation or removing parts.

For example, Microsoft recently announced FlexGo, a pay-as-you-go platform to extend PC ownership into emerging markets. FlexGo requires that system components individually track usage based on active minutes or a specific end date. When a consumer has used all of the available computer time, Microsoft limits access to the PC until the consumer adds more time. The company also imposes usage limitations when there are signs of system tampering. Microsoft has also added secure operating-system components to enable metered use of the software. A FlexGo software-development kit allows businesses to use their own billing systems to manage Microsoft's provisioning system to offer pay-as-you-go computer-use time to customers.

With stand-alone embedded-security challenges, Pure Digital manufactures a pocket-sized, one-time-use camcorder that records as much as 20 minutes of video and audio (**Figure 4**). The device is available through several camera- and convenience-store outlets for as little as \$20 plus a \$12 processing charge to copy your movies onto a DVD. The device includes a fixed-focus lens, a 1.4-in. color LCD, and speaker plus operator controls

### MORE AT EDN.COM

- For more on a one-time-use video-camera, go to [www.edn.com/article/CA629314](http://www.edn.com/article/CA629314).
- For some history on embedded-device security, go to [www.edn.com/article/CA434871](http://www.edn.com/article/CA434871).
- We encourage your comments! Go to [www.edn.com/060720cs](http://www.edn.com/060720cs) and click on Feedback Loop to post a comment on this article.

to record, play back, and delete unwanted scenes. Although the device is a hacker's delight, and several Web sites are devoted to extracting the video without returning the camcorder for processing, there are sufficient security measures to deter most users.

Security precautions and potential information-disclosure consequences have changed the fundamental design goals for embedded products. Designers are no longer driven to produce the simplest, lowest cost device for each project. Security requirements have forced designers to beef up resources with faster, more capable processors, secure data storage, and tamperproof hardware to protect the system and data while executing the application. EDN

### FOR MORE INFORMATION

AuthenTec Inc <a href="http://www.authentec.com">www.authentec.com</a>	LinuxWorks <a href="http://www.linuxworks.com">www.linuxworks.com</a>
Common Criteria <a href="http://www.common-criteria.org">www.common-criteria.org</a>	Microsoft <a href="http://www.microsoft.com">www.microsoft.com</a>
Dallas Semiconductor/ Maxim <a href="http://www.dalsemi.com">www.dalsemi.com</a> <a href="http://www.maxim-ic.com">www.maxim-ic.com</a>	NIST (National Institute of Standards and Technology) <a href="http://www.nist.gov">www.nist.gov</a>
General Micro Systems <a href="http://www.gms4sbc.com">www.gms4sbc.com</a>	Pure Digital <a href="http://www.puredigitalinc.com">www.puredigitalinc.com</a>

You can reach  
Technical Editor  
**Warren Webb**  
at 1-858-513-3713  
and [wwebb@edn.com](mailto:wwebb@edn.com).

