White Paper

How to Solve the 6 Top Security Challenges of Embedded IoT Design

August 2019

Abstract

Ensuring security for embedded IoT designs can be challenging and time-consuming, even for veteran developers. Explore these six common security challenges and discover how Renesas offers a platform-based approach to security that benefits from the latest advances in both hardware and software, and delivers in-depth, comprehensive defenses with multiple layers of protection.

Common Security Challenges for IoT

An estimated 31 billion IoT (Internet of Things) devices will be deployed by 2020, many with limited security controls that leave them ripe for hacking. Why are so many embedded systems designed with vulnerabilities? In large part, it's because developers face multiple challenges and complexities when securing embedded applications and devices. They must keep up with threat landscapes that morph daily, as well as meet always-evolving security standards. Simultaneously, complex applications may require meeting multiple standards, which can inhibit device compatibility and flexibility. In many development scenarios, higher-level security features may also come with higher costs and higher power consumption, which can adversely impact the marketability of the end device.

In this white paper, we identify six of the most common security challenges that embedded developers face and provide insights and answers to help streamline the security design workflow to accelerate delivery of secure devices, services, and systems to the market.

Here are the six security challenges for the embedded developer explored throughout this white paper:

1. How do I secure my device in 2019?
2. How do I secure my products so they are not replaced by unauthorized copies?
3. How can I manage security with less complexity?
4. How do I secure my device against multiple security threats?
5. I'm not a security expert, but I need a secure product. What do I need to know?
6. How can I get more standardization and support for security from vendors and put my own resources on the parts of the design that differentiate?

Challenge 1: How do I secure my device in 2019?

A few years back, application developers didn't need to worry about securing their products because devices and applications were not connected like they are now. Today, even the most basic items – from light bulbs to baby monitors and prescription drug containers – are connected to the internet or a cloud. Too often, security is overlooked or only addressed after it is too late.

In 2019, securing IoT applications from cyber threats to protect data and functionality is a critical concern for developers and must be built into devices from the start at both the hardware and software levels. A platform-based approach to security offers multiple layers of defense by taking advantage of the latest security advances in both hardware and software to implement in-depth, comprehensive protections.

For the hardware side, effective security needs to include:

- Secure key management, to ensure that keys are not accessible in an unencrypted state. The device should be able to securely generate and store keys, including private keys, to enable truly secure device-unique identity and provisioning.
- Hardware-accelerated encryption, hashing, and true random number generation, which accelerates cryptographic operations on the device. This hardware support saves both time and power.
- Secure memory access to protect specific regions of RAM and Flash memory from unauthorized access. Separate memory domains isolate sensitive code and data from non-secure code and data, while write-once protected memory safeguards code and data from change or reprogramming.

- Protected debugging and programming access, which reduces the risk of hackers using debugger and programming interfaces as attack vectors.

The software side should include:

- Integrated and optimized commercial-grade software with proven application frameworks and standard APIs.
- Driver level APIs to provide an easy interface to hardware security features.
- Cryptographic libraries with a collection of APIs that provide a wide range of security features including macro-level security functions, root-of-trust, and the ability to recognize trusted sources and code.
- Built-in support for common communication protocols and transports, such as Hypertext Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS), and other cloud-specific protocols.

Renesas has been a leader in embedded security for decades and is well positioned to address the heightened need for security in today's connected products. Renesas offers a platform-based approach to embedded security, providing a multi-tiered development infrastructure that provides in-depth security protection for a wide variety of embedded products.

For instance, the Renesas Synergy™ platform is a comprehensive, qualified development platform that includes production-grade software and a scalable family of pin-compatible MCUs, pre-integrated and pre-tested to provide security at multiple levels. The Synergy platform ensures that IoT applications are built on a secure, robust technology foundation.

The Synergy platform provides multiple key generation options through the Secure Crypto Engine (SCE) module. The SCE can generate a unique, cryptographic, hardware-based device identity that can be stored securely in internal flash by employing the Security Memory Protection Unit (SMPU) and the Flash Access Windows (FAW). These memory protection features offered by Synergy devices can also be used for storing secure boot code, certificates, and keys along with any other sensitive data. In addition, the SCE can provide secure key storage to prevent exposure of sensitive information, even in non-secure memory. Key isolation can be ensured by MCU-unique key wrapping, which encrypts keys specifically for each MCU, so keys are only accessible within the SCE module on the individual MCU that performed the wrapping.

The Secure Crypto Engine

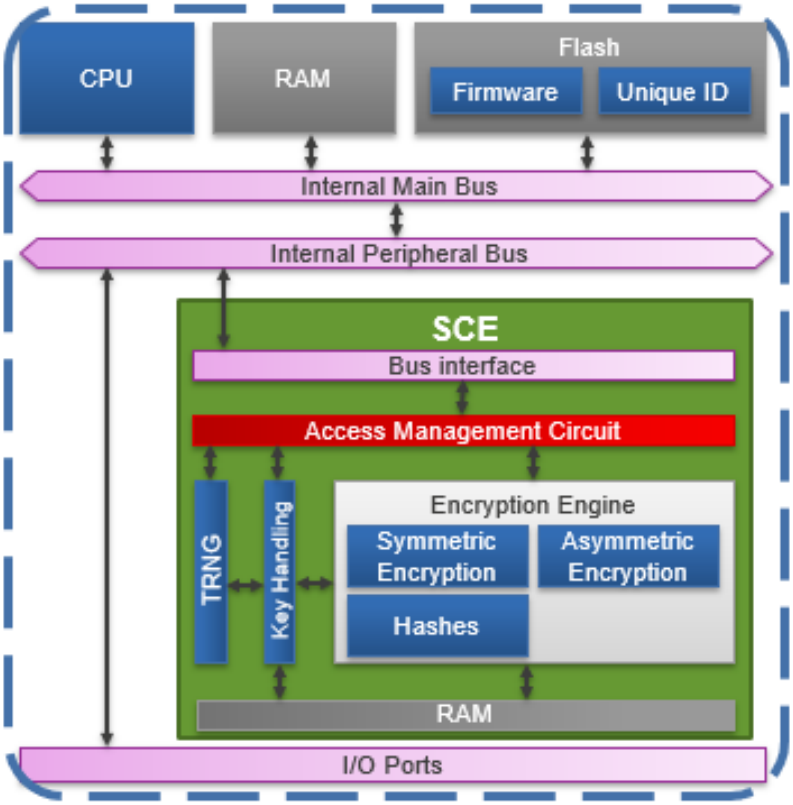

Figure 1: The Secure Crypto Engine, an isolated subsystem within the MCU (source Renesas Electronics Corp.)

Developers also need to ensure that their development platform makes it safe and easy to connect to the cloud. As IoT applications grow more complex and safety-critical, they require ever-more data processing power. Secure connections to the cloud become essential as these systems increasingly depend on cloud computing to deliver a hyper-scale compute and storage infrastructures for IoT data. Synergy MCUs deliver support for cloud connectivity with built-in MQTT and TLS modules, and the Synergy cloud connectivity applications provide secure, built-in connectivity to leading cloud environments, including Amazon Web Services (AWS), Google Cloud, and Microsoft Azure.

Challenge 2: How do I secure my products so they are not replaced by unauthorized copies?

Don't want your products replaced by imitations? Then make sure your competitors can't easily clone your device. To do this, you need to ensure that the products you sell contain proprietary features that only your organization can provide.

Global supply chains now require increased diligence and enhanced security to ensure product integrity and authenticity are maintained during manufacturing and production.

One way to do this is through secure manufacturing, which mitigates risk to intellectual property and maintains the integrity of production processes. The Synergy Secure Boot Manager provides a secure firmware flash programming solution that enables developers to dependably and securely program authorized firmware into Synergy MCU flash memory devices in remote manufacturing facilities. This protects the firmware from being pirated, modified, or installed on cloned hardware.

The Synergy Secure Boot Manager also delivers a strong root-of-trust that provides unique identities, hardware-protected keys, secure boot loader, secure flash update module, and cryptographic APIs to interface with the MCU hardware. Through a secure connection, the root-of-trust is pre-loaded into a high-volume programmer system designed for the manufacturing and provisioning of processing units. The provisioned chip stores the data securely and maintains tight control on how it is used.

Renesas Synergy Secure Boot Manager

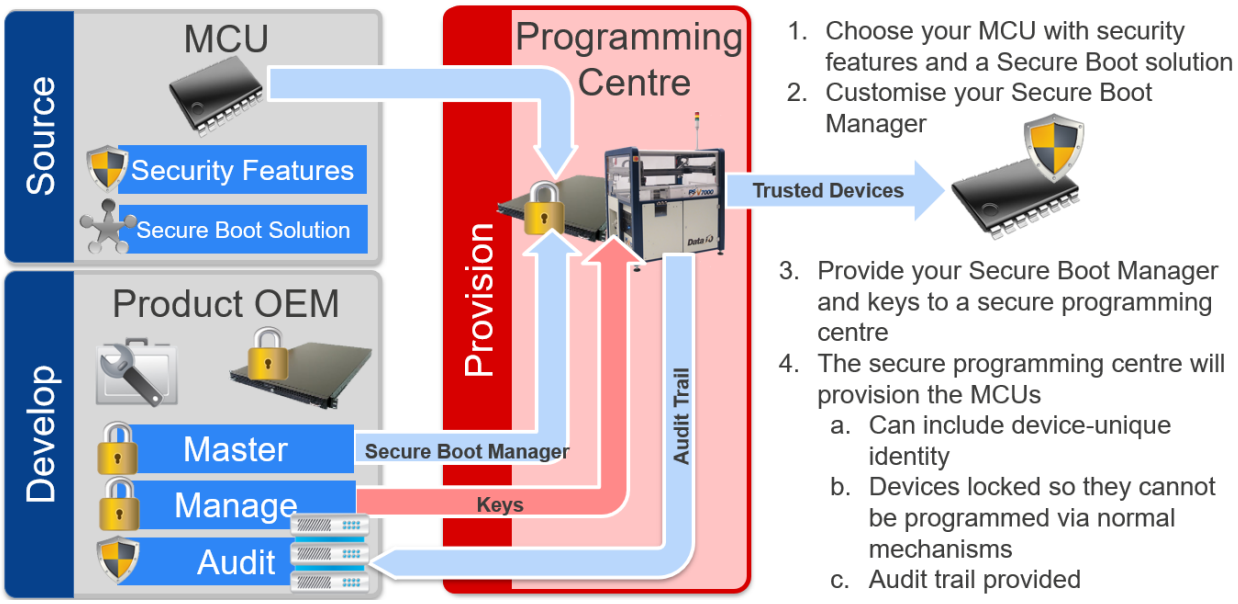

Figure 2: Renesas Synergy Secure Boot Manager provides a secure firmware flash programming solution (source Renesas Electronics Corp.)

Once products are in the field, the secure boot manager can securely update authorized firmware to the Synergy MCUs' flash memory with the on-chip root-of-trust validating and decrypting the firmware before flash

programming – all securely provisioned via secure cloud infrastructure made more reliable and trustworthy with Renesas cloud connectivity solutions.

Or, if you prefer, select Renesas partners can assist with secure provisioning and programming of solutions and services, and are committed to providing manufacturing security at a reasonable cost.

Challenge 3: How can I manage security with less complexity?

Designing in-depth, layered security for embedded designs can be challenging and time-consuming, and one way to reduce the learning curve is to ensure that the latest security advances and protocols are already built-in to the development platform. With the Synergy platform, developers don't have to learn all new and relevant protocols and other security safeguards to produce a secure application.

The Synergy Software Package simplifies complex functions encountered while developing secure connected embedded systems. The software secures areas of memory where developers can create and store portions of code that are Flash and SRAM read- and write-protected. Doing so allows developers to create customizable areas of memory that can be used to store temporal keys, private keys, and other sensitive data.

The Synergy platform supports both public key infrastructure (PKI), a cryptography methodology that offers authentication via digital certificates, and pre-shared key (PSK), an encryption model in which authentication is authorized when both peers in a digital connection specify the same key. PSK offers a simpler form of encryption and may provide appropriate levels of protection for situations such as access control for small numbers of users. Though more complex to initiate and manage, PKI is a form of asymmetric cryptography that can authenticate users, produce and distribute certificates, and maintain, manage, and revoke certificates. PKI, with public and private keys, is usually considered a more secure encryption model and is commonly used for authentication in large encryption systems.

The Synergy platform offers optimized commercial-grade software with standard APIs that simplify how interfaces are made with hardware security and encryption features. Application frameworks help streamline otherwise tricky wireless driver integration with a uniform interface between the application code and lower level drivers. This level of abstraction decreases complexity and makes it easier to integrate networking stacks, or to switch out or drop in drivers as needed.

Challenge 4: How do I secure my device against multiple security threats?

Today's cyberthreat landscape is filled with multiple bad actors and risks. Exploits and attack vectors await the unprepared and unprotected. To safeguard a device against multiple security threats requires securing the device's identity through hardware-based key generation. This identity can be securely stored in internal flash and leveraged to create trust, and provide privacy when added to designs and configured for target applications.

Establishing a strong device identity allows every IoT device to be singularly identified and authenticated as unique. This enables devices to be individually secured and to engage in encrypted communication with other secured devices and services. Strong device identity safeguards against multiple security threats through layered IoT security protections by providing the following features:

- **Trust.** Once connected to a network, the device must authenticate to create trust between other devices, services and users so that it can securely exchange encrypted data and information. Trust starts with properly authenticating the device to ensure it is a legitimate device and not a counterfeit.

- **Privacy.** The data and information captured and shared within IoT networks often includes data that is sensitive, personal or financial, which must be kept private and secure to meet regulatory compliance. Secured device identity provides the keystone to ensure confidentiality when IoT devices and systems connect to share data.

- **Integrity.** Ensuring that data shared within networks has not been altered is a key element of layered security. Data integrity is an often-overlooked requirement, but connected devices and systems rely on authenticity (trust), confidentiality (privacy), and integrity of the information being transmitted.

Renesas Synergy MCU SCE Hardware Security Features by Series

	Functions		Key Wrap	NIST CAVP	S7	S5	S3	S1
Identity & Key Exchange (Asymmetric)	RSA	Key Generation, Sign/Verify[1]	Y	Y[5]	1024/2048/4096	1024/2048/4096		
	ECC[4]	Key Generation, ECDSA, ECDH[2]	Y	WIP	NIST P192/P224/P256/P384	NIST P192/P224/P256/P384		
	DSA	Sign/Verify			L:2048/1024, N:256/226/160	L:2048/1024, N:256/226/160		
Privacy (Symmetric)	AES	ECB, CBC, CTR	Y	Y	128/192/256	128/192/256	128/256	128/256
		GCM		Y	128/192/256	128/192/256	128/256	
		XTS, CCM			128/256	128/256	128/256	
	3DES	ECB			192	192		
		CBC			192	192		
		CTR			192	192		
Data Integrity	Hash	GHASH		Y	Y	Y	Y	
		SHA1/224/256		Y	Y	Y		
	TRNG	Hardware Entropy with DRBG-AES-128		Y	Y	Y	Y	Y
Data Protection	Unique ID				Y	Y	Y	Y
	MPU	Arm, Bus Master, Bus Slave			Y	Y	Y	Y
	MPU	Security				Y	Y	Y[3]
	FAW	Program/erase protection			Y	Y	Y	Y
	SCE	Crypto module			SCE7	SCE7	SCE5	
	SCE	Key Installation and Key Wrapping			Y	Y	Y	

[1] 4096 bits Verify, Encrypt only
[2] Via Scalar Multiplication
[3] Not available on the S124
[4] SSP v1.5.0 required for low-level drivers
[5] SSP v1.6.0 required for low-level drivers

Figure 3: Renesas Synergy MCUs as available in the Synergy platform (source Renesas Electronics Corp.)

Digital data security is also a top priority for safeguarding against multiple security threats. Data at rest refers to data not actively in motion between devices or networks, usually parked in SRAM or non-volatile storage. To secure data at rest, Synergy MCUs offer data access controls, including read, write, read-write and write-once protections. Controlling access to stored data reduces the attack surface and increases system security.

In addition, Synergy MCUs deployed in the field can be updated remotely to provide protection against the latest cyber threats.

Challenge 5: I'm not a security expert, but I need a secure product. What do I need to know?

To deliver comprehensive, in-depth security protection for products based on embedded devices requires a highly integrated, optimized platform with multiple protocols and safeguards that work together to provide security at many levels.

The Renesas Synergy platform offers developers a head start by delivering a complete development environment that provides a unique, built-in set of hardware and software security capabilities. These build on a shared root of trust that meets the requirements of securing embedded devices and IoT networks. The platform also extends the ability to ensure secure, scalable manufacturing and protection of intellectual property.

Developers can also take advantage of Renesas' online library of application projects for step-by-step instructions and guidance on building end-to-end security solutions.

In addition, basing your designs on the Synergy platform gives you the support of the large, robust Renesas community and ecosystem of alliance partners. The Renesas network of trained and certified design service partners are available to support every stage in your design cycle, working with you to achieve your design and business goals. Leveraging Renesas partners can help speed development and extend deep expertise into your security solution development.

Challenge 6: How can I get more standardization and support for security from vendors and put my own resources on the parts of the design that differentiate?

Before you begin development, make sure to select an MCU solution that provides a highly integrated platform of functionalities that work together to deliver security at multiple levels. Malicious agents can take advantage of vulnerabilities in embedded designs when variations in design and security protocols create weak points that hackers can infiltrate. This is particularly a risk when MCU hardware, software, communication stacks, and drivers have not been standardized into a fully integrated framework.

A comprehensive, fully integrated development platform with in-depth security protections makes securing your design as simple and painless as possible. Pick a framework that is pre-integrated with key software, functionalities, stacks, and drivers already incorporated into the platform. This frees developers from dealing with lower-level integrations, allowing them to focus on designing the features and capabilities that will make their product stand out.

In addition, confirm that your solution provider has an active, comprehensive partner ecosystem. The option of outsourcing development of specific security features or functionalities to trusted experts can save time and strengthen your final product.

The Renesas Synergy platform is a comprehensive, qualified development platform that includes production-grade software, a scalable family of pin-compatible MCUs, application frameworks, functional libraries, HAL drivers, and advanced software tools and kits. It ensures that applications are built on a secure, robust technology foundation. In-depth, layered security is built in, and each device can be uniquely identified and authenticated to ensure secure communication between other devices, services and users.

With Renesas, security is built into the platform, enabling designers to focus their time and skills on higher-level challenges and innovation that address fast-moving IoT market opportunities and consumer demands. Since

everything has been pre-integrated, tested, and qualified by Renesas, engineering teams can begin application software development at the API level, saving months of time and effort.

Developers can also count on the expertise of Renesas partners, who are available to step in and help development of specific security features or functionalities, to support your existing team or to add valuable skills and experience to your development processes.

Conclusion

Renesas helps embedded developers meet the challenges of securing designs by offering a platform-based approach to security that takes advantage of the latest breakthroughs in hardware and software security to deliver in-depth, comprehensive protections with multiple layers of security. The Renesas Synergy Platform builds on a shared root of trust to secure IoT devices, services, and networks at a deep level extended to ensure secure and scalable manufacturing and protection of intellectual property across the product lifecycle.