Overview of Information Security and Assurance Considerations for Micro Controller Integration

James Burrell,
Ph.D.
Boston College
Boston, MA USA

Abstract - **The advancement of small-scale computing has enabled the integration of highly efficient microcontroller device integration into consumer, medical, automotive, and industrial devices. The miniaturized form factor, reduced resource specifications, and network connectivity of these devices are optimal for the unique requirements of embedded electronic sensors, industrial control systems, and Internet of Things applications. The direct physical accessibility and network enabled connectivity combined with reduced power, processing, and memory characteristics of these devices increases the physical and cyber security attack surfaces which complicate information security and risk management. This review article provides an evaluative summary of physical and cyber security risk, impact, and mitigation considerations associated with the integration of microcontroller devices into information and operational technology networks.**

***Keywords*—microconroller; embedded system; information security; information assurance; risk management**

I. INTRODUCTION

A microcontroller is a small-scale programmable computer device that provides a low-cost alternative to general purpose computers for embedded system applications. A microcontroller, also known as a microcontroller unit (MCU), is typically manufactured as a single silicon chip that contains a central processing unit (CPU), program memory, system memory, and input/output (I/O) functionality (Figure 1).

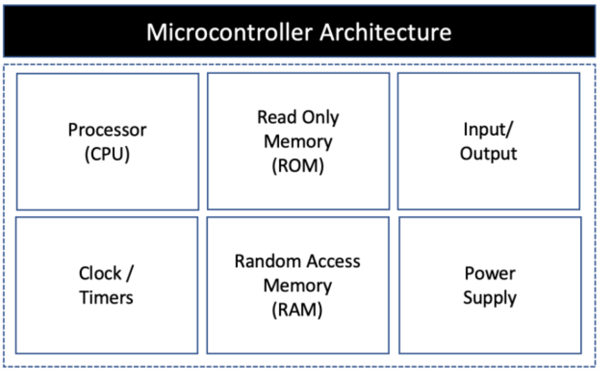


Figure 1. Basic Microcontroller Architecture Diagram.

The TMS1000 was the first commercial general-purpose microcontroller introduced in 1974 by Texas Instruments that was based on metal–oxide–semiconductor technology [1]. The Texas Instrument TMS1000 was a 4-bit microprocessor with a system clock, read only memory (1,000 bytes), and random-access memory (256 bytes) storage [2]. Microcontroller technology has advanced considerably and MCUs are available in 8, 16, and 32-bit architectures that provide low-cost integrated programmable chip alternatives to address a wide array of embedded system applications and requirements. As an example, the STMicroelectronics STM23 represents a high-performance line of MCUs that includes a 32-bit 100 MHz processor, floating point unit (FPU), memory protection unit (MPU), 128 KB flash memory, 32 KB static memory, 12-bit analog to digital (ADC) and digital to analog (DAC) converters, timers, and advanced communication interfaces [3]. The current market trend for microcontrollers is projected to exceed $51 billion in 2028 with primary markets identified as portable medical devices and advanced driver assistant systems (ADAS) [4]. The miniaturized form factor, low cost, diverse architecture, and analog and digital electronic interface compatibility with sensors and controls for industrial controls systems (ICS), Industrial Internet of Things (IIoT), Internet of Medical Things (IoMT), unmanned aerial system (UAS), and other applications. The rapid integration and adoption of IoT and other devices with embedded MCUs has resulted in concerns specifically related to the hardware and software security of these devices. General purpose MCUs are not designed to support high-security applications based on the limited resource characteristics of small-scale computing devices.

The distinctions between MCU-based configurations for ICS and IoT are becoming less defined with increasing similarities related to security and privacy requirements. The importance of information security and assurance is recognized as an essential requirement for the safe, reliable, and efficient operation of computing devices. In some instances, these embedded devices are considered discrete electronic devices without sufficient awareness of security and privacy implications. This is especially relevant when devices process and store sensitive data or control cyber-physical systems where security deficiencies could result in a compromise or failure of the device or associated control system. The three fundamental principles of information security are recognized as confidentiality, integrity, and availability (CIA) which provides a method of evaluating separate categories that in combination provide a comprehensive view of cybersecurity (Table 1).

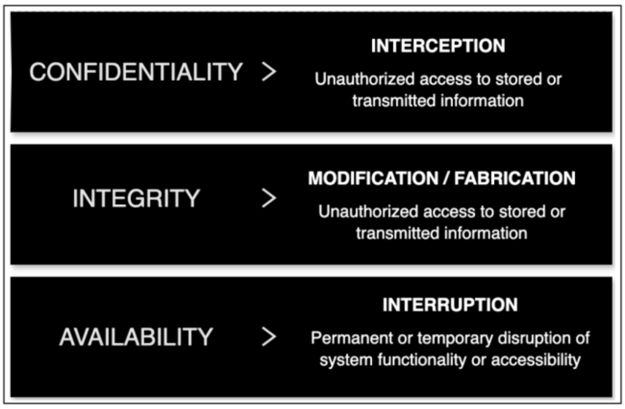
Table 1. Summary of the Information Assurance (IA) Principles.

Term	Definition
Confidentiality	Prevent unauthorized access to systems or disclosure of data.
Integrity	Prevent alteration, substitution, or damage to systems or data.
Availability	Provide continuous authorized access to systems or data.

The primary focus of information security and assurance risk assessments have been for information technology (IT) systems and networks used to process, store and transmit sensitive business, financial, and personal information. Microcontrollers and embedded systems are increasingly being integrated into both the IT and operational technology (OT) environments with design characteristics that increases the complexity for existing security and enterprise risk models designed for IT systems and architectures. The increase in the convergence of IT and OT systems has resulted in an expanding attack surface that includes the use of open-source software libraries with potential security issues during the product development process [5]. The number of cyberattacks on OT systems has been increasing and the complexity in securing these systems requires a focus on foundational security with risk-based approach using standardized controls, establishing clear roles and responsibilities, and rapid incident response capabilities [6]. The integration of MCU devices in IT and OT environments presents a complex challenge to maintain effectual levels of information security, assurance, and resilience. As a result, the identification and evaluation of potential vulnerabilities is necessary to maintain security, privacy, and safety for MCU devices, networks, and data within IT and OT environments.

II. EVALUATION OF INFORMATION SECURITY RISKS

The information security risks evaluated in this paper are categorized as interception, modification/fabrication, and interruption which describe the primary threats and vulnerabilities for MCUs and aligns with the CIA model (Figure 2).



CONFIDENTIALITY > **INTERCEPTION** Unauthorized access to stored or transmitted information

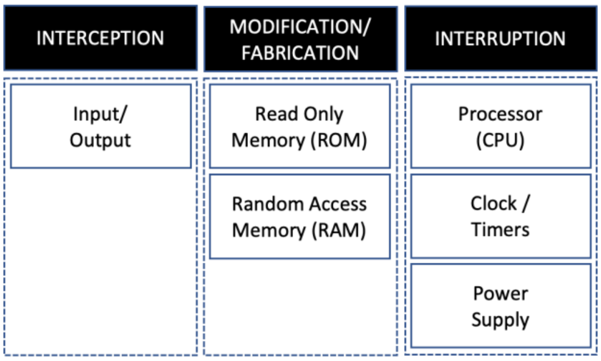
INTEGRITY > **MODIFICATION / FABRICATION** Unauthorized access to stored or transmitted information

AVAILABILITY > **INTERRUPTION** Permanent or temporary disruption of system functionality or accessibility

Figure 2. Selected Evaluative Information Security and Assurance Threat Categories.

These categories are recognized in information security risk management principles, to include cyber–physical systems, as cyber-attack methods [7]. For this evaluative summary, the modification and fabrication categories were combined based on similar definition and impact. The MCU components were aligned with the corresponding information security risk categories to evaluate selected cyber-attack methods and provide an overview of the cyber security threat landscape (Figure 3).

The most significant information security challenge relates to the physical accessibility of MCUs that are located and operated outside IT enterprise ecosystem [5][7][8]. Physical security has been a principal element of computer security since its inception that continues to represent a required knowledge and application domain for information security certifications. The concept of unrestricted access to a computing device and components requires physical hardening or security features to mitigate security vulnerabilities. The limited security specifications for general-purpose MCUs represent increased attack surfaces that effect the security of other IT systems and networks.



INTERCEPTION	MODIFICATION/ FABRICATION	INTERRUPTION
Input/ Output	Read Only Memory (ROM)	Processor (CPU)
	Random Access Memory (RAM)	Clock / Timers
		Power Supply

Figure 3. Selected Information Security and Assurance Risk Categories for Microcontroller Devices.

A summary of the information security and assurance risks associated with interception, modification/fabrication, and interruption are presented to increase awareness associated with MCU devices in both OT and IT environments.

A. Interception

The concept of confidentiality provides a level of assurance that information is restricted and available to authorized trusted entities. The interception or unauthorized access to real-time communication or stored data represents a significant security and privacy risk, especially for sensitive information. The requirement to provide secure data services is an increasingly essential function for modern MCU applications which is complicated by physical and wireless communication functionality with analog/digital system connections and universal asynchronous receiver/transmitter (UART) interfaces.

Research has determined that insecure network services and transport encryption have been identified as primary vulnerabilities to communication security [9]. The exploitation of wired I/O or serial communication connections requires direct access to the device, physical media, or connected systems to intercept control and data transmissions. The ability to monitor, capture, and analyze data transmissions from MCUs provides the capability to recover sensitive data or acquire information that could be used to initiate replay type attacks that reduce the effectiveness of authentication methods. The increased integration of wireless long-range communication in certain MCUs has introduced additional vulnerabilities [10]. The majority of network-enabled microcontrollers utilize low power communication protocols that include Bluetooth Low-Energy (Bluetooth LE) and LoRa (LoRaWAN) to provide long-range wireless communication. The spread-spectrum modulation technique utilized by these wireless protocols distributes the transmitted energy over a wide bandwidth segment using pseudo-random code sequences as opposed to a single narrowband frequency. Despite the signal characteristics of spread spectrum communication systems there are additional measures required to provide adequate security for the transmission of sensitive data. As an example, security researchers have demonstrated the vulnerabilities and susceptibility of LoRa and LoRaWAN to attack methods used for the recovery of message data despite the cryptographic security and message acknowledgement features specified in the protocol [11].

Encryption and authentication protocols are a primary method for securing the contents of data from unauthorized access and validating the identity of systems and networks. High-grade encryption methods generally require computationally intensive functions to perform encryption and decryption processes. The selection of a particular encryption algorithm or method involves an evaluation of a combination of factors that include an assessment of the required level of security, sensitivity of the data, and computational resource requirement for the encryption and decryption process. The incorporation of a separate co-processor is often used in microprocessor-based systems to reduce the impact of encryption computation on CPU performance. The limited power, processing, and memory capacity of general-purpose microcontrollers are typically insufficient to support high-grade encryption and decryption functions in addition to support secure encryption key generation and management. Certain communication protocols have embedded authentication methods for digital signature and certificate validation. Similar to encryption, the implementation of independent authentication methods requires additional computational, power consumption, and memory storage requirements.

The combination of properly implemented encryption, authentication, and secure communication protocols decrease interception vulnerabilities in MCUs when balanced with security requirements and available device resources.

B. Modification / Fabrication

The modification or fabrication of data or configuration information often involve integrity and code injection attacks. These attack methods impact MCU device integrity which could result in non-deterministic performance especially when performing artificial intelligence or other critical functions. There are also advanced adversarial attack methods that include replacement, reprogramming, and reconfiguration of the microcontroller using the Joint Test Access Group (JTAG) interface designed to provide accessibility to embedded systems. The ability to access or modify information contained in the program and system memory provides the ability to inspect and update firmware, algorithms, and security configurations. Advanced algorithm timing attacks and differential power analysis represent undetectable non-invasive analysis methods to monitor power consumption and information leakage analysis using side channel and other techniques have been successful in the recovery of secret key information [12].

Trusted execution environments (TEE) provide an increased level of assurance that reduces operating system integrity and configuration vulnerabilities. Advanced research on flash memory security is an example of the requirement to protect MCU components. A research study verified the ability to permanently change the contents of selected flash memory locations using a laser fault injection technique on memory contents during a read operation that modified the stored password to a predefined logic value and circumventing the login attempt countermeasures [13]. The implementation of hardware security architecture provides a base level layer of security to protect sensitive data, programming, and configuration information against software layer manipulation. There are MCUs with an embedded trusted platform module (TPM) as an embedded chip component or specialized microcontroller that provides hardware and software verification for boot and execution processes in addition to security certificates and credentials [14]. This level of protection is not commonly available in general purpose MCUs although microchip developers have introduced embedded and external hardware security module (HSM) and hardware security extensions (HSE) in the automotive sector to provide an enhanced level of security and safety.

Advancements in lightweight encryption research especially with block encryption methods provide end-to-end security for low-power devices. The block size, encryption key size, and number of iterations impact the computational requirements during the encryption and decryption processes. A study was conducted to evaluate ten lightweight block ciphers using two microcontroller boards. The evaluation of memory usage, energy consumption, throughput, and execution time which demonstrated an increase in usage and performance that corresponded with increased payload size that ranged from 16 to 2,048 bytes [15]. This research confirmed the value of assessing the sensitivity of the data and the selection of cryptographic parameters can often provide adequate security for resource constrained MCUs and other embedded devices.

C. Interruption

The interruption of MSU operation represents an unintentional or intentional failure condition primarily attributed to the power source, communications connectivity, or device failure conditions. The MCU I/O ports and control lines are vulnerable to direct manipulation and disconnecting the power source or I/O connections to a MCUs can disrupt the operation of cyber-physical or other critical systems that have financial, productivity, and safety impacts.

Denial of service (DoS) and distributed denial of service (DDoS) are attack methods that degrade computational and network services to prevent authorized accessibility to a system. This activity typically involves traffic from one or more computer systems directed to a target computing device to disrupt normal functionality for a short or extended period of time. A DoS or DDoS is an effective method of attack against network enabled MCUs without compensatory information security protection. In addition, unshielded MCUs and control lines are also susceptible to electromagnetic interference (EMI) and radio frequency (RFI) where intentional or unintentional EMI or RFI injection could introduce wired and wireless device and communication failures between connected equipment, and cloud aggregation sites.

III. MICROCONTROLLER SECURITY CONSIDERATIONS

As previously acknowledged, there are an expanding number of commercially available microcontrollers and applications in multiple sectors and operating environments. The recent adoption of electronic devices in an IT environment, with embedded network enabled microcontrollers, present information security risks that are considerably different than encountered with modern IT computers and peripherals. It is also recognized that the most effective measure to prevent or reduce the impact of a cyber-attack or compromise of a MCU device is rapid detection which represents a distinct challenge for device-based detection and requires the reliance on compensatory controls [16]. There is also current research being conducted to explore the use of machine learning to improve DDoS detection methods on IoT devices [17].

A selection of potential considerations is presented to assist with the evaluation and potential risk assessments to inform strategic technology investment, integration, and replacement strategies involving MCU technologies and devices.

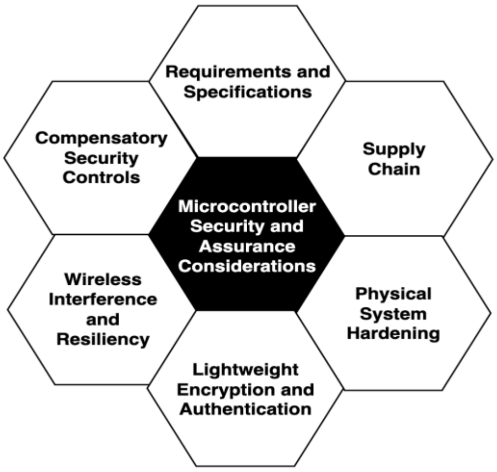

Requirements and Specifications
Compensatory Security Controls
Supply Chain
Microcontroller Security and Assurance Considerations
Wireless Interference and Resiliency
Physical System Hardening
Lightweight Encryption and Authentication

Figure 4. Selected Microcontroller Security and Assurance Considerations.

A. Microcontroller Requirements and Specifications

A key consideration for the evaluative process involves the review of requirements and the specifications for current microcontrollers applications. This review should include considerations if current or selected MCU could be upgraded or replaced by more powerful microprocessors that provide advanced processing capacity in addition to encryption, authentication, and other security resources. In circumstances where operational and infrastructure permit, the selection of secure microcontrollers may provide an optimal solution to achieve the balance of operating efficiency and security. Secure microcontrollers offer a single device solution for trusted execution, encrypted storage, secure software updates, and secure communication protocols [18]. There are also innovations in emerging MCU technologies that provide energy-efficient encryption for small-scale devices that reduces power consumption of public-key encryption by 99.75 percent with a 500 time increase in speed [19].

B. Supply Chain

The vulnerabilities associated with a global supply chain introduces potential risk for product development and deployment in IT and OT environments and highlights the importance of establishing a trusted supplier network. Supply chain attacks have a potential impact on the hardware and software security that involve manufacturers, suppliers, service providers, and owners [5]. The risks become increasingly less obvious when microcontrollers are incorporated into end user systems and products. The ability to detect supply chain vulnerabilities is complex and requires the analysis of hardware and firmware components which can be difficult for embedded MCU applications. The potential implications of supply chain vulnerabilities or compromise include replacement and modification of original components that impact quality, reliability, and security. The U.S. Presidential Executive Order for Improving the Nation's Cybersecurity enacted in 2021 addressed the vulnerabilities that exist in the global software supply chain and requires software developed for the federal government to include a software bill of materials (SBOM) [20]. The ability to apply SBOM to embedded systems has resulted in complexities with the identification of physical hardware components, manufacturers, configurations, firmware versions, and the auto generation of embedded code [21].

C. Physical Access and System Hardenings

Physical accessibility is the most significant risk to MCUs and connected systems. The scope of physical threats to these systems includes destruction, deactivation, replacement, and reconfiguration. Physical access may be mitigated in certain circumstances with the use of tamper resistant hardware modules. MCU system operation dependencies represent another category of vulnerabilities. As an example, the integration of an alternative power source to include photovoltaic or kinetic energy generation could mitigate primary power source interruptions. Advanced research has identified methods to harvest high-energy electromagnetic waves to power small electronic devices which could represent a possible option to mitigate this risk and maintain an increased level of resilience [22].

D. Lightweight Encryption and Authentication

The development of lightweight encryption and authentication protocols provide an enhanced level of data security while minimizing the impact on limited device resources. The U.S. National Institute of Standards and Technology (NIST) has examined the requirements and use cases for lightweight cryptography, which include an evaluation of candidate cryptographic systems, on the basis of security, costs, and performance. Current research includes a broad range of methods and techniques for implementing lightweight encryption algorithms. The U.S. National Institute of Standards and Technology (NIST) Lightweight Cryptography Project has been evaluating requirements and use cases for lightweight cryptography, which include an evaluation of candidate cryptographic systems, on the basis of security, costs, and performance. In February 2023, an algorithm was selected for that demonstrated NIST standard performance advantages on various target platforms without introducing security concerns [23]. There have also been advancements in lightweight message authentication that provide options to protect against interception and integrity that support different message lengths and keys sizes with power, memory, and execution efficiencies [24].

E. Wireless Communication Interference and Resiliency

The low-power signals utilized for LoRa, Bluetooth, and Bluetooth LE are susceptible to interference methods despite the use of spread spectrum signal modulation. Practical low cost LoRaWAN interference devices have been constructed from electronic components that are capable of disabling communications from MCUs located in the covered signal area [25]. A mesh network infrastructure can provide network resiliency in a limited coverage area or environment with device-to-device configurations that extends the effective communication distance with limited transmission power and power consumption. Accordingly, an upgrade to a Wi-Fi or 5G cellular enabled MCU may provide increased reliability and communications for critical systems.

F. Compensatory Security Controls

The physical accessibility of microcontroller devices combined with the lack of security controls represent considerable threats that are not commonly associated with other small scale computing devices. In instances where critical information security risks are unable to be mitigated with physical hardening or hardware-based security, the consideration of compensatory controls is recommended to enhance MCU security. Certain types of controls are conventionally present in enterprise networks and may meet the requirements for MCU security in IT environments. The use of simulation technology, data integrity checks, access control, and audit functions may provide organizations with early detection and the ability to rapidly respond to MCU information security incidents.

IV. CONCLUSION

A comprehensive inventory and assessment of the type, specification, configuration, and location of MCUs and enabled devices will assist with the identification of factors that impact the reliability, safety, and resilience of embedded systems. Increased awareness and consideration must also be provided for small-scale computing device integration that result in the introduction of microcontrollers into IT and OT environments. The success of any of these attack methods or conditions has the ability to disrupt the operation of the MCU and introduce cascading failures of critical systems and networks that could create hazardous and dangerous conditions especially for healthcare, environmental, and critical infrastructure conditions. The identified security risks associated with interception, modification/fabrication, and interruption that are unable to be mitigated due to limitations of the MCU should be evaluated and proportional security methods or hardware-based compensatory controls be implemented to address the unique security requirements of MCUs in enterprise IT and OT environments. Information security risk assessment, governance, and policies are essential components of an enterprise risk management. A comprehensive MCU security plan that involves strategic technology selection, IT governance, and policies are required to create an effective process to mitigate potential cybersecurity incidents.

REFERENCES

[1] K. R. Raghunathan, “History of Microcontrollers: First 50 Years,” IEEE Micro, vol. 41, no. 6, pp. 97–104, Nov. 2021, doi: 10.1109/MM.2021.3114754.

[2] M. Jiménez, R. Palomera, and I. Couvertier, Introduction to Embedded Systems: Using Microcontrollers and the MSP430. New York, NY: Springer New York, 2014. doi: 10.1007/978-1-4614-3143-5.

[3] STMicroelectronics, “STM32F410CB - STM32 Dynamic Efficiency MCU with BAM, High-performance and DSP with FPU, Arm Cortex-M4 MCU with 128 Kbytes of Flash memory, 100 MHz CPU, Art Accelerator -STMicroelectronics.” Available:https://www.st.com/en/microcontrollers-microprocessors/stm32f410cb.html.2024.10444344.

[4] Fortune Business Insights, “Microcontroller Market Size & Share Report [2021-2028].” Available: https://www.fortunebusinessinsights.com/microcontroller-market-106430

[5] K. Townsend, “Cyber Insights 2023 | ICS and Operational Technology,” SecurityWeek. Available: https://www.securityweek.com/cyber-insights-2023-ics-and-operational-technology/

[6] A. Alissa et al., “Enhancing Operational Technology (OT) cybersecurity | McKinsey.” Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/how-to-enhance-the-cybersecurity-of-operational-technology-environments

[7] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, “A Survey on Cyber–Physical Systems Security,” IEEE Internet Things J., vol. 10, no. 24, pp. 21670–21686, Dec. 2023, doi: 10.1109/JIOT.2023.3289625.

[8] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security—A Survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.

[9] X. Jiang, M. Lora, and S. Chattopadhyay, “An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices,” ACM Trans. Internet Technol., vol. 20, no. 2, pp. 1–24, May 2020, doi: 10.1145/3379542.

[10] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, “Exploring the Security Vulnerabilities of LoRa,” in 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, United Kingdom: IEEE, Jun. 2017, pp. 1–6. doi: 10.1109/CYBConf.2017.7985777.

[11] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, “Security Vulnerabilities in LoRaWAN,” in 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, FL: IEEE, Apr. 2018, pp. 129–140. doi: 10.1109/IoTDI.2018.00022.

[12] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, “Introduction to differential power analysis,” J Cryptogr Eng, vol. 1, no. 1, pp. 5–27, Apr. 2011, doi: 10.1007/s13389-011-0006-y.

[13] R. Viera, J.-M. Dutertre, R. Silva Lima, M. Pommies, and A. Bertrand, “Tampering with the flash memory of microcontrollers: permanent fault injection via laser illumination during read operations,” J Cryptogr Eng, vol. 14, no. 2, pp. 207–221, Jun. 2024, doi: 10.1007/s13389-023-00335-z.

[14] Intel Corporation, “Trusted Platform Module (TPM) Overview,” Intel. Available:https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/trusted-platform-module.html

[15] P. Panahi, C. Bayılmış, U. Çavuşoğlu, and S. Kaçar, “Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications,” Arab J Sci Eng, vol. 46, no. 4, pp. 4015–4037, Apr. 2021, doi: 10.1007/s13369-021-05358-4.

[16] O. Tushkanova, D. Levshun, A. Branitskiy, E. Fedorchenko, E. Novikova, and I. Kotenko, “Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation.,” Algorithms, vol. 16, no. 2, p. NA-NA, Feb. 2023, doi: 10.3390/a16020085.

[17] J. Mwaura, S. Araki, and K. Kakizaki, “A Study on DDoS Attacks Detection on IoT Devices Using Machine Learning for Microcontrollers,” in 2024 IEEE International Conference on Consumer Electronics (ICCE), Jan. 2024, pp. 1–4. doi: 10.1109/ICCE59016

[18] M. Noseda, L. Zimmerli, T. Schläpfer, and A. Rüst, “Performance Analysis of Secure Elements for IoT,” IoT, vol. 3, no. 1, Art. no. 1, Mar. 2022, doi: 10.3390/iot3010001.

[19] “Energy-efficient encryption for the internet of things,” MIT News | Massachusetts Institute of Technology. Available: https://news.mit.edu/2018/energy-efficient-encryption-internet-of-things-0213

[20] The White House, “Executive Order on Improving the Nation’s Cybersecurity,” The White House. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[21] T. Stalnaker, “SBOMS as a Solution in the Software Supply Chain,” 2024.

[22] “Energy-harvesting design aims to turn high-frequency electromagnetic waves into usable power,” Massachusetts Institute of Technology News. Available: https://news.mit.edu/2020/energy-harvesting-wi-fi-power-0327

[23] M. Sönmez Turan et al., “Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process,” National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8454, Jun. 2023. doi: 10.6028/NIST.IR.8454.

[24] G. Saldamli, L. Ertaul, and A. Shankaralingappa, “Analysis of Lightweight Message Authentication Codes for IoT Environments,” in 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Jun. 2019, pp. 235–240. doi: 10.1109/FMEC.2019.8795359.

[25] T. Perković, H. Rudeš, S. Damjanović, and A. Nakić, “Low-Cost Implementation of Reactive Jammer on LoRaWAN Network,” Electronics, vol. 10, no. 7, Art. no. 7, Jan. 2021, doi: 10.3390/electronics10070864.