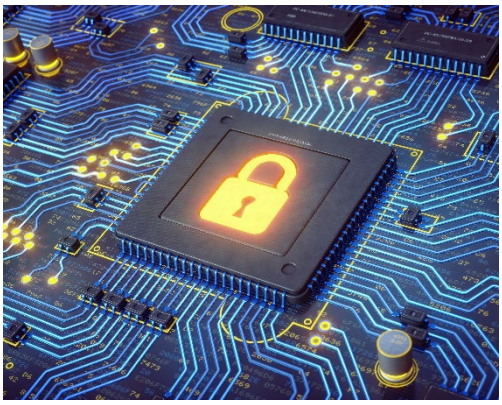
Solving IoT Security Issues with Embedded Microcontrollers

IoT security can be addressed with embedded microcontroller units (MCUs).



The Internet of Things (IoT) is no longer a buzzword. Instead, it has become an integral part of our lives. Every sector, from healthcare to manufacturing, uses IoT devices. However, while the total number of devices has been forecasted to reach 83 billion by 2024 [1], the security of these devices remains a significant concern. Without proper security measures, any connected IoT device is vulnerable to a breach, function loss, or hacking to steal user data or manipulate the system. This article examines how IoT security can be addressed with embedded microcontroller units (MCUs).

IoT Security Issues

A core part of the IoT is the connectivity to a network. Through this link, some 1.51 billion breaches of IoT devices took place from January to June 2020 [4]. To combat this, researchers of embedded systems are investigating how to address vulnerabilities of network links. These efforts have resulted in recent security advancements in embedded MCUs.

With improved processing on the edge (locally), embedded cryptography, and internet protocol (IP) security, embedded IoT security is helping to protect cloud processing through a network link. This is how IoT security issues are being tackled with embedded MCUs.

Need for IoT Security

As the number of connected IoT devices (nodes) increases, network vulnerability escalates because every node can be a potential entry point for a cyber-attack. Once a vulnerable node is compromised, it can be a link to other nodes, leading to ruinous effects, ranging from minor data breaches to catastrophic information leaks. Infrastructure damage can also occur, resulting in network disruptions and loss of valuable services.

Unfortunately, IoT devices do not have a one-size-fits-all solution to their security problems because of the wide variety of hardware and operating systems, and hackers continue exploiting connected devices.

However, to understand why IoT security has become paramount, we need a brief overview of possible IoT flaws and their devastating effects. One example we can all relate to is a fitness tracker. Fitness trackers are designed to measure body parameters to assess the user's health and fitness via cloud-based services. This sensitive information could be misused by third parties not at all interested in health improvement. In fact, users are increasingly concerned about their personal data, and, as a result, this kind of data is protected by privacy protection laws worldwide. Security-focused MCUs can help to protect data transmission against eavesdropping by unauthorized parties.

Challenges Addressed by MCUs

To tackle IoT security threats, specific features can be included in embedded MCUs. In particular, embedded MCUs need to address the following challenges for a secure IoT device:

- Protection of confidential software and data, such as intellectual property and device identity
- Protection of data integrity to safeguard reliable data transmission
- Provision of a robust foundation (root-of-trust) and a local cryptographic toolkit
- Secured end-to-end communication channels

How can Microcontrollers Solve IoT Security Problems?

To achieve IoT device security, MCUs comprise both hardware-based security and software mechanisms. Security-focused MCUs need to provide a cryptographic toolkit for the complete chain of security, including a hardware-based root-of-trust, true random number generation functionality in hardware, and user-code authentication.

Descriptions of processes that can be implemented on MCUs to improve IoT security are as follows:

Hardware-based security

For secure IoT applications, a hardware-based approach is preferred as it offers an immutable root-of-trust for the IoT device and integrated storage. In addition, it consumes less power than its software equivalent. Hardware-based security uses integrated circuitry to secure the IP and protect the system. For this reason, MCUs for IoT applications have sophisticated integrated hardware security features, such as cryptography blocks, code protection IP, and other hardware-based mechanisms.

Secure key storage

By nature, external memory is vulnerable to attackers wanting to exploit internal functions and confidential data. As a result, plaintext keys require protection from physical and logical attacks. A security-focused MCU offers an integrated flash memory that encrypts data within a secure processing environment, binding the key to only this MCU. In other words, immutable device identity and cryptographic keys are used for device authentication and data encryption. In particular, integrated secure memory is an effective countermeasure against identity spoofing and device cloning.

True random number generation

A true random number generation block obtains a number that is statistically random and based on some physical random variation that cannot be duplicated by rerunning the process. It is an essential cryptographic function required for many security mechanisms and protocols.

Symmetric key encryption and decryption

For a symmetric key cryptographic algorithm, such as the AES (Advanced Encryption Standard), the same key is used for encryption and decryption, called a secret, or private, key[6]. Compared to the asymmetric approach, symmetric ciphers are faster because their keys are significantly shorter and only one is required for the process. However, secure key management is a problem since the secret key is necessary for deciphering, creating vulnerabilities whenever the key is shared.

Asymmetric cryptography

To better secure the management of cryptographic keys, an asymmetric cipher scheme uses a pair of keys instead of one secret key for both sides – a public key and a private key. The public key used for encryption can be openly distributed without compromising security, and the private key is kept secret by the recipient needing to decrypt a confidential message. This way, key distribution and storage are easier to handle securely than with symmetric ciphers. While asymmetric ciphers are much slower, security-focused MCUs outperform software-only solutions by integrating various technologies, including crypto accelerators, secure key storage, and unique, immutable chip identifiers.

Hash algorithms

A secure hash algorithm (SHA) uses cryptographic functions to condense a dataset to render it unreadable by others. Essentially, a hash is a fingerprint of the original data. An SHA is not reversible, unlike encryption. In addition to this security, if the data are compromised, the hash value will change at the recipient's end, providing evidence of an attack. As an example, hash algorithms are often used for digital signatures.

Digital signatures

Public-key cryptography and hash algorithms are the main ingredients for digital signatures, which authenticate online communication among partners and maintain data integrity, e.g., when confidential messages are transmitted via public networks. Digital signatures are built on certificates for user public keys issued by a trusted third party, i.e., a public-key infrastructure (PKI) offered as a cloud service.

Renesas Microcontrollers

One company contributing to the secure embedded microcontroller revolution is Renesas. Renesas offers a multi-tiered development infrastructure that provides security protection for various embedded products at multiple levels [2].

With deep insights and an understanding of the need for improved security, Renesas has doubled down on privacy through advanced MCU technologies, including cryptography. Each Renesas Advanced (RA) Family MCU contains a Secure Crypto Engine (SCE), an integrated crypto subsystem that provides hardware acceleration for the most prevalently used cryptographic algorithms, key generation, and a true random number generator. Renesas binds encrypted keys to a specific MCU, so they are accessible only within the SCE module on the individual MCU that performed key-wrapping. The SCE contains dedicated RAM, which enforces the privacy of plaintext keys by not exposing them to any CPU-accessible bus.

Renesas's RA Family MCUs provide a flexible platform combining Arm Cortex-M cores with the company's embedded system peripheral IP. In addition, the RA Family's Flexible Software Package provides optimized HAL (hardware abstraction layer) drivers and a baseline software platform built on FreeRTOS and associated middleware. This option gives designers the flexibility to integrate their middleware and libraries of choice.

These new developments have expanded Renesas's portfolio, providing state-of-the-art technology, including MCUs and system-on-chip (SoC) products [5], for a more secure world.

Conclusion

With IoT devices flooding the market faster than their vulnerabilities can be identified, security-focused MCUs offer a viable path for confronting cyber threats on multiple fronts. They present a simplified solution with a security design ecosystem to facilitate point-and-click development environments. These specialized MCUs also reduce the cost overhead and power consumption, two primary considerations in the highly constrained IoT designs.

Trusted and reliable data exchange are prerequisites for most IoT use cases. Hence, this calls for improved security in technology as new products are constantly being rolled out every day, especially in the IoT and embedded microcontroller industry.

References

1. Smith Sam. IoT Connections to reach 83 billion by 2024 driven by maturing industrial use cases [Internet]. 2020 [cited 2022, April 17]. Available from: https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024

2. Renesas. How to solve the 6 top security challenges of embedded IoT design. [Internet]. 2019 [cited 2022, April 17]. Available from: https://www.renesas.com/us/en/document/whp/how-solve-6-top-security-challenges-embedded-iot-design?language=en#:~:text=In%20Renesas%20MCUs%2C%20a%20flexible,devices%20in%20remote%20manufacturing%20facilities

3. Shea Sharon. IoT security (internet of things security). [Internet]. 2022 [cited 2022, April 17]. Available from: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security

4. IoT Cyberattacks Escalate in 2021, According to Kaspersky [Internet]. 2021 [cited 2022, May 1]. Available from: https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

5. Renesas & dialog semiconductors join forces to advance global leadership in embedded solutions. [Internet]. 2021 [cited 2022, May 2]. https://www.gsaglobal.org/renesas-dialog-semiconductor-join-forces-to-advance-global-leadership-in-embedded-solutions/

6. Secret Key. [Internet]. [cited 2022, September 19]. Available from: https://www.techopedia.com/definition/24865/secret-key

(Rev.1.0 Mar 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu, Koto-ku, Tokyo 135-0061, Japan
https://www.renesas.com

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
https://www.renesas.com/contact-us

Trademarks

Doc Number: R01WP0014EU0100