2018 IEEE 32nd International Conference on Advanced Information Networking and Applications

Challenges and Methodologies of Hardware Security

Kin Fun Li and Narges Attarmoghaddam
Electrical and Computer Engineering
University of Victoria
Victoria, Canada
kinli@uvic.ca, nattarmoghaddam@uvic.ca

Abstract— **An attack on hardware typically results in a severer and difficult-to-recover damage, hence, it is our interest to focus this work on hardware security. A brief survey of security issues found in various application domains is presented, based on a collection of over seventy papers in IEEE Xplore archived since 2011. Challenges and potential solutions to different kinds of hardware attacks and threats are discussed. Finally, specific hardware security challenges are connected and mapped to each application domain.**

Keywords-cyber security, hardware security, security hardware, security challenges, security threats, security mechanisms, attack detection, attack prevention

I. INTRODUCTION

Cyber security has become a major research and industry focus since the inception of the Internet. The U.S. government spent 7.5 billion in 2007 on cyber security, and this figure increased almost fourfold to 28 billion in 2017 [63]. According to a UK government survey, almost half of the UK firms were having cyber security problems in 2017 [66].

Since an attack can occur at any one of the layers (e.g., operating system, network, application software) in the cyber world, there are many approaches to combat the various cyber security attacks including malware, ransomware, denial-of-service, etc. An attack on hardware typically results in a severer and difficult-to-recover damage. For example, Bidmeshki et al. demonstrate that even low-cost hardware-based attacks could be catastrophic [9]. Hence, we are interested to investigate issues related to hardware security.

This work is based on a brief survey of over seventy prominent papers on hardware security published in IEEE Xplore since 2011. We start with examining hardware security issues pertinent to each of the five identified broad application domains in section II. Next, hardware security challenges found in the survey and the corresponding potential solutions are described in section III. By connecting the materials in sections II and III, specific hardware security challenges are mapped onto each application domain in section IV. Finally, discussions and conclusions are presented in section V.

II. SECURITY ISSUES IN APPLICATIONS

From the collection of papers reviewed, we can identify five main areas of applications where hardware security is of a major concern: mobile system, embedded system, network, memory, and IC design. Features and issues specific to each of these domains are presented below.

A. Mobile Agents and Systems

1) Trends and Challenges

Arabo and Pranggono study the trends and challenges of smart device security in smart homes [3]. They identify the major security issue being mobile malware, and propose an integrated solution to address this issue.

To detect vulnerabilities and malicious software on mobile devices, Wang and Alshboul present and evaluate four testing approaches: mobile forensic, penetration test, static analysis, and dynamic analysis [70]. They conclude that mobile security tools are still in their infancy, and further research and development are necessary.

Shen and Wu present a proposal to improve authentication and credentials management in a mobile agent environment [58]. They also describe how to build trusted mobile agents by the use of trusted computing platforms.

2) Techniques and Solutions

Fournaris discusses hardware attempts to provide security and trust mechanisms in mobile platforms [17]. The Trusted Computing Group initiative [66] for mobile trust is highlighted. Hardware cryptographic algorithms are presented and it is suggested that the best solution is Elliptic Curve cryptography and the associated Pairing Based protocols.

Another interesting approach for mobile security is the design and implementation of an entire security chip. Ju et al. present one such chip, the Mobile Trusted Module, with I/O interface to a mobile device. Results of testing the prototype chip with a smartphone are discussed.

Maruaisap and Kumhom propose a hardware scheme to increase security in Controller Area Network (CAN) commonly found in vehicles [40]. This scheme makes use of a hardware-based key generator and the Advanced Encryption Standard (AES). Key generation and time delay among the nodes in the network are examined in detail.

In [42], Milosevic et al. discuss security challenges in mobile device design. They present mitigation techniques for physical attacks that can be implemented during the design stage. Potential hardware implications due to software malware are also discussed.

3) The Internet-of-Things (IoT) Realm

In this age of Internet-of-things (IoT), numerous security challenges exist. Koley and Ghosal address major security and privacy flaws in IoT devices and present possible solutions to

1550-445X/18/$31.00 ©2018 IEEE
DOI 10.1109/AINA.2018.00136

make them secure [34]. Hardware Trojans in IoT systems and detection techniques are also addressed.

Ray and Bhadra look at security challenges from the design perspective, specifically the vulnerability arises due to the tradeoffs made between functionalities and security in System-on-Chip (SoC), using automated design tools [49].

Malicious insertions into digital signal processing IoT devices in the form of hardware Trojan are studied by Syed and Lourde in [61]. Methods to identify hardware Trojans and their impact on CORDIC are demonstrated using Xilinx FPGAs.

In [7], various cryptographic algorithms including AES, 3DES, Twofish and RSA are compared, and implemented in ASICs. Bahnasawi et al. find that the AES algorithm in ASICs is the most suitable one for IoT applications.

B. Embedded System Security

Nowadays, many embedded systems are designed using intellectual property (IP) blocks. Wach and Ip examine security intellectual property (SIP) hardware building blocks [68]. They also discuss the many security specific challenges of SIP's design and integration, and the strategies to alleviate the impact of these challenges.

The various approaches to address embedded system security are described below.

1) Hardware Accelerators

Fiorin et al. use a hardware approach to implement Security Enhanced Linux (SELinux) [16]. Based on an FPGA platform, they report improvement in performance overhead and energy consumption, while a limited chip area is maintained.

Babecki et al. present a reconfigurable framework for hardware accelerator as security kernel (HASK) [6]. HASK is capable of supporting and accelerating a wide range of security applications with commonly used building blocks. Through simulation, they show HASK improves over both software and FPGA platforms in throughput and energy-delay product. Another hardware security proposal relies on nonvolatile resistive random access memory based FPGAs [12]. Chen and colleagues' scheme utilizes internal block RAMs housing obfuscated configurations to protect design data from attacks in embedded systems.

FFT, a notable time-consuming task, is widely used in cryptographic algorithms. Argenziano proposes an FFT hardware accelerator [4]. The architecture, implementation, and performance are presented based on an FPGA platform.

Continue to explore the cryptographic side, Thiruneelakandan and Thirumurugan present a secure FPGA-based VLSI Crypto system that accelerates compute-intensive cryptographic algorithms including SEA, MD5 and SHA2 [1]. Experimental results on a Cybernetic application show their system improves performance in speed, area, and security.

2) Protection Mechanisms

Pouraghily and colleagues argue the low effectiveness of using software-based protection mechanism due to embedded system's power and processing limitation [47]. They propose hardware-based monitoring to detect abnormal operation in operating system and applications. An FPGA prototype is implemented to illustrate the effectiveness of their approach. Similarly, Wang et al. use a hardware-assisted monitoring architecture for program code protection [69].

Lukacs et al. present a hardware-enforced security mechanism for portable operating systems and embedded devices, by detecting all known kernel rootkit attacks [39].

Gu et al. devise a scheme to map an application task graph onto a FlexRay automotive communication hardware platform, with the goal of meeting security as well as real-time deadline requirements [21]. This scheme prevents attackers from injecting malicious messages into the broadcast network in vehicles.

Secured cryptoprocessor based on Trusted Platform Module (TPM) is a good way to protect information from possible attacks. Karter et al. examine the security features and issues within TPM and evaluate its advantages and disadvantages [29].

3) Security Enhancement techniques

Lin et al. propose an architecture that enhances hardware security against side channel attacks [38]. They insert FIFOs between two adjacent pipeline stages and make random duration for data staying in the FIFOs. Thus, the execution time of hardware modules becomes unpredictable. An implementation of such a FIFO-filled pipeline is realized with the Advanced Encryption standard (AES) algorithm.

At the System-on-Chip (SoC) level, Kim and colleagues present on-the-fly reconfigurable architectural features to recover from system malfunction as a result of hardware-based attacks [31].

Liu et al. present a bus architecture for run-time hardware Trojan protection [10]. The novel bus controller and a random number generator make the implementation of this SoC bus architecture possible.

C. Network Security

Liang et al. provide a comprehensive presentation on the challenges and solutions in mobile social networks [37]. The drawbacks of existing solutions are discussed and further research directions are recommended.

Revolutionary changes in network technologies are noted by Zhou et al. [74]. They present an evolving defense mechanism that can cope with new network advances, and possibly emerging security threats.

In order to take advantage of what reconfigurable computing can offer, Muehlbach and Koch present a high-level domain-specific language Malacoda for application-level network processing, to bridge the gap between network expertise, and hardware architecture and design knowhow [44]. Malacoda descriptions are automatically translated into hardware blocks on FPGAs.

D. Memory Security

Non-volatile memories (NVMs) are easier target than their volatile counter-parts due to the nature of persistent data in NVMs. Ghosh et al. present an excellent investigation on data security and privacy challenges, threats and possible countermeasures in NVMs [20].

By remapping the data locations in memory, Kan et al. aim to reconcile SRAM security with SRAM soft error reliability

[28]. The remapping makes the prediction of data locations in memory difficult, thus deterring hardware Trojan attacks.

In [72], Wiersema et al. propose the combination of access monitors with the proof-carrying hardware (a formal runtime verification technique) to secure memory access in reconfigurable systems.

To increase security in memory systems, Neagu and Sebestyen employ data scrambling technique and information entropy models [45]. Dissemination rules are used in the scheme. The evaluation of their methodology is discussed.

E. IC Design Security

Currently there are many existing and proposed solutions in dealing with the security of integrated circuits (IC).

Gayathri et al. propose a logic obfuscating method for IC security, in particular, against counterfeiting, reverse engineering and IP theft [19]. In their method, the functionality of the IC is concealed by embedding extra keys into the original design.

However, several new device technologies have emerged recently and pose new security concerns. Shamsi et al. argue that the new devices, other than the traditional CMOS, used for integrated circuits provides opportunities for attacks as well as for remedies [57]. They present these hardware security challenges with non-CMOS integrated circuit designs.

Dofe et al. examine three-dimensional (3D) integrated circuits [15]. Security threats are identified and counter-measures are introduced. They propose a network-on-chip 3D obfuscation method to make reverse engineering more difficult. Similarly, Gu et al. propose several designs in 3D architectures to implement countermeasures against security threats [22].

In [46], Potlapally expresses concern in the complicated validation process of commercial computing platforms due to their complex hardware. Challenges and opportunities in validating security in industrial hardware are discussed.

Moghaddam et al. illustrate how test points, in addition to enhancing design testability, can be used to improve hardware security against reverse engineering, IC cloning, and IP theft, by hiding design functionality from adversaries [43].

Fujimoto et al. have an interesting approach to test the security and trust of commercial devices [18]. They employ On-Chip Power noise Measurements (OCM) to test security against side-channel attacks. Suggestions on how to validate hardware security and trust using OCM are also presented.

III. Security Challenges and Solutions

This section describes the challenges in hardware security, and the corresponding existing solutions, partly based on the excellent introduction and survey by Rostami, Koushanfar and Karri [53]. Interested readers are encouraged to explore further with their work that includes a classification of threat models, defenses and evaluation metrics for hardware attacks. Below is a brief introduction to challenges and solutions based on their classification scheme [52].

A. Hardware Trojans

Malicious circuits or their modifications are injected either during the design or manufacturing phase. Readers are referred to the hardware Trojan work by Milosevic et al. on mobile systems [42] and Sengupta on consumer electronics devices [55]. There are in general two types of detection methods. Invasive detection requires precise and costly equipment to make appropriate measurements; however, the device under test is rendered useless after. Based on functional and parametric testing external to the IC, the associated methods, however, are non-invasive in nature.

B. IP Piracy and IC Overbuilding

These occur mainly at the foundries where IPs are stolen and an excessive number of ICs are made. Countermeasures include:

- Physical Unclonable Functions (PUFs) [13]
- Watermarking where the designer's signature is integrated into the design [27]
- Fingerprinting where the signatures of both the designer and the buyer are embedded into the design [71]
- Obfuscation where additional hardware are incorporated into the design thus hiding the actual composition [48]
- Metering where the manufactured hardware can be tracked [1]
- Split manufacturing where a module is separated and manufactured by different foundries [25]

C. Reverse Engineering

By examining the hardware device details, one can backtrack and retrace the design, then reuse or improve upon it. Again, obfuscation is a well-known technique to counter reverse engineering [48]. Also camouflaging, a technique that makes two functional modules lookalike at the layout level, is widely used [62].

D. Side-Channel Analysis

When in operation, hardware devices and modules have certain physical characteristics that can be detected and extracted by an attacker, such as power consumption, timing, or electromagnetic emission. Countermeasures include:

- Physical unclonable functions (PUFs) [13]
- Leakage reduction where the side channel traces are made independent of the information being handled [60]
- Noise injection where artificial noise is injected into the side channel thus making retrieving information difficult [33]
- Key update where the secret key is frequently updated from a predefined sequence of keys [32]
- Secure scan chains where unauthorized accesses are blocked by the use of mirroring and randomizing techniques [1]

E. Counterfeiting

As the term implies, hardware design and modules are copied or imitated illegally. Countermeasures include:

- Physical unclonable functions (PUFs) [13]
- Fingerprinting [71]
- Hardware metering and auditing where hardware can be tracked post fabrication [35]
- Device aging models/sensors where the lifetime of the hardware module can be sensed and estimated thus preventing selling previously used chips [36]

IV. Hardware Security Challenges in Specific Applications

By relating materials in the previous two sections, specific hardware security challenges can be mapped onto each application domain. In this section, application specific challenges are described within the classification framework by Rostami, Koushanfar and Karri [53].

A. Hardware Trojans

- Mobile Systems:
  - Security challenges for mobile system design are discussed in [42]
  - Hardware security threats in DSP applications is the focus of [61]
- Embedded Systems:
  - FPGA is a popular delivery platform for embedded systems but care must be taken in its design and implementation considering hardware Trojan threats [59]
  - A System-on-Chip bus architecture is proposed to protect security chips from hardware Trojans [10]
  - A proposed system architecture performs run-time testing and verification against Trojans in SoC based hardware systems [30]
- IC Designs:
  - The SAFER PATH architecture is designed to operate safely even under active hardware Trojans. In this architecture, instruction and data are fragmented, programs are replicated, and decision makings are voted on [8]
  - Hardware Trojans and IP piracy are the major security vulnerabilities in consumer electronics devices and they are expected to have major impact on the operation of the device [54][55]
  - Low cost hardware Trojan aware scheduling mechanism based on loop unrolling has been implemented at the high-level synthesis layer [56]

B. IP Piracy and IC Overbuilding

- IC Technology:
  - Test points are employed to improve circuit testability, in addition to provide security[43]
  - Hardware security measures are big challenges in newer device technologies than CMOS [57]
  - Logic locking technique has been employed in counteracting IP theft. By inserting additional gates into the original design, the functionalities and implementation of the design can be concealed from IP threats [64]
  - Gate level netlist and layout geometry of IPs are targets for piracy and overbuilding, thus it is important to implement practical obfuscation mechanism to prevent such adversaries [73]

C. Reverse Engineering (RE)

- Test points can be used to hide the functionalities of hardware modules and prevent RE threats [43]
- Logic obfuscation method can be employed to prevent RE at the netlist level and the layout level geometry [73]

D. Side-Channel Analysis

- Embedded Systems:
  - Hardware support for security against side-channel attacks using FPGAs as a Trusted Computation Base in cloud computing [14]
  - Adding randomly delayed FIFOs between pipe stages to make hardware to be less vulnerable to side-channel attacks [38]
  - To enhance security against portable operating system and embedded system attacks, a thin layer bare-metal hypervisor is used [39]
- Memory Security:
  - Memory threats are decreased by the use of data scrambling and information entropy models [45]
- IC Designs:
  - Hardware security measures are big challenges in newer device technologies than CMOS [57]
  - Gu et al. propose several designs in 3D architectures to implement countermeasures against security threats [22]
  - Scan chains are used to protect sensitive information from attackers [41]
  - The SASEBO-GIII board is equipped with an FPGA developed for security evaluation against side-channel attacks (SCAs) [23]

E. Counterfeiting

  - By inserting additional gates into the original design, a logic locking technique, the functionalities and implementation of the design can avoid counterfeiting [64]

V. CONCLUSIONS

We present a brief survey of hardware security challenges and solutions. Techniques and methodologies employed in various application domains are discussed. It seems that no generic, one-size-fit-all solution can be used to deter all kinds of hardware security threats and attacks. Rather, it is appropriate to focus on a specific application domain and devise potential solutions to counteract the security issues in that class of applications; for example, hardware security in

the realm of Internet of Things. Indeed, this is the current focus in our investigation of hardware related security issues.

ACKNOWLEDGMENT

This work is supported by an NSERC Discovery grant and a University of Victoria Graduate Fellowship.

REFERENCES

[1] M. Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, ‘‘Scan based side channel attacks on stream ciphers and their counter-measures,’’ INDOCRYPT, 2008.

[2] Y. Alkabani and F. Koushanfar, ‘‘Active hardware metering for intellectual property protection and security,’’ 16th USENIX Security Symp., 2007

[3] A. Arabo, B. Pranggono, “Mobile Malware and Smart Device Security: Trends, Challenges and Solutions,” 19th International Conference on Control Systems and Computer Science, 2013.

[4] D, Argenziano, “Implementation of an FFT hardware accelerator for security applications,” 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2015.

[5] A. Asaduzzaman, M. F. Mridh, M. Uddin, “An Inexpensive Plug-and-Play Hardware Security Module to Restore Systems from Malware Attacks,” International Conference on Informatics, Electronics and Vision (ICIEV), 2013.

[6] Ch. Babecki, W. Qian, S. Paul, R. Karam, S. Bhunia, “An Embedded Memory-Centric Reconfigurable Hardware Accelerator for Security Applications,” IEEE Transactions on Computers, Vol. 65, No. 10, 2016.

[7] M. A. Bahnasawi, Kh. Ibrahim, A. Mohamed, M. Kh. Mohamed, A. Moustafa, K. Abdelmonem, Y. Ismail, H. Mostafa, “ASIC-Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications,” 28th International Conference on Microelectronics (ICM), 2016.

[8] M. Beaumont, B. Hopkins, T. Newby, “SAFER PATH: Security Architecture using Fragmented Execution and Replication for Protection Against Trojaned Hardware,” Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012.

[9] M. Bidmeshki, G. R. Reddy, L. Zhou, J. Rajendran, Y. Makris, “Hardware-Based Attacks to Compromise the Cryptographic Security of an Election System,” IEEE 34th International Conference on Computer Design (ICCD), 2016.

[10] L. Changlong, Z. Yiqiang, Sh. Yafeng, G. Xingbo, “A System-On-Chip Bus Architecture for Hardware Trojan Protection in Security Chips,” IEEE International Conference of Electron Devices and Solid-State Circuits 2011.

[11] Y. Chen , W. Zhang , H. Li, “A Hardware Security Scheme For RRAM-Based FPGA,” 23rd International Conference on Field programmable Logic and Applications, 2013.

[12] A. Chen, “Comprehensive Assessment of RRAM-based PUF for Hardware Security Applications,” IEEE International Electron Devices Meeting (IEDM), 2015.

[13] A. Chen, X. Sh. Hu, Y. Jin, M. Niemier, X. Yin, “Using Emerging Technologies for Hardware Security Beyond PUFs,” Design, Automation & Test in Europe Conference & Exhibition (DATE), 2016.

[14] V. Costan, S. Devadas, “Security Challenges and Opportunities in Adaptive and Reconfigurable Hardware,” IEEE International Symposium on Hardware-Oriented Security and Trust, 2011.

[15] J. Dofe, Q. Yu, H. Wang, E. Salman, “Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs,” International Great Lakes Symposium on VLSI (GLSVLSI), 2016.

[16] L. Fiorin, A. Ferrante, K. Padarnitsas, F. Regazzoni, “Security Enhanced Linux on Embedded Systems: a Hardware-accelerated Implementation,” 17th Asia and South Pacific Design Automation Conference, 2012.

[17] A. P. Fournaris, “Toward Flexible Security and Trust Hardware Structures for Mobile-Portable Systems,” IEEE Latin American Transactions, Vol. 10, No. 3, 2012.

[18] D. Fujimoto, M. Nagata, Sh. Bhasin, J. Danger, “A Novel Methodology for Testing Hardware Security and Trust Exploiting On-Chip Power Noise Measurement,” The 20th Asia and South Pacific Design Automation Conference, 2015.

[19] G. Gayathri, T. Thangam, M. Kasthuri, “An Efficient Logic Obfuscating Strategy for Hardware Security Using SIC Generator,” International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017.

[20] S. Ghosh, M. Khan, A. De, J. Jang, “Security and Privacy Threats to On-Chip Non-Volatile Memories and Countermeasures,” IEEE/ACM International Conference on Computer-Aided Design , 2016.

[21] Z. Gu, G. Han, H. Zeng, Q. Zhao, “Security-Aware Mapping and Scheduling with Hardware Co-Processors for FlexRay-Based Distributed Embedded Systems,” IEEE Transactions on parallel and distributed systems, Vol. 27, No. 10, 2016.

[22] P. Gu, Sh. Li, D. Stow, R. Barnes, L. Liu, Y. Xie, E. Kursun, “Leveraging 3D Technologies for Hardware Security: Opportunities and Challenges,” International Great Lakes Symposium on VLSI (GLSVLSI), 2016.

[23] Y. Hori, T. Katashita, A. Sasaki and A. Satoh, “SASEBO-GIII: A Hardware Security Evaluation Board Equipped with a 28-nm FPGA,” The 1st IEEE Global Conference on Consumer Electronics, 2012.

[24] A. S. Iyengar, S. Ghosh, K. Ramclam, “Domain Wall Magnets for Embedded Memory and Hardware Security,” IEEE journal on emerging and selected topics in circuits and systems, Vol. 5, No. 1, 2015.

[25] R. Jarvis and M. G. McIntyre, ‘‘Split manufacturing method for advanced semiconductor circuits,’’ U.S. Patent 7 195 931, 2004.

[26] H. Ju, Y. Kim, Y. Jeon, J. Kim, “Implementation of a Hardware Security Chip for Mobile Devices,” IEEE Transactions on Consumer Electronics, Vol. 61, No. 4, 2015.

[27] A. Kahng et al., ‘‘Watermarking techniques for intellectual property protection,’’ IEEE/ACM Design Automation Design Conference, 1998.

[28] S. Kan, M. Ottavi, J. Dworak, “Enhancing Embedded SRAM Security and Error Tolerance with Hardware CRC and Obfuscation,” IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), 2015.

[29] L. Karter, L. Ferhati, I. Tafa, “Security Evaluation of Embedded Hardware Implementation,” Science and Information Conference, 2015.

[30] L. Kim, John D. Villasenor, “Dynamic Function Verification for System on Chip Security Against Hardware-Based Attacks,” IEEE transactions on reliability, Vol. 64, No. 4, 2015.

[31] L. Kim, J. D. Villasenor, “Dynamic Function Replacement for System-on-Chip Security in the Presence of Hardware-Based Attacks,” IEEE Transactions on reliability, Vol. 63, No. 2, 2014.

[32] P. C. Kocher, ‘‘Leak-resistant cryptographic indexed key update, ’’ U.S. Patent 6 539 092, 2003.

[33] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, ‘‘Introduction to differential power analysis,’’ J. Cryptogr. Eng., vol. 1, no. 1, 2011.

[34] S. Koley, P. Ghosal, “Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions,” IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing, 2015.

[35] F. Koushanfar, G. Qu, and M. Potkonjak, ‘‘Intellectual property metering,’’ Inf. Hiding Workshop, 2001.

[36] F. Koushanfar et al., ‘‘Can EDA combat the rise of electronic counterfeiting?’’ IEEE/ACM Design Autom. Conf., 2012.

[37] X. Liang, K. Zhang, X. Shen, X. Lin, “Security and privacy in mobile social networks: challenges and solutions,” IEEE Wireless Communications, Vol: 21, Pages: 33 – 41, 2014.

[38] K. J. Lin, Ch. P. Weng, T. K. Hou, “Enhance Hardware Security Using FIFO in Pipelines,” 7th International Conference on Information Assurance and Security (IAS), 2011.

[39] S. Lukacs, A. V. Lutas, D. H. Lutas, Gh. Sebestyen, “Hardware Virtualization Based Security Solution for Embedded Systems,” IEEE International Conference on Automation, Quality and Testing, Robotics, 2014.

[40] A. Maruaisap, P. Kumhom, “A Hardware-Based Security Scheme for In-Vehicle CAN,” International Computer Science and Engineering Conference (ICSEC), 2016.

[41] A. Mehta, D. Saif, R. Rashidzadeh, “A Hardware Security Solution against Scan-based Attacks,” IEEE International Symposium on Circuits and Systems (ISCAS), 2016.

[42] J. Milosevic, A. Ferrante, F. Regazzoni, “Security Challenges for Hardware Designers of Mobile Systems,” Mobile Systems Technologies Workshop, 2015.

[43] E. Moghaddam, N. Mukherjee, J. Rajski, J. Tyszer, J. Zawada, “On Test Points Enhancing Hardware Security,” IEEE 25th Asian Test Symposium, 2016.

[44] S. Muehlbach, A. Koch, “Malacoda: Towards High-Level Compilation of Network Security Applications on Reconfigurable Hardware,” ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), 2012.

[45] M. Neagu, Gh. Sebestyen, “Increasing Memory Security through Data Scrambling and Information Entropy Models,” 15th IEEE International Symposium on Computational Intelligence and Informatics, 2014.

[46] N. Potlapally, “Hardware Security in Practice: Challenges and Opportunities,” IEEE International Symposium on Hardware-Oriented Security and Trust, 2011.

[47] A. Pouraghily, T. Wolf, R. Tessier, “Hardware Support for Embedded Operating System Security,” IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2017.

[48] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, ‘‘Security analysis of logic obfuscation,’’ IEEE/ACM Design Automation Conference, 2012.

[49] S. Ray, J. Bhadra, “Security Challenges in Mobile and IoT Systems,” 29th IEEE International System-on-Chip Conference (SOCC), 2016.

[50] G. S. Rose, N. McDonald, L. Yan, B. Wysocki, “A Write-Time Based Memristive PUF for Hardware Security Applications,” IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2013.

[51] G. S. Rose, J. Rajendran, N. McDonald, R. Karri, M. Potkonjak, B. Wysocki, “Hardware Security Strategies Exploiting Nanoelectronic Circuits,” 18th Asia and South Pacific Design Automation Conference (ASP-DAC), 2013.

[52] M. Rostami, F. Koushanfar, J. Rajendran, R. Karri, “Hardware Security: Threat Models and Metrics,” IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2013.

[53] M. Rostami, F. Koushanfar, R. Karri, “A Primer on Hardware Security: Models, Methods, and Metrics,” Proceedings of the IEEE, Vol: 102, Pages: 1283 - 1295, 2014.

[54] A. Sengupta, “Hardware Security of CE Devices,” IEEE Consumer Electronics Magazine, 2017.

[55] A. Sengupta, “Hardware Vulnerabilities and Their Effects on CE Devices: Design for Security Against Trojans,” EEE Consumer Electronics Magazine, 2017.

[56] A. Sengupta, S. Bhadauria, S. P. Mohanty, “TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling with Optimal Loop Unrolling Factor During High Level Synthesis,” IEEE Transactions on computer-aided design of integrated circuits and systems, Vol. 36, No. 4, 2017.

[57] K. Shamsi, W. Wen, Y. Jin, “Hardware Security Challenges Beyond CMOS: Attacks and Remedies,” IEEE Computer Society Annual Symposium on VLSI, 2016.

[58] Zh. Shen, X. Wu, “An Improved Security Method for Mobile Agent System by Using Trusted Computing Platform,” International Conference on Intelligent Computation Technology and Automation, 2010.

[59] D. M. Shila, V. Venugopal, “Design, Implementation and Security Analysis of Hardware Trojan Threats in FPGA,” IEEE ICC-Communication and Information Systems Security Symposium, 2014.

[60] M. Stanojlovic and P. Petkovic, ‘‘Strategies against side-channel-attack,’’ Small Syst. Simul. Symp., 2010.

[61] A. Syed, M. Lourde R., “Hardware Security Threats to DSP Applications in an IoT network,” IEEE International Symposium on Nanoelectronic and Information Systems, 2016.

[62] SypherMedia, ‘‘Syphermedia library circuit camouflage technology.’’ [Online]. Available: http://www.smi.tv/solutions.htm

[63] thebestvpn, “Cyber Security Statistics,” online: https://thebestvpn.com/cyber-security-statistics-2018/

[64] T. Thangam, G. Gayathri, T. Madhubala, “A Novel Logic Locking Technique for Hardware Security,” International Conference on Electrical, Instrumentation and Communication Engineering, 2017.

[65] A. Thiruneelakandan, T. Thirumurugan, “An Approach Towards Improved Cyber Security By Hardware Acceleration Of Openssl Cryptographic Functions,” International Conference on Electronics, Communication and Computing Technologies, 2011.

[66] Trusted Computing Group, online: https://trustedcomputinggroup.org/

[67] UK government, “Almost half of UK firms hit by cyber breaach or attack in the the past year,” online: https://www.gov.uk/government/news/almost-half-of-uk-firms-hit-by-cyber-breach-or-attack-in-the-past-year

[68] M. Wachs, D. Ip, “Design and Integration Challenges of Building Security Hardware IP,” 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015.

[69] X. Wang, Q. Shen, P. Du, R. Zhang, W. Wang, L. Li, B. Xu, H. Ji, “Hardware-Assisted Monitoring for Code Security in Embedded System,” IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing, 2015

[70] Y. Wang, Y. Alshboul, “Mobile Security Testing Approaches and Challenges,”First conference on Mobile and Secure Services, 2015.

[71] J. B. Wendt, F. Koushanfar, and M. Potkonjak, ‘‘Techniques for foundry identification,’’ Design Automation Conference, 2014.

[72] T. Wiersema, S. Drzevitzky, M. Platzner, “Memory Security in Reconfigurable Computers: Combining Formal Verification with Monitoring,” International Conference on Field-Programmable Technology, 2014.

[73] J. Zhang, “A Practical Logic Obfuscation Technique for Hardware Security,” IEEE Transactions on very large scale integration (VLSI) systems, Vol. 24, No. 3, 2016.

[74] H. Zhou, Ch. Wu, M. Jiang, B. Zhou, W. Gao, T. Pan, M. Huang, “Evolving Defense Mechanism for Future Network Security,” IEEE Communications Magazine, 2015.