International Journal of Business and Technology

Volume 9
Issue 1 *Spring 2021*

Article 21

March 2021

Review of cybersecurity hardware devices

Eriselda Malaj
Technical University of Sofia, Sofia, Bulgaria,, Eriselda.malaj@hotmail.com

Recommended Citation

Malaj, Eriselda (2021) "Review of cybersecurity hardware devices," *International Journal of Business and Technology*: Vol. 9: Iss. 1, Article 21.
DOI: 10.33107/ijbte.2021.6.3.19
Available at: https://knowledgecenter.ubt-uni.net/ijbte/vol9/iss1/21

Review of cybersecurity hardware devices

Eriselda Malaj [1], Galia Marinova [2]

[1] Technical University of Sofia, Sofia, Bulgaria, E-mail: Eriselda.malaj@hotmail.com

[2] Technical University of Sofia, Sofia, Bulgaria, Email: gim@tu-sofia.bg

Abstract. In the modern world, cybersecurity is an important issue in the field of technology. The main security problem is the security of the data we receive on the server side after being sent by the client or by the sensors. Nowadays cybersecurity is seen as an area where software is more important than hardware and this led to an increase in the number of securities at the software level. By increasing security at the hardware level cyber security takes another dimension. Network infrastructure devices serve for the realization of communication of applications, data, services and multi-media. These devices include firewalls, routers, servers, switches, load-balancers, domain name systems. Intrusion detection systems and storage area networks. All of these infrastructure devices are the main target of cyberattacks because all data traffic passes through them. A router attack can monitor all network traffic. Network data can be monitored and modified. Also, the presence of an attack on the switch can monitor, modify and deny traffic to hosts within the network. Most organizations that use old unencrypted protocols to manage their hosts make it easier to obtain credentials from cyberattacks. Security at the hardware level is one of the most important issues for the proper functioning of computer systems. Hardware security includes limited access to sensitive information, risks and potential security threats, protection against unauthorized, and enhancement of hardware performance. This paper provides an overview of internet security hardware devices and some recommendations.

Keywords: hardware device, security, attack, biometrics, scans, cryptography, fingerprint

I. Introduction

The most popular of cybersecurity devices are firewalls - hardware security systems which create a barrier between the Internet and an internal network, effectively regulate and manage network traffic based on several protocols. Firewall can be hardware appliance or software, or include together software and hardware devices. Most computers use software-based firewalls to secure their data from Internet threats, many routers also contain the firewall components. Such network security devices as routers, virtual private network gateways, crypto-capable routers, intrusion detection systems and secure modems are also very popular. Intrusion detection systems are devices that monitor malicious activities in a network, log information about such activities and take active steps to stop them, and then report them. The assets under consideration are the hardware components themselves, for instance, integrated circuits (ICs) of all types, passive components (such as, resistors, capacitors, inductors), and printed circuit boards (PCBs); as well as the secrets stored inside these components, for instance, cryptographic keys, digital rights management (DRM) keys, programmable fuses, sensitive user data, firmware, and configuration data [1].
There are few types of hardware security devices in fig 1, that can be described, as follows:

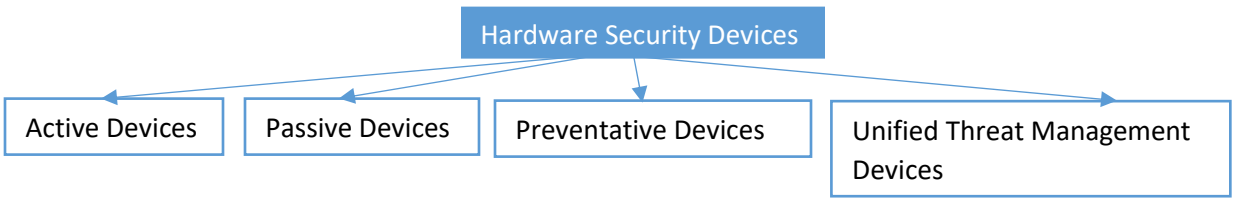

Fig.1 Hardware security devices Classification

- **Active devices** - antivirus scanning devices, content filtering devices, firewalls, which block the surplus traffic;
- **Passive devices** - which identify and report on unwanted traffic, such as intrusion detection appliances;

- **Preventative devices** - vulnerability assessment appliances and penetration testing devices, which scan the networks/software/database and identify security problems;
- **Unified Threat Management (UTM) devices** - such as content filtering, web caching, firewalls, which serve as all-in-one security devices.

The outline of the paper is the following: in Section II, a research method, in Section III types of algorithms that are implemented on the devices, in section IV. Results of the literature review and finally Section V concludes and future work.

II. Research method

This paper tries to answer the following Research Questions:

RQ1. What are the security threats on hardware devices?

RQ2. How can the security of hardware devices be improved?

RQ3. Why should we use cyber security hardware?

RQ4. Which are hardware devices security Tools and Techniques?

RQ5. Evolution of Hardware Security

III. Types of algorithms implemented

Generally, cryptographic algorithms are grouped and organized into two major categories: Symmetric and Asymmetric, but in practice today's algorithms use a hybrid combination of two algorithmic forms: symmetric and asymmetric. These two types of algorithmic groupings differ in the forms and types of keys they use for encryption and decryption operations [2].

Cryptography is one of the most powerful tools that organizations use to protect information. Cryptography applications can find: -Anti malware, Audits, Forecasts, ID managements, Intellectual property, secure message communications, Weakness management, Physical protection, Transaction security, Wireless, etc. In figure 2 we have explained the classification of the cryptographic algorithm [16].

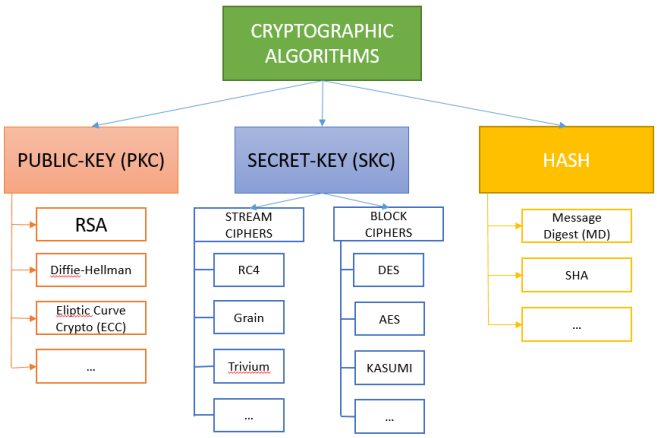

Fig. 2 Cryptographic algorithm classification.

A. Symmetric Cryptography

Encryption methodologies that require the same secret keys to encrypt and decrypt a message, use what is known as private key encryption or symmetric encryption. Symmetric encryption methods use mathematical operations

programmed by very fast computer algorithms with the sole purpose that the encryption and decryption process executed quickly even on smaller computers. One of the most popular systems is the Data Encryption Standard (DES), which uses 64-bit blocks and 56-bit keys. Triple DES (3DES) is a cryptosystem, offering greater security than DES. 3DES is an advanced DES application, however within a few years the value of this type of key also dropped. Triple DES uses a "key bundle" that includes three DES keys: K1, K2 and K3, each of 56 bits. The tracker or upgraded version of 3DES is the Advanced Encryption Standard (AES). [16] The algorithm from the beginning is designed to be unclassified, publicly disclosed, and available free worldwide. AES replaces both DES (almost no use) and 3DES (very limited use now). AES implements a block cipher called Randel Block Cipher with a variable block length and a key length of 128, 192, or 256 bits. Depending on the size of the key, the number of rounds varies from nine to thirteen: (For a 128-bit key, used nine rounds plus one final round; For a 192-bit key, used eleven rounds plus one last round; For a 256-bit key, used thirteen rounds plus one last round). After Randel adapted as AES, the ability to use blocks of variable sizes standardized into a single 128-bit block for simplicity. Block Cipher and Stream Cipher are the symmetric key cipher. The main difference between Block and Stream cipher is that block cipher converts the plaintext into ciphertext by taking plain text's block at a time. While stream cipher converts the plain text into cipher text by taking 1 byte of plain text at a time.

B. Asymmetric Cryptography

Symmetric encryption systems use only one key to both encrypt and decrypt a message. Asymmetric encryption uses two different but interconnected keys, and each used to either encrypt or decrypt the message. If key A is used to encrypt the message, only key B can decrypt it and if key B is used to encrypt the message only key A can decrypt it. Asymmetric encryption used to provide a better solution to privacy, security, and verification problems. This technique has the greatest value when one of the keys used as a private key, which means it is kept secret, and made known only to the owner of the second key, and the other key serves as a public key, which means it is stored in a public location that anyone can access and use. Therefore, these types of encryption are generally known as public key encryption. Asymmetric algorithms are one-way functions. A one-way function is simple to process in one direction and extremely complex in processing in the opposite direction. This is the essence of public key encryption. Public key encryption based on Hash values, which calculated from an input number in a hash algorithm. Output is the sum of input values. It is virtually impossible to extract the original values without knowing how those values used to create the hash value. One of the most popular public key cryptosystems is **RSA(Rivets-Shamir-Adelman)** based on the name of the developers. RSA is the first public algorithm developed in 1977 and published for commercial use [16]. In Table 1 we compared symmetric vs asymmetric encryption.

Table 1. Comparison between symmetric vs asymmetric encryption.

Differentiator	Symmetric Key Encryption	Asymmetric Key Encryption
Symmetric Key vs Asymmetric key	Only one key (symmetric key) is used, and the same key is used to encrypt and decrypt the message.	Two different cryptographic keys (asymmetric keys), called the public and the private keys, are used for encryption and decryption.
Complexity and Speed of Execution	It's a simple technique, and because of this, the encryption process can be carried out quickly.	It's a much more complicated process than symmetric key encryption, and the process is slower.
Length of Keys	The length of the keys used is typically 128 or 256 bits, based on the security requirement.	The length of the keys is much larger, e.g., the recommended RSA key size is 2048 bits or higher.
Usage	It's mostly used when large chunks of data need to be transferred.	It's used in smaller transactions, primarily to authenticate and establish a secure communication channel prior to the actual data transfer.
Security	The secret key is shared. Consequently, the risk of compromise is higher.	The private key is not shared, and the overall process is more secure as compared to symmetric encryption.
Examples of Algorithms	Examples include RC4, AES, DES, 3DES, etc.	Examples include RSA, Diffie-Hellman, ECC, etc.

III. Results of the literature review

RQ1. What are the security threats on hardware devices?

Nowadays network devices are the main targets for attackers. The factors that affect the vulnerability of network infrastructure devices are listed below:

- Small office/home network devices – for this residential class routers: integrity-maintenance, run antivirus and other security tools that help protect general purpose hosts.
- Operators of network devices don't change the default settings of purchased devices, also don't perform regular patching.
- Internet service providers may not replace devices on a customer's property once the devices aren't longer supported by the manufacturer.
- After cyber intrusions, operators or owners of the network often bypass the damage investigation on network devices, they only look for the intruder and restore hosts.

RQ2. How can improve the security of hardware devices?

To improve the level of security in hardware devices it is suggested to implement the following recommendations:

- Harden network devices,
- Secure access to infrastructure devices,
- Perform Out-of-Band Management,
- Validate integrity of hardware.

A. Harden Network Devices

In order to increase the security of the network infrastructure, the protection of the network equipment should be realized. A wide range of guidelines have been provided to protect them, including standards and best practices on how to improve network equipment security. In the list below are some recommendations that should be implemented, these recommendations are in line with site security policies, laws, regulations, standards and industry best practices.

The recommendations are:

- Disable unencrypted remote admin protocols used to manage network infrastructure (e.g., File Transfer Protocol [FTP], Telnet,).
- Disable unnecessary services (e.g., Hypertext Transfer Protocol [HTTP], discovery protocols, source routing, Bootstrap Protocol, Simple Network Management Protocol [SNMP]).
- Do not use SNMP community strings, but use SNMPv3 (or subsequent version).
- Secure access to the console, virtual terminal lines, and auxiliary.
- Use the strongest password encryption available, and implement robust password policies.
- Protect switches and routers by controlling access lists for remote administration.
- Restrict physical access to switches and routers.
- Back up configurations and store them offline. Use the latest version of the network device operating system and keep it updated with all patches.
- Periodically test security configurations against security requirements.
- Protect configuration files with encryption or access controls when sending, storing, and backing up files.

B. Secure Access to Infrastructure Devices

Administrative privileges should be restricted for infrastructure devices because intruders may use administrative privileges to access the network. [9] Administrators of cybersecurity must implement secure access policies and procedures. Below we have listed some recommendations: These include hardware keys for biometric security devices, multi-factor authentication and more obscure and powerful hardware.

The recommendations are:

- **Implement multi-factor authentication (MFA):** Attackers exploit weak authentication. Authentication is a process used to validate a user's identity. MFA uses at least two identity components to authenticate a user's identity. Identity components include
    - An object the user has possession of (e.g., token),
    - Something the user knows (e.g., password),
    - A trait unique to the user (e.g., fingerprint).
- **Encrypted Flash Storage:** To increase hardware security the best solution is encrypted flash storage. There are many companies that offer this service but the most important is Kingston which offers 6 encrypted flash storage options. Many devices have it integrated into the hardware keypad.
- **USB Fingerprint Readers:** Fingerprint readers authentication to provide a high level of biometric security. Microsoft has tried to create an environment for adoption of biometric authentication through Windows Hello, which supports iris scanning, facial recognition, and fingerprint readers. The use of fingerprint readers to protect the device is one of the first levels of security the device can have against unauthorized intruders.
- **Biometrics Readers:** Retina Scans, Iris Scans, Fingerprint, Physical Modalities, Voice recognition.
- **USB MFA Security Keys:** The USB device functions for two-factor and passwordless authentication. One of them is YubiKey which is used by companies such as Facebook and Google. W3 Consortium announced WebAuthn for web authentication.
- **Hardware Network Filters:** This device performs hardware network filtering such as Winston filters packets traffic in network. Winston functions as a VPN uses ARM processor. This hardware is on the network and it protects every device on the infrastructure.
- **IoT Device Shields:** IoT devices are the main point of entry for malicious actors because the level of security in these devices is very low and they are often used as botnets. One solution for protecting IoT devices to identity theft attacks and malware is Bitdefender BOX. The BOX claims to block common password theft attack vectors, malware and identity theft attacks, even for devices without an OS.
- **Manage privileged access.** Use a server that provides authorization, authentication, and accounting (AAA) services to store access information for network device management. Using MFA makes it more difficult for intruders to steal and reuse credentials to gain access to network devices.

C. Perform Out-of-Band Management (OoB)

OoB management uses alternate communications paths to remotely manage network infrastructure devices. These dedicated communications paths can vary in configuration to include anything from virtual tunneling to physical separation. Using OoB access to manage the network infrastructure will strengthen security by limiting access and separating user traffic from network management traffic. OoB management provides security monitoring and can perform corrective actions without allowing the adversary (even one who has already compromised a portion of the network) to observe these changes [7].

OoB management can be implemented physically, virtually, or through a hybrid of both. Although building additional physical network infrastructure can be expensive to implement and maintain, it is the most secure option for network managers to adopt. Virtual implementation is less costly but still requires significant configuration changes and administration. In some situations, such as access to remote locations, virtual encrypted tunnels may be the only viable option.

Recommendations

- Ensure that management traffic on devices comes only from OoB.
- Segregate standard network traffic from management traffic.
- Apply encryption to all management channels.
- Encrypt remote access to infrastructure devices such as terminal or dial-in servers.
- Manage all administrative functions from a dedicated, fully patched host over a secure channel, preferably on OoB.
- Harden network management devices by testing patches, turning off unnecessary services on switches and routers, and enforcing strong password policies. Monitor the network and review logs. Implement access controls that only permit required administrative or management services (e.g., SNMP, Secure Shell, Trivial FTP, Network Time Protocol, FTP, Server Message Block [SMB], Remote Desktop Protocol [RDP]).

D. Validate Integrity of Hardware

Gray market device can pose network risks because it hasn't been tested to meet quality standards. Secondary products carry the risk of second-hand products, stolen because of supply chain breaches. Unauthorized software can be embedded in the device and after being put into operational use damages the entire network of the organization. Recommendations are listed below to validate the integrity of the hardware [5]:

- To purchase only from authorized resellers and maintain strict control of the supply chain.
- To validate hardware authenticity, require resellers to enforce integrity checks of the supply chain.
- After installation, inspect all devices for signs of tampering.
- Validate serial numbers from multiple sources.
- Download updates, patches, upgrades and software from validated sources.
- Perform hash verification, and compare values against the vendor's database to detect unauthorized modification to the firmware.
- Monitor and log devices, Verifying network configurations of devices, on a regular schedule.
- Train network administrators, procurement and owners' personnel to increase awareness of gray market devices.

RQ3. Why Should You Use Cyber Security Hardware?

Various security vulnerabilities and attacks on hardware have been reported over the last three decades. Earlier, they primarily focused on implementation dependent vulnerabilities in cryptographic chips leading to information leakage. However, emerging trends in electronic hardware production, such as intellectual-property-based (IP-based) system on chip (SoC) design, and a long and distributed supply chain for manufacturing and distribution of electronic components leading to reduced control of a chip manufacturer on the design and fabrication steps have given rise to many growing security concerns. This includes malicious modifications of ICs, also referred to as Hardware Trojan attacks [12], in an untrusted design house or foundry. Another important aspect of hardware security relates to the hardware design, implementation, and validation to enable secure and reliable operation of the software stack. It deals with protecting sensitive assets stored in a hardware from malicious software and network, and providing an appropriate level of isolation between secure and insecure data and code, in addition to providing separation between multiple user applications [1]. Two major topics in this area are as follows. (1) Trusted execution environment (TEE), such as ARM's Trust Zone, Intel SGX, and Samsung Knox, which protects code and data of an application from other untrusted applications with respect to confidentiality (the ability to observe a data), integrity (the ability to change it), and availability (the ability to access certain data/code by the rightful owner). The confidentiality, integrity, and availability are referred to as CIA requirements. They form three important pillars for secure execution of software on a hardware platform. Establishment of these requirements is enabled by a joint hardware-software mechanism, with hardware providing architectural support for such an isolation, and facilitating effective use of cryptographic functions, and software providing efficient policies and protocols. (2) Protection of security-critical assets in an SoC through appropriate realization of security policies, such as access control and information flow policies, which govern the CIA requirements for these assets.

RQ4. Which are hardware devices security Tools and Techniques?

A. Security Products: The combination of continued chip technology advances and an unprecedented level of globalization in the semiconductor industry has spurred enormous changes in the way chips are designed, manufactured, and used. These changes bring many benefits to the consumer including lower prices and faster time to market for products and services, but they have also created a widening set of opportunities for would-be attackers to insert malicious circuits during the chip design process that could be used to launch a hardware attack. The nature of the hardware security threat and outlines a multipronged approach to address it involving [4]:

- a change in design practices within the semiconductor industry,
- the establishment of a national-level capability to coordinate a quick response to an attack,
- improved testing procedures to detect corrupted chips before they are placed into products
- the inclusion of built-in defenses into chips to identify and thwart attacks as they occur.

B. Firewall: Firewalls create a barrier between the internal network and outside networks, such as the Internet. They monitor incoming and outgoing traffic and determine whether to allow that traffic through or block it using a pre-defined set of rules. Firewalls can be either hardware or software. There are several types of firewalls: (Packet-Filtering Firewalls, Circuit-Level Gateways: Stateful Inspection Firewalls, Application-Level Gateways, Next-Generation Firewalls**).**

C. Network load balancer (NLB): Load balancers are physical units that direct computers to individual servers in a network, based on factors such as server processor utilization, number of connections to a server or overall server performance. Organizations use load balancers to minimize the chance that any particular server will be overwhelmed and to optimize the bandwidth available to each computer in the network. A load balancer can be implemented as a security software or hardware solution, and it is usually associated with a device, a router, a firewall, a network address translation (NAT) appliance and so on. A load balancer splits the traffic intended for a website into individual requests that are then rotated to redundant servers as they become available. A key issue with load balancers is scheduling, determining how to split up the work and distribute it across servers. There are several load balancing methods: (Round-robin, Affinity, No affinity, Single affinity, Class C affinity, Least connection, Agent-based adaptive load balancing, Chained failover, Weighted response time, Software-defined networking) [10].

D. Authentication and Authorization Technologies: Authentication may require the user to put in a username and password, scan a card or undergo biometric identification through methods such as fingerprint scanning, voice recognition or retina scans. Authentication may also involve the server giving the client a certificate that verifies its identity. Directory-based services like Active Directory authenticate users and use authorization rules to control their access permissions. Other technologies use methods such as digital certificates and public key infrastructure solutions. The Simple Network Management Protocol (SNMP) also provides additional security. [11]

E. All-in-One Network Security Hardware Appliances: Some security equipment combines multiple features into one device. These types of devices are sometimes called network security hardware appliances. These tools act as an all-in-one security gate and may perform the functions of a network firewall, VPN and router. It works to prevent threats from entering your network and can alert you if an attempted attack occurs. There are various types of these all-in-one devices. One example is the Cisco Adaptive Security Appliance 5500 series, which provides next-generation firewall security and VPN functionality. The Juniper NetScreen-5GT includes a next-generation firewall, VPN capabilities and integrated malware protection. [12]

RQ5. Evolution of Hardware Security

Over the past three decades, the field of hardware security has evolved rapidly with the discovery of many vulnerabilities and attacks on hardware. Figure 3 provides a brief timeline for the evolution of hardware security. The Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program was introduced by DARPA in 2014 to develop technology to trace and track electronic components PCB to chip to small passive components as they move through the supply chain. Over the past decade, many efforts by both government and industry to enable secure and trusted hardware platform have been observed with more to come in near future [15].

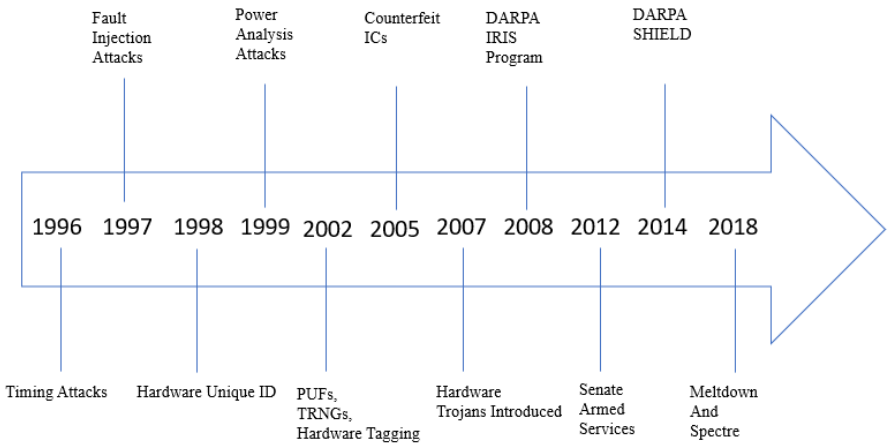

Fig.3 The evolution of hardware security

IV. Conclusion

Nowadays hardware security is the main topic in security issues, due to the growing computing edge, IoT and cloud. In this review we have addressed security threats on hardware devices and we have recommended how to improve the security of

hardware devices. We have explained the evolution of hardware security and some of the hardware security tools and techniques. In many cases hardware security is in conflict with performance optimization such as limited battery conditions or low power. Optimization is the most important task of design but also the main cause of information flow. One challenge for hardware security is the lack of EDA tools to support it. An added challenge is that it is difficult to measure security and difficult to balance security versus throughput, area, or power optimizations.

Acknowledgement

This study is realized and partly supported by the CEEPUS network CIII-BG-1103-06-2122, especially in the part Joint doctoral program within CEEPUS.

V. References

1. S. Ray, E. Peeters, M.M. Tehranipoor, S. Bhunia, System-on-chip platform security assurance: architecture and validation, Proceedings of the IEEE 106 (1) (2018) 21–37.
2. M. Barbareschi, P. Bagnasco, A. Mazzeo, Authenticating IoT devices with physically unclonable functions models, in: 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2015, pp. 563–567.
3. A. Vijayakumar, V.C. Patil, D.E. Holcomb, C. Paar, S. Kundu, Physical design obfuscation of hardware: a comprehensive investigation of device and logic-level technique, IEEE Transactions on Information Forensics and Security (2017) 64–77.
4. U.S. Senate Committee on Armed Services, Inquiry into counterfeit electronic parts in the Department of Defense supply chain, 2012.
5. Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it. https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/.
6. M. Tehranipoor, U. Guin, D. Forte, Counterfeit integrated circuits, Counterfeit Integrated Circuits (2015) 15–36.
7. F. Piessens, The Cyber Security Body of Knowledge. University of Bristol, 2019, ch. Software Security, version 1.0. [Online]. Available: https://www.cybok.org/
8. N. Smart, The Cyber Security Body of Knowledge. University of Bristol, 2019, ch. Cryptography, version 1.0. [Online]. Available: https://www.cybok.org/
9. H. Kaislin, Top-Down Digital VLSI Design: From Architectures to Gate-Level Circuits and FPGAs. Morgan Kaufmann, 2015.
10. W. Slegers, Security Evaluation Scheme for IoT Platforms, version 1.2, TrustCB, 2019. [Online]. Available: https://www.trustcb.com/iot/sesip/
11. F. Turan and I. Verbauwhede, "Compact and flexible FPGA implementation of Ed25519 and X25519," ACM Transactions on Embedded Computing Systems, vol. 18, no. 3, p. 21, 2019.
12. N. Suri, The Cyber Security Body of Knowledge. University of Bristol, 2019, ch. Distributed Systems Security, version 1.0. [Online]. Available: https://www.cybok.org/
13. J. Balasch, F. Bernard, V. Fischer, M. Grujic, M. Laban, O. Petura, V. Rozic, G. V. Battum, I. Verbauwhede, M. Wakker, and B. Yang, "Design and testing methodologies for true random number generators towards industry certification," in International IEEE European Test Symposium - ETS 2018, ser. IEEE Computer Society, Bremen,DE, 2018, p. 10.
14. R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans," Computer, vol. 43, no. 10, pp. 39–46, 2010.
15. J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ser. CCS '13. ACM, 2013, pp. 709–720. [65] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. J. Rajendran, and O. Sinanoglu, "Provably-secure logic locking: From theory to practice," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '17. ACM, 2017, pp. 1601–1618.
16. CompTIA Security+ Deluxe Study Guide, Fourth Edition, Emmett Dulaney, Chuck Easttom