Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.3, 2018, pp.28-32
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2018.7.3.1904

Survey on White-Box Attacks and Solutions

V. Porkodi[1], M. Sivaram[2], Amin Salih Mohammed[3] and V. Manikandan[4]
[1,3,4]Assistant Professor, [2]Associate Professor,
Lebanese French University, Department of Information Technology, Erbil, Iraq
[3]Assistant Professor, University of slahaddin, Department of Software Engineering, Erbil, Iraq
E-Mail: porkodi.sivaram@lfu.edu.krd, sivaram.murugan@lfu.edu.krd, kakshar@lfu.edu.krd, v.manikandan@lfu.edu.krd

(Received 27 August 2018; Revised 10 September 2018; Accepted 30 September 2018; Available online 9 October 2018)

***Abstract* - This Research paper provides special white-box attacks and outputs from it. Wearable IoT units perform keep doubtlessly captured, then accessed within an unauthorized behavior due to the fact concerning their bodily nature. That case, they are between white-box attack systems, toughness the opponent may additionally have quantity,visibility about the implementation of the inbuilt crypto system including complete control over its solution platform. The white-box attacks on wearable devices is an assignment without a doubt. To serve as a countermeasure in opposition to these problems in such contexts, here analyzing encryption schemes in imitation of protecting the confidentiality concerning records against white-box attacks. The lightweight encryption, intention in accordance with protecting the confidentiality over data towards white-box attacks is the recently stability good algorithm. In that paper, we read the extraordinary algorithms too.**

***Keywords:* Wearables, Internet of Wearable Things, Personally Identifiable Information, Unauthorized Exposure, Privacy Challenges, Delegation of Use, Attack Surfaces**

I. INTRODUCTION

IoT is the network of physical devices and other items such as electronics, software, sensors, actuators and network connectivity. Privacy gives that personal information are collected, processed, protected and destroyed legally and fairly. Security controls limit access to personal information and protection against its unauthorized use. Wearable consumer electronic devices, such as smart wristbands, watches, glasses, and helmets, are rapidly becoming important for sensing, communication, and computing in peoples' daily lives. The Fact that the acquired data are transmitted via wireless communication and highly sensitive to consumers' privacy, wearable devices require protection measures for data confidentiality. Without effective protection, the private data on consumers, such as eyesight, blood pressure, heartbeat frequency, or even location can be exposed. These data may further reveal a person's health state, medical condition, and moving/living, or even indicate some extremely private affairs. From the security researcher's perspective, wearable devices are potentially located in a typical white-box attack context (WBAC), where the adversary may have total visibility of the

Implementation of the built-in a cryptosystem, with full control over its execution platform. As a countermeasure, White-box encryption schemes (WBES) have been devised to provide practical-level protection for implementations of symmetric encryption schemes. Now in this era, there is a huge rise in the field of the internet of things and wearable devices in particular. As with other new ,highly problematic digital technologies, IoT and wearable tech will challenge existing social, economic and legal norms. Wearable consumer electronic devices, are rapidly becoming important for sensing, communication, and computing in peoples' daily lives. These raise a variety of privacy and safety problems. So here studying an effective way to the privacy and security of wearable IoT devices.

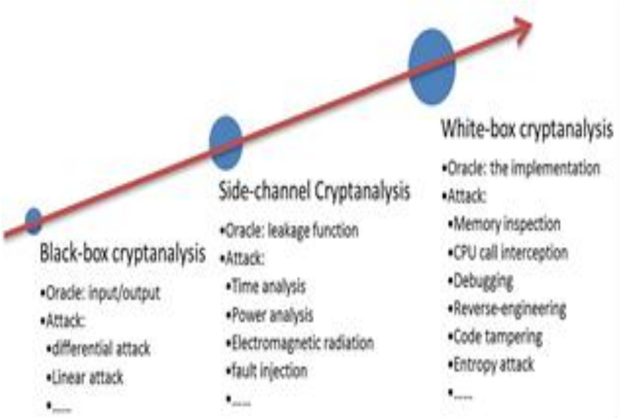

Fig. 1 Threats in black-box,grey-box, and white-box contexts

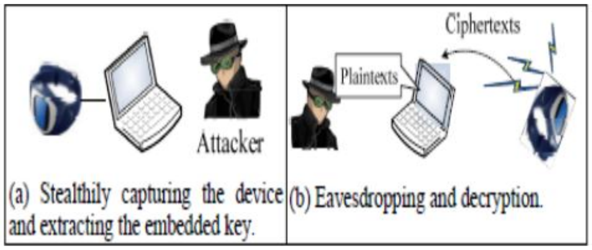
Attacker
(a) Stealthily capturing the device and extracting the embedded key.
Ciphertexts
Plaintexts
(b) Eavesdropping and decryption.

Fig. 2 Stealthy attacking process

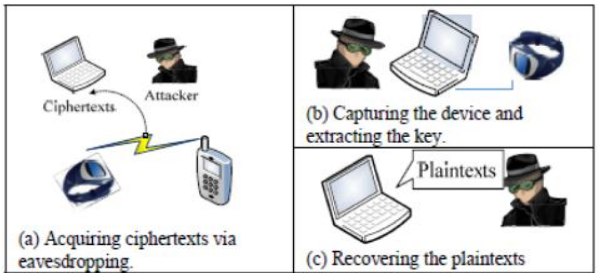
Attacker
Ciphertexts
(a) Acquiring ciphertexts via eavesdropping.
(b) Capturing the device and extracting the key.
Plaintexts
(c) Recovering the plaintexts

Fig. 3 Exposed attacking process

Now in this era, there is a huge rise in the field of internet of things and wearable devices in particular. As with other new and highly problematic digital technologies, IoT and wearable tech will challenge existing social, economic and legal norms. Wearable consumer electronic devices ,are rapidly becoming important for sensing, communication, and computing in peoples' daily lives. These raise a variety of privacy and safety problems.This new era of Internet of Things (IoT) and wearable devices, small embedded devices loaded with sensors collects information from its surroundings, then process it and relay it to remote locations for further analysis. The question of the possibility and effects of compromising such devices. So here studying an affective way to the privacy and security of wearable IOT devices using White-Box Encryption Scheme.

There are two categories of security models for symmetric encryption schemes in WBACs, and they capture the security requirements of encryption and decryption. The security model of decryption is mainly adapted from the scenario of protecting decryption modules in digital right management systems, In this paper, we focus on the security of encryption and the implementation of encryption algorithms (rather than decryption algorithm) in WBACs because wearable devices are generally responsible for encrypting the acquired data.

Unbreakability of a white-box implementation means that, even if an adversary has full access to the implementation, it is still unable to extract the embedded key information. One-wayness of a white-box implementation means that, even if an adversary has full access to the implementation, it is still unable to decrypt the ciphertexts. Clearly, the former definition is weaker than the latter definition.

II. LITERATURE SURVEY

Here systematically study the security issues in wearable communications. Specifically, we start with an overview of security concerns for typical wearable applications.As a key part of wearable technology, the communications among multiple wearable devices lead to significant security concerns because wearables often store and process sensitive personal information (e.g., sensed daily activities).[1]. In addition, because of the portable and ubiquitous nature, wearable devices may have to operate in unknown or hostile environments, further raising the possibility of being attacked by adversaries. Single-Person Entertainment applications, wearable devices are usually designed to support one single user. An example is shown in Fig. 2, which depicts a wearable gaming system that monitors the movements of a user and transmits the monitored data to a remote console. Then the wearable devices receive feedback from the console via the controller and convey it to the user through headphones, video glasses, vibrating alerts, and so on. The most critical security concern for such a single-person entertainment application is the privacy of the device bearer. In particular, the bearer may consider the data captured and transmitted through wearable devices to be private and would not willingly disclose it to a third party.

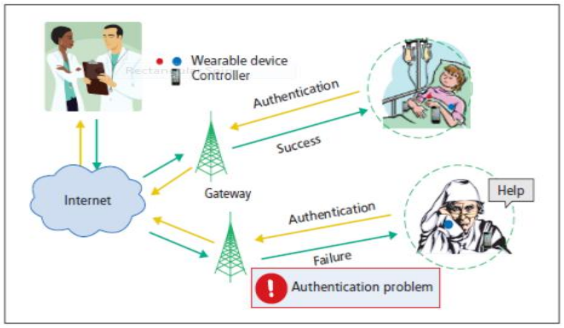

Fig. 4 Main security concern for single-person healthcare or assisted living

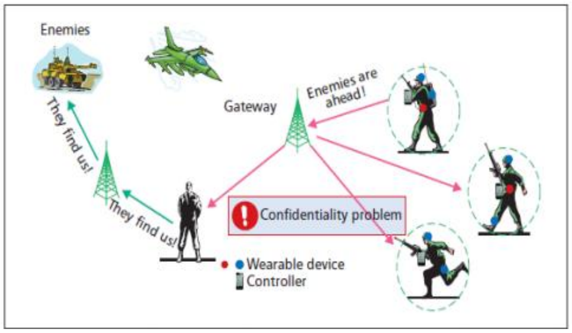

Fig. 5 Main security concern for multi-soldier battle support systems

Patient data should be protected as it carries sensitive personal information that might be exploited by agents such as insurance companies, or a patient may simply not want unauthorized persons to know his/her health conditions. On the other hand, healthcare wearable devices provide critical life support; thus, a malicious instruction may result in catastrophic/fetal outcomes; therefore, a critical challenge is to properly authenticate the instructions received by all wearable devices before using them to reconfigure the wearables. Here in this proposes a layered architecture for the secured wearable communication. A layered adaptive security architecture that consists of the following four layers: secure wearable devices, secure controller, secure single network for wearable communications, and secure ubiquitous wearable connections. Secure wearable devices achieved by sharing secrets established by authenticated key management protocols, or by upper layer protocols such as TSL, if the wearable devices can afford the corresponding computational overhead. Secure controller layer requires strong access control and cryptographic mechanisms to prevent unauthorized exposure of the data and unauthorized changes of device/system settings.An access control mechanism to secure the controller should be carefully designed to provide both access control and desired flexibility. Secure single network for wearable communications security services required here include confidentiality, authentication, integrity, and replay protection. These security services can be granted through encryption and message authentication code. A reasonably long sequence number and a nonce should be used to guarantee freshness and to protect against replay attacks.

Note that the secure single network for wearable communications layer provides functions similar to the security layers in IEEE 802.15.4 and IEEE 802.15.6, which are handled at the MAC layer. Ubiquitous wearable connections are realized by the successful interactions between multiple networks consisting of different wearable devices, an interaction mechanism in which each network contributes data to a centralized server, which in turn aggregates the information collected from multiple networks for applications such as disease surveillance.

Privacy and Security in Internet of Things and Wearable Devices[2]. Examples which represent each category, the Google Nest Thermostat and the Nike+ Fuelband, are selected ,and show how current industry practices of security as an afterthought or giving an add-on affect the resulting device and the potential effects to the user’s security and privacy.

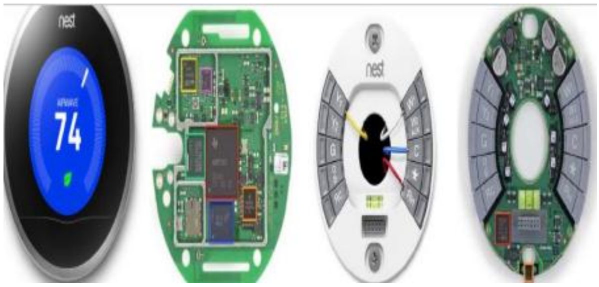

Fig. 6 Front (left) and backplate (right) of a Nest Thermostat (credit: Nest, iFixit)

Due to the short time to market engineers are given to finish a product, believe that most of the current IoT and wearable devices suffer from similar issues. Software protection becomes ineffective if the hardware is vulnerable to attack. This raises safety and privacy issues with users, is their information safe? Moving forward, will continue to probe other IoT devices for security, with the goal of finding vulnerabilities in their hardware. Ultimately, this will lead to a better understanding of design issues and how to correct them.Will attempt to build prototypes of smart devices that utilize our proposed chain of trust to test for their viability and ability to prevent malicious attacks.

The smart watches and mobile wearable devices have becom the rapid dominant sensing, computing and communication devices in peoples’ daily lives.[3] Mobile crowd sensing is an emerging technology based on the sensing and networking capabilities of such mobile wearable devices. MCS has shown great potential in improving peoples’ quality of life, including healthcare and transportation, and thus has found a wide range of novel applications. However, the privacy of the user and data trustworthiness are the two critical challenges faced by MCS. Here introduce the architecture of MCS and showing its unique characteristics and advantages over traditional wireless sensor networks, which gives results in the inapplicability of most existing WSN security solutions. Wireless broadband connections, MCS can operate in an environment which is not feasible or economical for WSNs. Second, since mobile wearable devices have much more resources than sensor nodes in terms of computing power, memory, and energy, more requirements can be met by MCS applications. Third, sensing devices in MCS are mobile in nature. Therefore, they can collect spatio-temporal data in a much easier way than traditional WSNs. Fourth, the sensing process is more intelligent as participants can take control of the sensing process. Fifth, sometimes WSNs have high installation and maintenance cost, and possibly insufficient node coverage. However, as MCS leverages existing sensing devices and communication infrastructure, there is virtually no establishment cost.

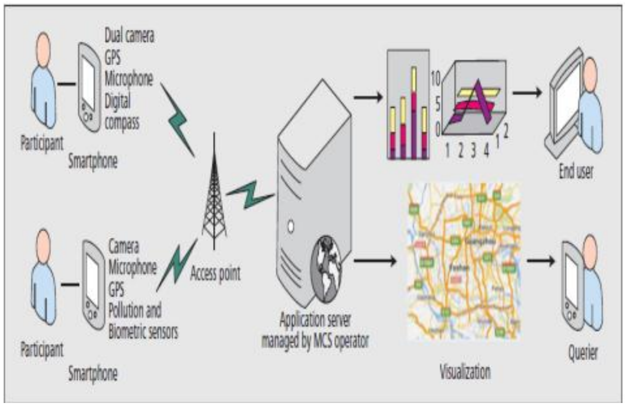

Fig. 7 The architecture of a typical mobile crowd sensing application.

MCS is an innovative computing paradigm that bears great potential and can lead to a wide range of novel applications relating to, for example, environmental monitoring, transportation, and entertainment. In this article, presented the advantages of MCS over traditional WSNs. At the same time, also identified two important challenges of MCS, user privacy and data trustworthiness. They are the two major barriers to the success and massive deployment of MCS systems. It is important to overcome these challenges in order to move this field forward.

In the Era of the Internet of Wearable Things, the Internet undergoes a fundamental transformation as billions of connected ”things” surround us and embed themselves into the fabric of our everyday lives.[4] However, this is only the beginning of true convergence between the realm of humans and that of machines, which materializes with the advent of connected machines worn by humans, or wearables. The resulting shift from the Internet of Things to the Internet of Wearable Things (IoWT) brings along a truly personalized user experience by capitalizing on the rich contextual information, which wearables produce more than any other today’s technology.

White-Box attack context is the setting that the attacker has total access to the software execution and can observe or manipulate the dynamic execution of whole or part of the algorithm[5]. In order to protect AES software operated in such context, Chow et al. Designed an obfuscated AES implementation with a set of key-dependent look-up tables, which was proposed at SAC 2002. A secure implementation of White-Box AES after a detail analysis of B-Attack technique on CWB-AES implementation. In this scheme, the obfuscation works on at least two cells of an AES state, the attacker cannot divide it into small ones and remove it using a B-Attack. This scheme is more secure than CWB-AES. The time complexity of White-Box AES implementation is O(224), which can be performed in seconds on PCs. This scheme is slower than CWB-AES (O(220)) and need more size. While it is more secure, it does come at quite a substantial price. Careful choices must be taken as to where and how to employ it.

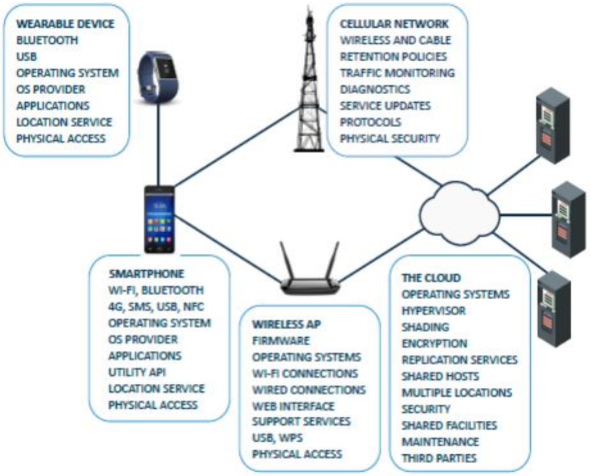

Fig. 8 Classification of the attack surfaces for wearables

Here Whitebox implementation requires less memory space than that of Chow et al. implementation[6]. Here solution relies on using the dual ciphers and raises the complexity of Billet et al. attack from 230 to 291. The structure changes make the original cipher more intricate for the adversary such that he has to repeat the attack of Billet et al. for all possible combinations of dual ciphers. Raising the attack complexity to 291 operations does not provide theoretical security for a 128-bit AES decryption key, it is useful from a practical perspective. In addition to providing the white-box AES with a protection against practical attacks, design implementation is comparable in time and space requirements to that of Chow et al.

Existing algorithms for white-box attack contexts require large memory footprint and not applicable for wireless sensor networks scenarios.[7] As a countermeasure against the threat in this contextin the proposed method a class of lightweight secure implementations of the symmetric encryption algorithm SMS4. The basic idea of this approach is to merge several steps of the round function of SMS4 into table lookups, blended by randomly generated mixing bijections. Therefore, the size of the implementations are significantly reduced while keeping the same security efficiency. The strong white-box SMS4 encryption algorithm is immune from all known attacks and their potential modifications against SMS4. Hence, it is expected to provide a much longer protection time. Moreover, they can also serve as countermeasures against a variety of side-channel attacks such as fault analysis, electromagnetic analysis and power analysis.

In this proposel an approach to select the values of these parameters[8], based on required latency and battery lifespan. In an example case we demonstrated how CC2540 SoC can be configured to last for a year on a single CR2032 coin cell battery, while providing ability to refresh session key twice a day and keeping latency under two seconds.

Embedded devices with constrained computational resources,such as wireless sensor network nodes ,electronic tag readers,roadside units in vehicular networks,and smart watches and wristbands, are widely used in the IoT.[9] Many of such devices are deployed untrustable environments,and others may be easy to lose leading to possible capture by adversaries.Accordingly ,in the context security research , these devices are running in white-box attack context, were the adversery may have total visibility of the implementation of the build into the system with the full control over its execution.The proposed encryption scheme is executed with secret components specialized for resource constrained devices for white box attacks, and the encryption algorithm requires relatively small amount of static data ,ranging from 48 to 92 KB. Security and the efficiency of the proposed scheme have been theoreticaly analysed with positive results and experimental evolution have indicated thjat the scheme satisfies the resource constraints in terms of limited memory use and low computational cost. Ultra-Lightweight White-Box Encryption Scheme for Securing Resource-Constrained IoT Devices is the second most recently implemented system.

The Light-Weight White-Box Encryption Scheme with Random Padding for Wearable Consumer Electronic Devices[10] scheme originates from the consideration of the paradox of designing WBESs based on substitution-affine networks: if all the components are bijective, then the implementation of the WBES’s encryption algorithm can be divided into a series of short substitutionaffine networks of less than five layers, which are subject to known attacks, such as . Otherwise, the ciphertexts cannot be decrypted because non-bijective transformations are not invertible. At the same time, also consider the characteristics of wearable devices: 1) they are usually embedded devices with limited storage and computational power; and 2) in many applications, only a small piece of data is sent each time. In a “one stone two birds” manner, proposed solution uses random padding that does not need to be correctly decrypted as part of the input. It enables us to insert non bijective linear transformations in each round to achieve security in WBACs, and it randomizes ciphertexts to support extra security features in BBACs as a byproduct. Moreover, the substitution on each piece of random padding (3 bits) depends on the corresponding piece of plaintext (5 bits). Finally, instead of using strong components with large parameters, small parameters are used to fit resource-constrained wearable devices. classical cryptanalysis techniques against block ciphers, such as linear analysis and differential analysis, mainly assume that all the components (e.g., substitutions and diffusion transformations) are publicly known and the only secret is the cipher key. Therefore, these techniques are not prominent threats against the proposed scheme, which is built on a number of secret substitutions and diffusion matrices. Finally, random padding not only enables the involvement of nonbijective transformations in each encryption round, but also provides an extra security margin for encryption in electronic codebook (ECB) mode.And it is the most recently proposed algorithm for encryption of IoT wearable devices.

III. CONCLUSION

Device capture attacks have been identified as the most dangerous security challenge to wearable consumer electronic devices. Here in this survey, studied different white-box attacks and different solution methods. And the recently proposed scheme was A light-weight WBES with random padding for securing implementations of symmetric encryption in wearable devices. The main novelty of the scheme is that random padding does not need to be correctly decrypted and thus enables non-bijective linear transformations to be used in each encryption round to achieve security in WBACs. Additionally, as an extra security margin in BBACs, limited ciphertext randomness is acquired with almost no additional cost, either in computation or communication overheads. The storage cost of static data for encryption is only 95 KB, and the time cost is relatively small on various devices, according to our experimental results, which indicate that the scheme fits applications in wearable computing.

REFERENCES

[1] Shengling Wang, Rongfang Bie, Feng Zhao, Nan Zhang, Xiuzhen Cheng, and Hyeong-Ah Choi, "Security in Wearable Communications", *IEEE Network,* September/October 2016.

[2] Orlando Arias, Student Member, IEEE, Jacob Wurm, Khoa Hoang, and Yier Jin, Member, IEEE "Privacy and Security in Internet of Things and Wearable Devices", *IEEE Transactions on MultiScale Computing Systems*, 2015.

[3] Daojing He, Sammy Chan and Mohsen GuizanUser Privacy And Data Trustworthiness in Mobile Crowd Sensing", *IEEE Wireless Communication*, February 2015.

[4] Aleksandr Ometovy, Sergey Bezzateev?, Joona Kannistoy,JarmoHarjuy,SergeyAndreevy,"Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things", *IEEE*, pp. 2327-4662, 2016.

[5] Yaying Xiao Shanghai Jiao Tong University Shanghai, China, Xuejia Lai Shanghai Jiao "A Secure Implementation of White-Box AES", *IEEE*, 2009.

[6] K.-H. Rhee and D. Nyang "Protecting White- Box AES with DualCiphers" ICISC 2010, LNCS 6829, pp. 278–291, 2011

[7] Yang Shi, Wujing Wei and Zongjian He"A Lightweight White-Box Symmetric Encryption Algorithmagainst Node Capture for WSNs", *Sensors*, Vol. 15, pp. 11928-11952, 2015.

[8] I. Muslukhov, S. T. Sun, P. Wijesekera, Y. Boshmaf and K. Beznosov, "Decoupling data-at-rest encryption and smartphone locking with wearable devices", *Pervasive and Mobile Computing,* Vol. 32, No. 10, pp. 26-34, 2016.

[9] Y. Shi, W. Wei, Z. He, and H. Fan, "An ultra-lightweight whitebox encryption scheme for securing resource-constrained IoT devices," *Computer Security Applications,* Los Angeles, California, pp. 16-29, 2016.

[10] Yang Shi, Xiaoping Wang, and Hongfei Fan, " Light-Weight White-BoxEncryption Scheme with Random Padding for Wearable Consumer Electronic Devices", *IEEE Transactions on Consumer Electronics*, Vol. 63, No. 1, February 2017.