Strengthening the link between the real and the digital world

Reducing Security Vulnerabilities in Connected Cars and Factories with Secured Flash

Whitepaper

Sandeep Krishnegowda, Senior Director of Flash Product Marketing; and Naseem Aslam, Product Marketing Principal Memory Solutions, Cypress Semiconductor Corp, an Infineon Technologies Company

Introduction

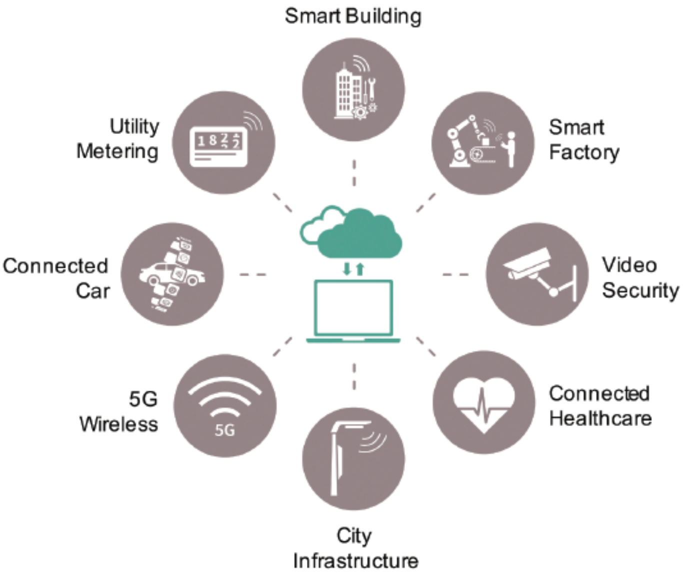
Analysts estimate that more than half of all cars sold in the U.S. this year will come with internet connectivity(1), and Gartner believes more than 750,000 cars with autonomous driving capabilities will roll off manufacturing lines by 2023(2). As more vehicles become connected and go autonomous, the possibility of bad actors taking control of cars on the road is very real, and likely to become of increasing concern.

In 2015, hackers famously took control of an SUV through its infotainment system, first interfering with audio and climate controls, and then bringing the car to a stop in traffic on a busy St. Louis highway. The hackers then proved they could go beyond these tactics by stopping the engine and disabling the brakes.

The point of entry for their “experiment” was through the vehicle’s internet-connected entertainment system, where the hackers rewrote the firmware and planted their code in an adjacent chip. The re-scripted chip was then able to send commands to other parts of the car through its internal CAN bus computer network.(3)

Smart factories are vulnerable to security threats, too

Security threats are not only an issue for connected cars, though, they are also a big concern to automated factories. In recent tests conducted by Trend Micro's Forward-Looking Threat Research Team, researchers were able to demonstrate how easily one could alter factory robot settings with the intent to control the robot, damage its parts or cause injuries to people who work near it. The research also identified tens of thousands of industrial devices residing on public IP addresses that could be hacked.(4)



Smart factory attacks not only threaten to impact production and generate significant financial loss for a company, but they can also risk lives. Verizon research estimates that 86% of attacks in manufacturing are targeted, and almost half involve theft of intellectual property.(5)

In hospitals, a security flaw was recently discovered in commonly used anesthesia and respiratory machines that would allow hackers to adjust specific commands, including the composition of gases in the machines. (6) According to Techcrunch, hackers could gain access to the tools through the hospital network, change the machine's protocol, and execute commands with no authentication required. These examples illustrate how vulnerable connected equipment can be, and why greater security is needed.

Other IoT Systems Also at Risk

Security threats can impact everyday life in other ways as well. Recently, a major manufacturer of portable medical equipment recently recalled a line of insulin pumps after discovering a potential vulnerability that would allow hackers to change the device's settings via an RF signal.(7) The increased or decreased doses of insulin could result in life-threatening changes in blood sugar levels for the patient using the device.

To legislatively minimize such hacks from occurring, the state of California passed SB-327 in 2018. The IoT Security Law, as it is named, became the first in the U.S. to require all connected devices sold in the state to have some form of security protection built in.(8) Secured Flash is one way that helps manufacturers meet this strict requirement.

Increased Security in Embedded Systems

Connected devices, including cars, smart factories, hospital equipment, and portable medical products, are all vulnerable to cyberattack through many different paths, including software updates, data downloads, and connections to the cloud. One of the primary targets of hackers is the flash memory device, which stores boot code, security keys and other critical data that are used to keep the system functioning properly.

Most systems use secured SoCs with embedded Flash (eFlash) and operate in a trusted execution environment (TEE) in order to safeguard the system from malicious attacks. However, with the need for more performance and lower power at the edge, advanced processors are migrating toward 22 nm technology and below. It is becoming more difficult for engineers to find a reliable, nonvolatile memory technology available on advanced technology nodes. Some options such as RRAM and MRAM have been considered contenders to take on this role, however they have not been able to meet the requirements in a production environment due to data integrity and cost issues, respectively. The solution is to extend Hardware Security Module (HSM) functionality to a secured external Flash, as shown in Figure 1 below.

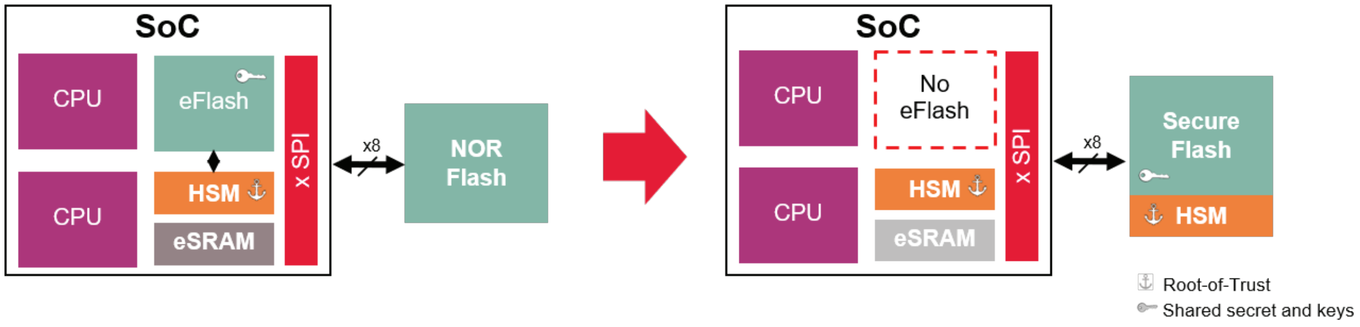


Figure 1: The dis-integration of eFlash will create the need to extend Hardware Security Module (HSM) functionality to a secured external Flash.

How Flash Can be Compromised

There are many ways in which external Flash memory can be compromised in a system:

Impersonation. One way this is done is by borrowing pop-up notifications from a legitimate installer to gain access to the system. Users may not realize they are being hacked because the installer looks legitimate.

Replaying Transactions. This is when the hacker rolls back the contents of the Flash device targeting previously known vulnerabilities in the system.

Stealing Security Keys. Performed during provisioning operations in an unsecure facility, when storage assets and keys are being programmed into the device.

Cloning. Hackers clone the device, replace it and this way compromise the integrity of the Flash device.

Intrusion. This is done by tampering with the contents of the Flash device. This is when hackers work their way into the Flash device and edit or replace the system files to disrupt the performance of the machine.

Snooping Attacks. During transactions to and from the Flash device, Flash devices can be compromised by extracting unprotected system keys or passwords.

Disclosing Contents of the Flash device through side-channel attacks and gaining access to system secrets.

How to Implement Security with External Flash

Security considerations in Flash device are based on C.I.A. model:

C	CONFIDENTIALITY	Protecting data stored in Flash device so it is not available or disclosed to unauthorized parties
I	INTEGRITY	Keeping the Flash data accurate and unmodified without detection and/or authorization
A	AUTHENTICITY	Protecting services (e.g. Read/Write) so they are available only to authorized parties

To make secured NOR Flash “fail safe” and part of the “trusted boundary” of a secured processing environment, it must implement a hardware-based root-of-trust to establish the identity of the device. It also must provide end-to-end protection to prevent the modification or copying of code and/or data, including authentication and encryption, secured key storage, and secured regions with protected read/write access where bits can be exchanged between the HSM in the SoC and a cryptographically secured flash memory.

As shown in Figure 2 below, Secured NOR Flash provides hardware-protected secured storage for security keys, certificates, password hashes, application-specific data, configuration data, and biometric sensor data. Using standard bus protocols such as QSPI and xSPI, it can work with the host to achieve the security levels required in demanding connected applications, while retaining full compatibility with existing host memory controllers. Secured NOR Flash can deliver safe system boot-up, log critical information, and extend working memory for essential functions.

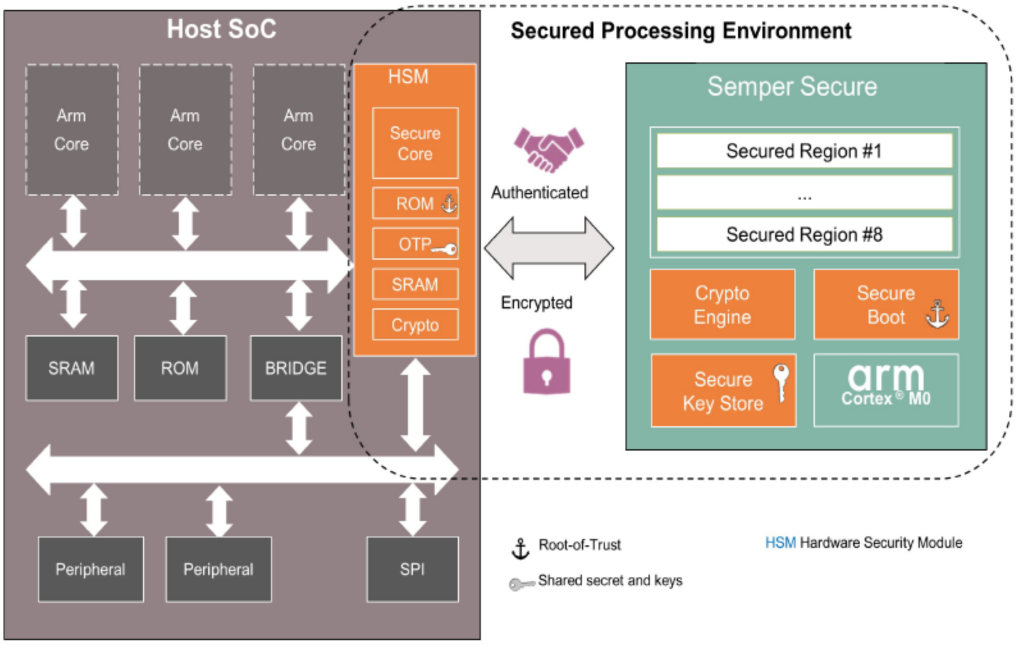


Figure 2: External NOR Flash works with the host processor to achieve high levels of security for demanding applications.

External Secured Flash for A utomotive and Industrial Applications

Secured Flash is an ideal solution for a variety of automotive and industrial applications. Target industrial applications include smart factories that use autonomous systems to monitor and control the factory, industrial machine vision cameras, medical equipment, test and measurement equipment, and M2M communications.

Key automotive applications include Advanced Driver Assistance Systems (ADAS), gateways, telematics, instrument clusters, and powertrain controls. These systems rely on Flash memory for storage of safety-critical algorithms and data. Some of the ways secured Flash can help protect drivers include:

- Secured Code Storage – Secured Flash devices can be used to cryptographically store sensitive system data including security keys, certificates, passwords, configuration data, biometric sensor data, and can also support authenticated and encrypted transactions.

- Fast Secure Boot – Automotive applications must be able to reply to CAN messages within 100 ms of power-on, or risk driver safety. Secured Flash can enable secure boot that authenticates with the host MCU and starts code execution in less than 10 ms.

- Secured Firmware Over the Air (FOTA) Updates – Secured Flash enables end-to-end security protection by allowing only authorized updates that can be managed directly from a remote server or cloud. This is a big deal, considering most cars have more than 100 Electronic Control Units (ECUs) and more than 100 million lines of software code. It also enables remote device health monitoring by detecting if any critical assets were compromised, and a recovery mechanism to restore system integrity.

Cypress' Semper Secure Flash technology

Cypress' Semper Secure NOR Flash technology is the only secured Flash memory device to deliver security, safety, and reliability to automotive, industrial, and communications systems at a low total cost-of-ownership.

Semper Secure NOR Flash integrates an Arm® Cortex® M0 processor inside the NOR Flash memory. It provides hardware-protected secured storage for security keys, certificates, passwords, and other critical data, and can also support authenticated and encrypted transaction to protect against security threats. Using standard bus protocols, it works with the host MCU to achieve security levels required in demanding connected applications.

The block diagram in Figure 3 shows how Semper Secure establishes a secured processing environment in many different layers. First, Semper Secure provides a hardware root-of-trust with a hardware-accelerated crypto-engine that enables secure boot, storage, and over-the-air updates. It also facilitates authenticated and encrypted transactions by providing secured regions with configurable access controls and built-in protection against side-channel attacks. Additionally, its flexible, in-memory compute architecture with advanced cryptography algorithms keeps pace with the constantly-changing security landscape, ensuring that products that use the technology are not only safe today, but also adapt to future needs without the need for system hardware redesigns.

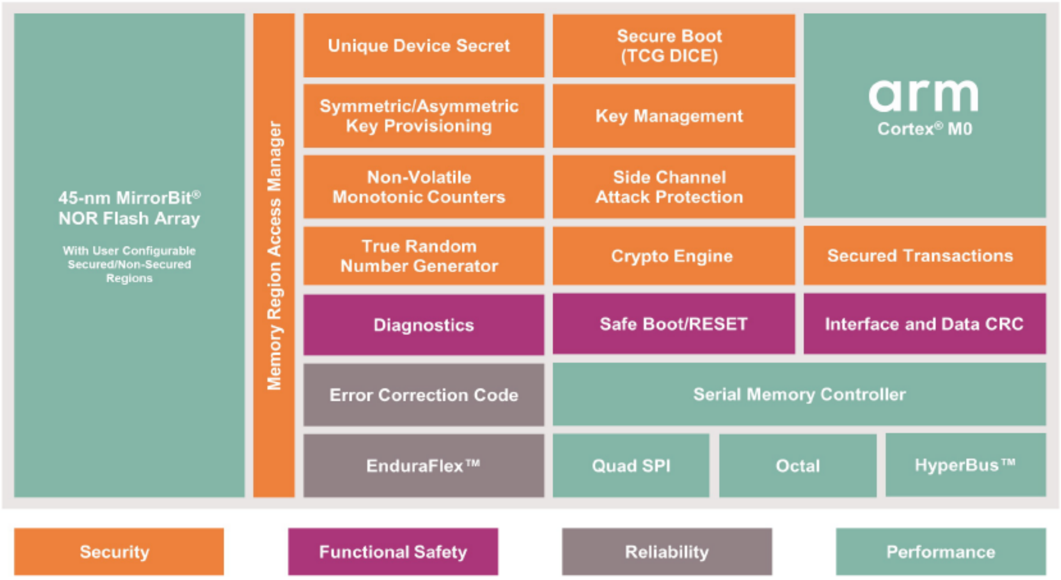


Figure 3: Semper Secure block diagram illustrates the many layers of security that are built into this external NOR Flash device

Conclusion

Automobiles and factories are becoming more connected, driving the need for greater system security. As shrinking design geometries are forcing Flash devices outside the trusted execution environment of a secured MCU with embedded Flash, new secured Flash devices must offer solutions that protect critical system data from attacks. Cypress' Semper Secure Flash provides a trusted solution to meet these demanding requirements with adaptability for future needs. For more information about Semper Secure Flash, please visit www.cypress.com/sempersecure.

End Notes:

1 Lemos, Robert, "Car Hacking Hits the Streets," Dark Reading, January 7, 2020,
https://www.darkreading.com/edge/theedge/car-hacking-hits-the-streets/b/d-id/1336730

2 Moore, Mike, "Smart Cars Could be Hijacked via AI Hacking," TechRadar, February 19, 2020,
https://www.techradar.com/news/smart-cars-could-be-hijacked-via-ai-hacking

3 Greenberg, Andy, "Hackers Remotely Kill a Jeep on the Highway with Me in It," Wired Magazine, July 21, 2015,
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

4 Maguire, Ed, "Hacking the Factory Floor: Cybersecurity in Smart Manufacturing,"
TechTarget (contributed article from Momenta Partners); June 28, 2018,
https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Hacking-the-factory-floor-Cybersecurity-in-smart-manufacturing

5 Kotelec, Michael, "Cybersecurity in Manufacturing: Targeting Trade Secrets and New Technology,"
Manufacturing Business Technology, January 29, 2019, (contributed article from Verizon)
https://www.mbtmag.com/security/article/13249195/cybersecurity-in-manufacturing-targeting-trade-secrets-and-new-technology

6 Whittaker, Zack, "A Widely-Used Infusion Pump can be Remotely Hijacked, Say Researchers," Techcrunch, June 13, 2019,
https://techcrunch.com/2019/06/13/alaris-infusion-pump-security-flaws/

7 Doffman, Zak, "FDA Warns of Dangerous Cybersecurity Hacking Risk with Connected Medical Devices,"
Forbes Magazine, June 28, 2019, https://www.forbes.com/sites/zakdoffman/2019/06/28/fda-issues-cybersecurity-warning-over-hacking-risk-for-connected-medical-devices/#1c8e21a7561d

8 "California Legislative Information, Bill Information: SB-327 Information Privacy, Connected Devices," 2017-2018.
https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

Cypress Semiconductor Corporation
198 Champion Court, San Jose CA 95134
phone +1 408.943.2600 fax +1 408.943.6848
toll free +1 800.858.1810 (U.S. only) Press "1" to
reach your local sales representative