DOI: https://doi.org/10.5281/zenodo.11109048

UDC: 004.735

HARDWARE AND SOFTWARE PROTECTION MEANS OF PROTECTION OF CYBER ATTACKS OF INTERNET OF THINGS DEVICES

Rakhimov Bakhtiyorjon Nematovich
Military Institute of Information and Communication Technologies and
Communications of the Ministry of Defense of the Republic of Uzbekistan,
chief, doctor of technical sciences, professor

Muradova Alevtina Aleksandrovna
TUIT named after Muhammad al-Khwarizmi, PhD, associate professor
a.muradova1982@inbox.ru

ANNOTATION

The article presents hardware and software protection against cyberattacks for Internet of Things devices. Methods of the Trusted Platform Module, hardware monitoring of microarchitecture and SIEM system events, architectures supporting ARM TrustZone and Intel Software Guard Extension (SGX), and a DDoS attack detection structure called BRAIN are presented. The detailed architecture of intrusion detection and prevention systems (IDS/IPS) is provided.

Keywords: *IoT, threats and vulnerabilities, cyber threats, DDoS attacks, Trusted Platform Module, cryptoprocessor, SIEM systems, BRAIN, IDS, IPS.*

АППАРАТНЫЕ И ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ КИБЕРАТАК УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

АННОТАЦИЯ

В статье представлены аппаратные и программные средства защиты от кибератак устройств интернета вещей. Представлены методы Trusted Platform Module, аппаратный мониторинг событий микроархитектуры и SIEM-системы, архитектуры с поддержкой ARM TrustZone и Intel Software Guard Extension (SGX), структура обнаружения DDoS-атак под названием BRAIN. Приведена подробная архитектура систем обнаружения и предотвращения вторжений (IDS/IPS).

Ключевые слова: *IoT, угрозы и уязвимости, киберугрозы, DDoS-атаки, Trusted Platform Module, криптопроцессор, SIEM-системы, BRAIN, IDS, IPS.*

Introduction. Internet of Things, IoT, Internet of Things - a network of electronic devices equipped with built-in technologies for interacting with each other and the external environment. Although IoT devices appear to be harmless, they are not without security and privacy concerns as there are many threats and vulnerabilities in the current IoT design [1].

IoT security vulnerabilities lead to countless threats and attacks that can potentially compromise critical infrastructure and even national security, cause physical and financial losses, and more. McAfee's Quarterly Cybersecurity Threat Report reports that 176 new cyber threats emerge every minute [2].

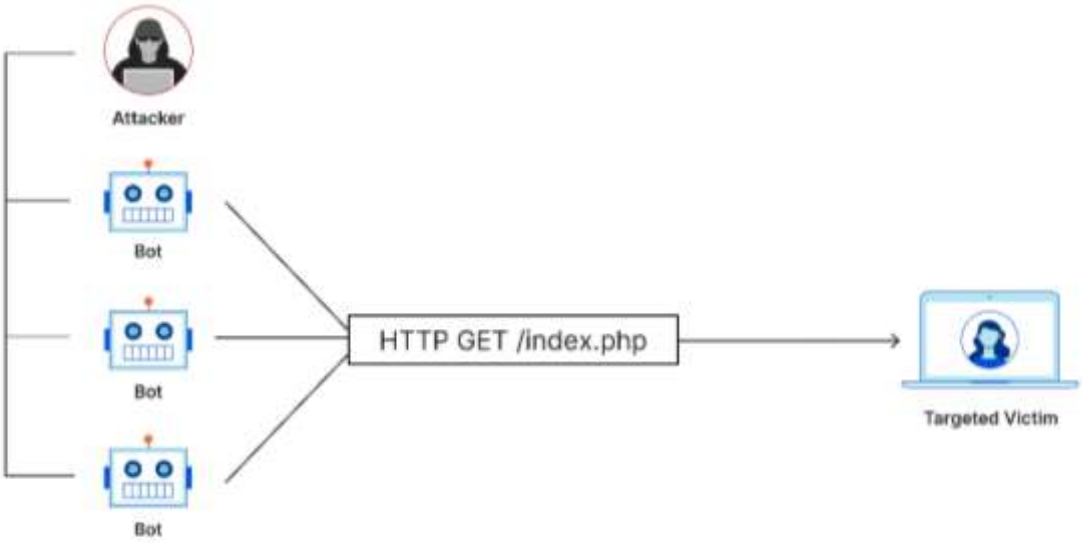

Fig. 1. Application layer attack example

Literature and methodology. Hardware security methods. Hardware security systems use hardware modules and can collect microarchitecture information to analyze prevailing threats and vulnerabilities at the software level. Hardware-based techniques provide a wide range of solutions for secure and reliable IoT applications [3]. One of the basic requirements for performing a secure information transaction between IoT devices over an untrusted network is the use of a reliable and secure key management and data processing scheme on the hardware. In this regard, the Trusted Platform Module (TPM is the name of the specification that describes the cryptoprocessor in which cryptographic keys are stored to protect information, as well as the general name of the implementations of the specified specification) have proven themselves well. Such TPMs allow the use of cryptographic keys that can be tied to specific platform parameters and protected from disclosure by any other untrusted hardware component, process, or software. ARM TrustZone and Intel Software Guard Extension (SGX)-enabled architectures add new functionality to modern system-on-a-chip SoCs, providing a reliable and secure environment for running security-critical processes, even though privileged kernel and software potentially harmful. Crypto-secure processors such as AEGIS and Ascend use single-chip architectures to provide private and authentic processing with encrypted and obfuscated instruction execution [4].

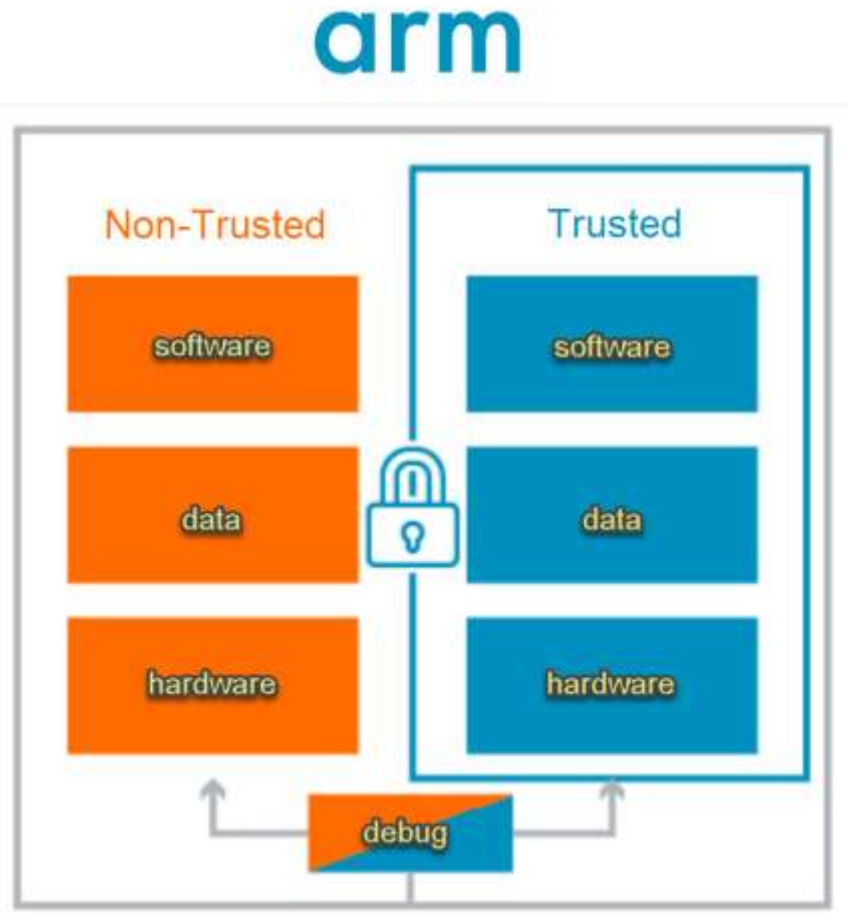

Fig. 2. Arm TrustZone security technology architecture

Microarchitectural event monitoring. Hardware-based microarchitecture and SIEM (Security information and event management) event monitoring offers fine-grained filtering for individual runs, can collect multi-dimensional information, and provides faster response than software-based anti-malware counterparts.

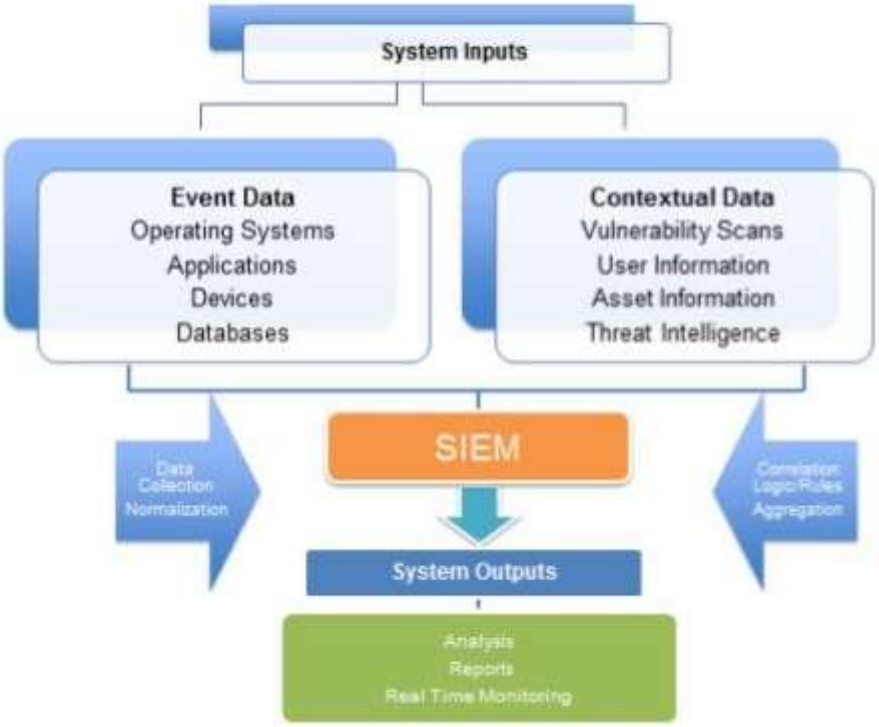

Fig.3. SIEM system architecture

Developers from NYU Polytechnic School of Engineering, Brooklyn, New York, USA proposed a host-based DDoS attack detection framework called BRAIN (BehavioR based Adaptive Intrusion detection in Networks). It uses hardware features to simulate secure behavior and DDoS attacks. To detect DDoS attacks, it uses machine learning techniques to model application behavior and network statistics. The DDoS Prevention Interface (DDoSPI) responds to any detected attack by blacklisting IP addresses (and deleting if necessary) based on a dynamic network and HPC-based threshold, thereby preventing an attacker from learning device security criteria and policies [5].

Results. Improving security using machine learning techniques. Various machine learning methods have been developed to study and distinguish such events and identify any type of anomaly with higher detection accuracy and fewer errors. Two main requirements for such methods are: selection of high-precision microarchitectural features for event collection using high-performance computing; selection of effective machine learning methods for classification and regression problems [6].

At this stage, measures are taken when a threat is detected. This could be alerting the user to a potential threat, terminating suspicious processes, or a more critical event such as shutting down the entire device to protect data and the system. The uses of a disassembler are varied - it can be used to trace and reconstruct code, reverse engineer source code, joint hardware/software certification, and most importantly, to verify the integrity of software running on an IoT device.

A widely known class of cyber threats is a third-party channel attack. Such attacks violate the confidentiality of cryptosystems by using information about the ongoing physical processes in the device, for example, by measuring the operation time, current-voltage characteristics, electromagnetic radiation of the device, and so on. Attackers, collecting a sufficient amount of statistical data, after some analysis, can guess what algorithm is used in the cryptosystem, gain access to secret keys, or make changes to the algorithm. Thus, an attacker easily bypasses the protection and takes possession of the IoT device [7].

Most malware can be detected through side-channel power failures. Their proposed system monitors the device's power consumption and uses machine learning to detect potential anomalous behavior. Such methods can be used to attest and authenticate IoT devices on an untrusted network. A runtime monitoring system using electromagnetic radiation (EM) as a side channel is also implemented. It can detect abnormal behavior during program execution, such as the injection of malware or other code, using supervised machine learning classifiers. This method is potentially well suited for monitoring the security of IoT and embedded devices because it does not require additional resources on the monitored machine, nor does it require a wired connection as would be the case with power side-channel information collection.

Discussion. Hardware information security solutions for IoT devices perfectly complement existing software security mechanisms. In addition to the PMU, various embedded sensors, such as temperature sensors, as well as new architectures can be used to provide security [8].

To protect themselves, organizations using an IoT sensor system implement intrusion detection and prevention systems (IDS/IPS). IDS (Intrusion Detection System) - intrusion detection system, IPS (Intrusion Prevention System) - intrusion prevention system. There are three main types of IDS: 1) Network IDS are installed at the edges of the network and analyze all passing traffic for malicious activity. 2) Hosted IDS operate on separate servers, workstations or devices. 3) Application IDS specialize in individual services and applications [9]. Intrusion Prevention Systems (IPS) - actively block detected attacks. Once IPS detect malicious traffic or behavior, they use techniques to stop it: Packet filtering, IP address and protocol blocking. Terminating suspicious network connections. Termination of processes and applications associated with the attack. Changing the access rights of the compromised account.

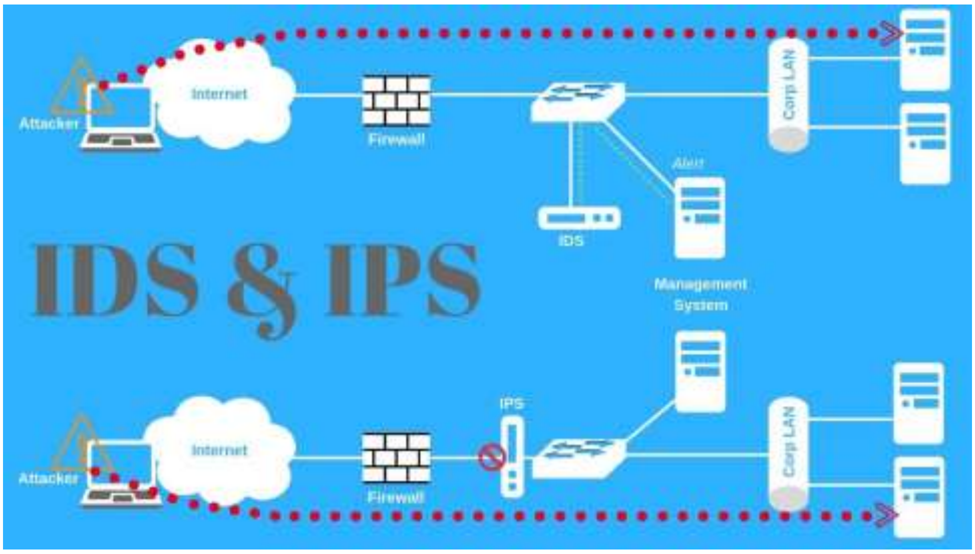

Fig.4. Architecture of IDS and IPS systems

Conclusion. With the advent of IoT devices and IoT-centric applications, it is imperative to provide a reliable and secure platform for this space to ensure maximum protection against current and future cyber-attacks. It is necessary to use both hardware and software solutions in a hybrid manner. Hardware-based protection for IoT devices has proven its effectiveness and versatility. However, there is no doubt that further research is needed in developing appropriate security mechanisms for lightweight IoT applications. IDS/IPS systems serve as an additional layer of protection that allows you to quickly identify and stop sophisticated cyber attacks that traditional solutions like firewalls cannot protect against. Working in real time, they instantly respond to the very first signs of intrusion, which can save a company from cyberattacks even at the most unexpected moment. Only an integrated approach to the implementation of IDS/IPS will provide reliable data protection from cyber threats.

REFERENCES

1. Namiot, D.E., & Sukhomlin, V.A. (2023). On the cybersecurity of Internet of Things systems. International Journal of Open Information Technologies. ISSN: 2307-8162, vol. 11(2), pp. 85-97.

2. Vereshchagina, E.A., Kapetsky, I.O., & Yarmonov, Ya.S. (2021). Internet of Things security issues. Textbook - M.: World of Science. pp. 105.

3. Muradova, A.A., & Begmatov, Sh.A. (2024). Methods for managing the reliability and quality of IoT sensors. *Multidisciplinary Scientific Journal GOLDEN BRAIN*. Vol.2, Issue 4, pp. 49-58.

4. Chernyak, L. (2012). Internet of Things platform. *Open systems*. №7, 44 p.

5. Internet Security Threat Report. Symantec: Mountain View. (2017). Vol. 22. 77 p.

6. Muradova, A.A. (2023). Cyber security risks of IoT devices. *Republican scientific and practical conference on the topic "Role of information and communication technologies in the formation of innovative economy".* Tashkent, Uzbekistan.

7. Muradova, A.A. (2023). Network security of the internet of things (IoT) in organizations. *Problems of information security and cyber security in the field of information technologies and communications" Republican scientific and practical conference*. TUIT. Tashkent, Uzbekistan.

8. Muradova, A.A. (2023). Reliability and security of the Internet of things. *Multidisciplinary Scientific Journal SCHOLAR*. Vol.1,27, 109-117.

9. Muradova, A.A. (2023). Basic steps to secure the Internet of Things. *Multidisciplinary Scientific Journal SCHOLAR*. Vol.1,31, 71-76.