An Assessment of Recent Attacks on Specific Embedded Systems

Khattab M. Ali Alheeti
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, UK
University of Anbar, College of computer - Anbar, Iraq
Kmali@essex.ac.uk

Shoaib Ehsan, Klaus D. McDonald-Maier
School of Computer Sciences and Electronic Engineering
University of Essex
Colchester, UK
{sehsan,kdm}@essex.ac.uk

***Abstract*— In this paper, we present an assessment of recent attacks on embedded systems, in particular mobile phones, wireless sensor networks, unmanned aerial vehicles and unmanned ground vehicles. As these systems become increasingly connected and networked, the number of attacks on them increases exposing them to real threats and risks, particularly when used in mission critical applications. It is necessary to investigate all aspects of the security systems associated with embedded systems in order to help protect these systems from attackers. In this we present a survey on a number of embedded systems to show system vulnerabilities, recent attacks and the security measurements undertaken to protect the embedded systems.**

Keywords-embedded system security; mobile phone security; wireless sensor networks; autonomous vehicles; security unmanned aerial vehicles.

I. INTRODUCTION

Embedded systems are purpose build computers that are designed to perform a specific function or a number of functions. These systems have a vital role in many applications such as manufacturing, commerce and are sometimes applied in mission critical applications. The embedded systems in electronic devices, such as tablets, smart phones, network routers, smart cards, and networked sensors, have become increasingly popular in recent years [1].

The two main factors that allow attackers to target such systems are the complex nature of the embedded systems and their continuous connection with the Internet. Malicious users exploit vulnerabilities in embedded systems in order to steal important data, damage or disable the entire system. In the past, the number of attacks on embedded systems were limited by the fact that the systems were independent, but has changed due to increased use of internet-connected devices [2]. The security of embedded systems has become a serious problem [3].

This paper surveys current research into the security of several specific embedded systems. We selected four types of embedded systems for our analysis security: mobile smart phones, wireless sensor networks, unmanned ground vehicles and unmanned aerial vehicles. We selected these specific embedded systems due to their increasing importance:

- Smart phones: these devices play a significant role in our daily lives, according to ABI Research, the number of attacks smart phones has increased by 261% in the past two years [4].
- Wireless sensors: These devices are of interest because of their small size and their low power usage. They are easily placed in any environment, which makes them effective in monitoring both indoors and outdoors [5].
- Unmanned aerial vehicles: These are of interest because they have both national and international significance in aerial surveillance and monitoring, where they are increasingly considered more effective and successful than airplanes [6].
- Unmanned ground vehicles: These robotic vehicles are of interest because they are effective in reducing human errors and saving passengers' lives [7].

It is important to identify the threats, vulnerabilities and attacks in order to determine the future security directions that can be used to protect embedded systems.

The main objectives of this paper are:

- Identifying the vulnerabilities of embedded systems.
- Differentiating the types of attacks on the four types of embedded systems of interest.

Exploring security mechanisms used to protect these systems.

In Section II we will look at the current security properties of embedded systems, then, in Section III we will identify vulnerabilities and threats. In Section IV we will identify attack directions and in Section V we will review possible security countermeasures for embedded systems. In Section VI we will present our conclusion.

II. SECURITY PROPERTIES

In general, security in embedded systems must include the following three properties: confidentiality, integrity and the ability to authenticate [8]. Security should also prevent unauthorized access to the system or network. In this section, we briefly explain each property: Confidentiality refers to preventing attempts to eavesdrop on information by attackers. Integrity refers to keeping data from alteration or illegal manipulation. Lastly, authentication serves to send and receive data securely only between the intended users. Moreover, another important feature of security systems is keeping system resources available to users, some attackers seek to achieve a Denial of Services (DoS). Finally, a security system should have the ability of resisting to the system itself. Typically, attackers exploit the vulnerabilities instead of attacking the security system directly.

III. Vulnerabilities & threats

We believe that all human-made systems contain vulnerabilities, which can potentially be exploited by attackers [9]. In order to provide an efficient security system that has the ability to protect the system, an analysis of potential attacks on embedded systems was undertaken.

A. Vulnerabilities

Embedded systems have several weaknesses which can lead to the loss or unintended capture of information, disruption, tampering or the destruction of the entire system. These vulnerabilities are [1]:

- Energy drainage (exhaustion attack): The limitations on available energy in embedded systems is considered one of the weaknesses that can be exploited by attackers by "increasing the computational load, reducing sleep cycles, or increasing the use of sensors or other peripherals" [1].
- Physical intrusion (tampering): The proximity of the attacker to the embedded system can allow him to link to it directly by making power analysis attacks or snooping attacks on the bus system.
- Network intrusion (malware attack): Networks in embedded systems are exposed to the same threat as traditional networks such as buffer overflow attacks.
- Information theft (privacy violations): Data stored on the embedded systems is exposed to unauthorized access that leads to leaked data (cryptographic keys or electronic currency on smart cards).
- Introduction of forged information (authenticity): This threat happens when the data fed to the systems is incorrect or is forged data, which gives inaccurate results (wrong video feeds in security cameras).
- Confusing/damaging of sensors or other peripherals: Is similar to the introduction of incorrect data from the sensors or peripherals (tampering).
- Thermal event (thermal virus or cooling system failure): Embedded systems need to operate in an ideal environment in terms of temperature (high temperature leads to damage).
- Reprogramming systems for other purposes (stealing): Reprogramming embedded systems to change their main function

B. Threat Model

Modelling threats is a security engineering activity to analyse threats to systems or applications in a systematic manner. The main goal of such modeling is to demonstrate that the threats are not obvious or hidden to the developer. This information serves to build a security strategy to protect systems and provide a roadmap for the future data security. By understanding and diagnosing potential risks to the systems, developers can provide a smart way to manage these threats. Modelling threats is considered a powerful tool, because it does not specify simple vulnerabilities, but determines the actual threats against the systems. Embedded software presents a set of unique challenges for developers and designers in order to reduce or eliminate these threats. Some modelling techniques are static analysis, threat modelling and penetration testing.

Threats can be distinguished from vulnerabilities in terms of events. Threats are external events, which are designed to attack or breach the security system by exploiting vulnerabilities that are in the system. They can be resolved or overcome by finding alternative solutions to them, however, threats are constantly changing their approach to attack and steal highly important information or destroy the system through various malicious codes, viruses to deny the service.

IV. Attacks Direction

The increased number of attacks on embedded systems is carried out either using a physical or logical means. Security approaches for these systems must cover multiple aspects: availability, user identification and security contents, storage, network access and communication [10]. Current traditional security systems, such as security protocols (IPSec and SSL) and cryptographic methods are unable to protect some embedded systems because their security systems constitute a kind of an extra burden to the systems, for example, overhead in processing time, data buffering and memory [1]. Attacks against embedded systems can be classified into two types according to their level of access to the system:

A. Physical & Side channel attacks

The attacker can access these devices directly using a physical connection. We have classified physical and side channel attacks into two main categories: invasive and non-invasive attacks. Invasive attacks include intervention or manipulation of the inside system such as [11,12]:

1) Micro-probing: Analyzes the integrated circuits under the microscope.

2) Reverse Engineering: Is used to understand the internal structure of the embedded systems and to learn or simulate their functions.

Noninvasive attacks are attacks that do not need to access the system from the inside. This type of attack is sophisticated and low effort compared to an invasive attack. There are a number of methods employed for this kind of attack [12]:

1) Timing analysis: attackers try to violate the cryptosystem by analyzing the time it takes to execute computations. [14,15].

2) Power analysis: Attackers gather information by measuring the energy consumed. There are two ways to analyze, a simple power analysis (SPA) and differential power analysis (DPA) [16].

3) Electromagnetic analysis: The attacker can detect information by measuring the electromagnetic radiation emitted by the system [17].

4) Fault injection: this is a side channel attack and it is subdivided into different types [10,11]:

- Latch-up: injects faults in embedded systems through a sudden change in voltage [18].
- Round reduction reduces the number of rounds of encryption algorithms, this allows the attacker to extract the secret key as well as reverse engineer the system [19].

- Optical fault injection: a technique for changing the random access memory by using the photoelectric effect [20].
- The Bellcore attack: an active attack that exploits incorrect computations in the derivation of the keys for any secret encryption protocols [21].

Side channel attacks are fairly straightforward to implement and can potentially allow attackers to steal confidential information and to leave without trace. Accordingly, security threats for embedded systems can be classified depending on the objectives or the manner of the attack [22].

B. Logical Attacks

The attacker can penetrate the software or cryptographic security systems. Code injection attacks have become the predominant software attack [9], they are the injection of malicious code remotely through the network in order to exploit weakness in the systems application software. Cryptographic attackers exploit weaknesses in the cryptographic protocols (e.g. by guessing the password).

Figure 1 shows common types of attacks on embedded systems:

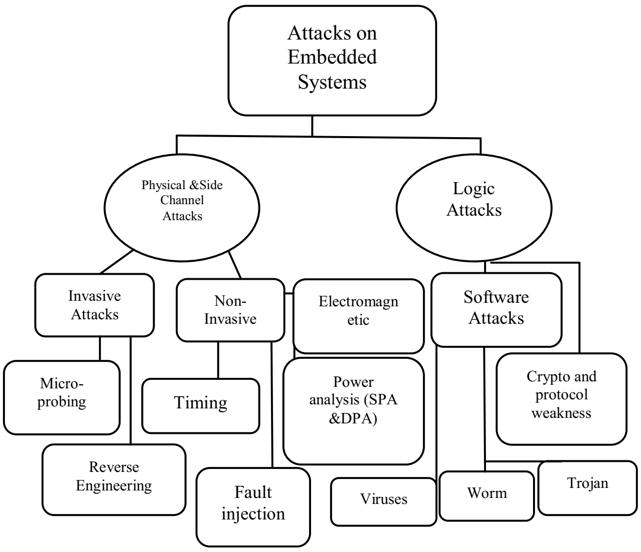

Fig. 1 Common types of attacks on embedded systems

V. Security Countermeasures For Embedded Systems

In the following sections, we list some common types of security countermeasures for embedded systems. Techniques to prevent code injection attacks have been divided into nine sets, based on the system components and techniques used in countermeasures [13]:

a) Architecture based countermeasures.

b) Safe languages.

c) Static code analyzers.

d) Dynamic code analyzers.

e) Anomaly detection techniques.

f) Sand boxing or damage containment approaches.

g) Compiler support.

h) Library support.

i) Operating system based countermeasures.

There are many countermeasures against side-channel attacks [16, 23]:

a) Masking.

b) Window method.

c) Dummy instruction insertion.

d) Code/algorithm modification.

e) Balancing.

f) Other methods such as (Randomization and Blinding).

VI. Attacks And Countermeasure In Embedded Systems

A. Smart Phones

One-sixth of the world uses smart mobile devices such as smart phones and tablets [24]. Smart phone devices are not only used for the purpose of conversation, but for surfing the Internet, sending and storing various data. This makes the devices easily exposed to attackers. These devices are supported by third-party applications, which helped to increase the number of attacks and the emergence of various threats such viruses, malware, worms and Trojan viruses [24]. Third-party applications are installed in the operating system of smart mobile devices, which play an important role in supporting a lot of entertainment applications and service programs. On the other hand, these applications have made mobile devices vulnerable to attacks [25].

Intrusion prevention mechanisms such as encryption and authentication are not sufficient to protect these devices against powerful attacks. Currently, intrusion detection systems are inappropriate for embedded systems or mobile systems due to their added power consumption and memory usage, and new low resource detection systems need to be investigated.

1) Types of Attacks on Smart Phones

Mobile phone devices are exposed to many types of attacks [25]:

a) Malware: This type of attack is designed to reach the device secretly and without the consent of the owner. This type of attack prevents or impedes the use of the device through the exploitation of resources and alters or damages the user's data.

b) Trojan Attackers: Trojans are common in computers nowadays and are used to transmit spam email to Internet users. This type of attack affects also mobile phones and often targets online banking and financial service data.

c) Worm: This type of attack is self-replicating, destroys data and can target mobile applications, lunched from a Trojan attacker.

We can classify the attacks of mobile phone into two types (depend on their operating systems):

a) Cyber attacks: This type of attack allows hackers to access the information that is supposed to be encrypted on operating systems [25]. Attackers can access the encrypted information and bypass the operating system by man-in-the-middle attacks.

Malware attacks: this attack has a direct impact on the operating system [25]. This allows the attacker to erase and transfer all personal information available on mobile phones.

2) Countermeasure Security

Currently there are four steps to reduce or detect malicious code on mobile devices:

a) Monitor: The amount of data traffic across the network [26].

b) Increase system defences: Which in turn reduces the possibility of installing malware attacks on the devices, by using such tools as sandboxes [25].

c) Develop admission control mechanisms: To these devices to make access difficult and only allow access through the use of trusted hardware [26].

d) Accessing: The file system of the mobile and scanning the data in the computer [26].

B. Wireless Sensor Network

Security in wireless sensor networks is a very important issue as they are often deployed in mission critical environments with limited resources.

Intrusion detection is a common method to defend the wireless sensor network, yet it is not an efficient one. A devastating attack in wireless sensor networks is the sleep deprivation attack, which leads to the depletion of power. The aim of this attack is to increase the power consumption of the target node, which leads to reduced battery life. Current studies on sleep deprivation attacker focused on mitigating the use of MAC based protocols such as S-MAC, T-MAC, B-MAC, etc. [5].

Wireless sensor network refers to a system that consists of a set of nodes that have limited resources and low-cost work-sensing information from the external environment which can be sent to sink code. They include many applications, such as traffic and environmental monitoring, health care and military applications. However, wireless sensor networks are susceptible to a number of attacks such as jamming, battery drainage, routing cycle, Sybil and cloning. Due to the limited energy resources, memory and computation of these sensor nodes, complex security mechanisms cannot be implemented. Therefore, it is important to find an efficient approach to protect wireless sensor networks.

Most attacks against the network layer of wireless sensor networks are:

a) Spoofed, altered, or replayed routing information

b) Selective forwarding

c) Sinkhole attacks

d) Sybil attacks

e) Wormholes

f) HELLO flood attacks

The DoS attacker can focus on the different layers of the network protocols:

a) Physical layer: this attack may be jamming and tampering.

b) Link layer: this attack may be a collision, exhaustion and unfairness.

c) Network layer: this attack may be neglected and greed, homing, misdirection and black holes

d) Transport layer: this attack may be malicious flooding and desynchronization.

C. Unmanned Aerial Vehicles

Unmanned Aerial Vehicles (UAV) have been exposed to several cyber-attacks over the past few years [27], since they lack countermeasures. A recent example is the capture of a US UAV by Iranian forces, and the current view is that it was captured due to a weakness in the aircraft GPS system, which helped the attacker to take control of the plane [28]. A second theory is a crash landing of the UAV due to a technical malfunction [28]. Both theories assert that the problems are security challenges. Threats for the mission of UAVs are the connection to ground control, which leaks sensitive data and in turn leads to loss of control.

The quantity and quality of data carried by unmanned aircraft constitutes a rich target allowing the attacker to steal information or manipulate it, such was the loss of a Sentinel to Iranian military forces (RQ-170) in 4 Dec 2011 [28] and "the keylogging virus that infected the U.S. UAV fleet at Creech Air Force Base in Nevada in September 2011" [29]. This shows us that the security measures in the past were not able to protect these UAVs. Solid protection mechanisms to protect against attacks must be developed.

In this paper, we investigate recent attacks on the unmanned aircraft and develop a plan to assess the risks to this type of aircraft, depending on the infrastructure for communication. System designers try to minimize the vulnerabilities in the system that can be exploited by the attacker. If the attacker cannot have physical access to the plane, they will try to reach it remotely. In this case, the attacker might exploit that this type of planes depend largely on external inputs and might not be able to get a reliable wireless connection to ground control.

There are two types of communications for the UAV, namely [29]:

a) Bidirectional information communication between the UAVs and ground control.

b) Communication with the external environment for the receipt of information from the sensors.

1) Recent Attacks

Recently, attacks can be classified into three types [30]:

a) Hardware Attack: In this type, attackers have the ability to access the components of the UAVs directly.

b) Wireless Attack: In this type, attackers can achieve their attacks by using one of the wireless interfaces of the UAVs.

c) Sensor Spoofing: In this type, attackers can transfer false data to the UAVs through the on-board sensors of the drone itself.

2) Proactive Risk Assessment Scheme

Risk is evaluated based on the internal components of the UAV. The risk assessment depends on the type of security that we need to protect the UAV.

a) Although there are several security techniques applied in UAVs, we can observe through the recent attacks that these systems need a stronger security systems to effectively repell attacks.

D. Unmanned Groung Vehicles

In the past decade, mechanical components have been replaced by electronic components creating the so-called semi-autonomous vehicles. These vehicles contain more than 50 electronic control units (ECUs). The motivation for using autonomous vehicles is that they have a positive impact on people's lives by improving the traffic flow and safeguarding the infrastructure from accidents.

Most car companies are installing and updating the firmware in a traditional way, but the trend today is for updates to be installed and updated over the air, the so called firmware updates over the air (FOTA) [31]. This approach carries a lot of benefits, including: is more convenient for the customer and saves time, the update process is faster and improves safety [32]. Unfortunately, the development of this service was accompanied by external threats that target vehicles. Studies show that internal networks for vehicles do not have adequate protection systems against malicious attacks [32], and consequently, they will be easy to penetrate by attackers.

1) Types of Attacks on Unmanned Vehicles

Traditional attacks on vehicles are physical attacks: Cutting break-wire or breaking the lock mechanism. The new technology (FOTA) has led to the emergence of vulnerabilities and new attacks such as cyber attacks. These attacks can install malicious programs that threaten the infrastructure of the vehicle and human life [32]. This attack has been designed to adapt to the limited possibilities of the hardware and software systems in intelligent vehicles. However, we need a mechanism to safeguard the integrity of the information sent to the firmware and prevent unauthorized access by attackers.

Attacks have been classified as follows: indirect physical access, short range wireless access and long range (direct and indirect) wireless access [12].

a) Indirect Physical Access Attacks: This type focuses on a third-party attack that will attack the vehicle later.

- OBD port: Attacker can use the diagnostic port to achieve his attack on the vehicle. The attacker can connect a pass-through device to the OBD port through the WiFi, which can achieve his attack remotely. Vulnerabilities in communications API enable the attacker to achieve his attack remotely (computer).
- CD player: In this type, we can distinguish two vulnerabilities. First, the inclusion of a disk (CD) expected to contain the firmware updates, but in fact, it contains malicious code. Second, decoding the WMA file, this helps to broadcast messages over the bus for the internal network.
- USB port: vehicle media player can access a corrupted file stored on a USB key. This type brings other attacks through smart mobile devices

b) Short Range Attacks: Attacks using short-range wireless networks. This attack can constitute a direct attack by targeting the vehicle's communication, or indirectly through the driver's devices that are usually connected to the vehicle such as smart phones.

- Wireless pairing of mobile devices: Modern vehicles are likely to be coupled with mobile devices. For example, a driver connects their mobile phone with the vehicle via Bluetooth.
- Car-to-car communications: Communication between the vehicle and another vehicle is very important in the exchange of information or between vehicle and infrastructure. The attacker can eavesdrop on the exchange or send fake data.
- Tire Pressure Monitoring System (TPMS): This consists of pressure sensors inside tires by which the data are sent to an electronic control unit via radio frequency emitter. The attacker can eavesdrop on these signals and send false signals from 40 meters to the electronic control unit and trigger a spark alarm light.
- Wireless unlocking: A lot of vehicles have the technology to open their doors remotely. These signals are encrypted and transmitted through the air.

c) Long-range Direct Attacks: This type of attack is implemented via remote control.

- Telephony: detection of several vulnerabilities in the telematic unit. Some of the attacks are done over the 3G network.
- Web browsing: vehicles have a web browser that creates a gateway for the injection of malware.

d) Long-range Indirect Attacks: This kind of attack is indirectly remote controlled.

- App store: owner of a vehicle using an app store to download some programs, which are can be harmful due because they expose the vehicle to attacks such as Trojans.

Side channel triggers: Broadcast signals of a certain Radio Data System (RDS) constitutes a danger to the electronic control units.

2) Security Countermeasures

Encryption systems are considered one of the most effective protection for these systems from attacks. There has been a number of security counter measurements applied on Unmanned Vehicles such as cryptography, software integrity and anomaly detection. Control Area Networks (CAN) are employ as internal networks in cars. These networks do not support unique Electronic Control Unit (ECU) as transmitters or receivers. Hence, it is difficult to know where the message was generated or received. Therefore, traditional intruder detection systems cannot be applied on similar internal networks of semi-autonomous vehicles. It is however possible to apply them to the gateway of the internal networks.

VII. Conclusion

The security of embedded systems is a very important issue that designers and programmers must take into consideration. The importance of security systems is in their application in critical infrastructure exposed to many attacks as well as to minimize the weaknesses that made embedded systems easy to penetrate. We elaborated on four types of embedded systems and security measures for them as well as the type of attacks directed at these systems. We concluded that these systems require sophisticated protection systems that can prevent or reduce the number of attacks. Finally, through our investigati of the vulnerabilities of embedded systems, and recognizing , the different threats, future work on security systems can be customized to the specific characteristics of embedded ssystems

REFERENCES

[1] P. Kocher, R. Lee, G. McGraw, "Security as a New Dimension in Embedded System Design," DAC '04 Proceedings of the 41st annual Design Automation Conference no.1-58113-828-8, pp. 735-760, 2004.

[2] D. K. Nilsson, U. E. Larson, "Secure Firmware Updates over the Air in Intelligent Vehicles," Communications Workshops, 2008. ICC Workshops '08. IEEE International Conference on , no. 978-1-4244-2052-0, pp. 380-384, 2008.

[3] S. Shane Clark, B. Ransford, A. Rahmati, S. Guineau, J. Sorber, Kevin Fu, et al., "WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices," in Proceedings of USENIX Workshop on Health Information Technologies, 2013.

[4] BYOD and Increased Malware Threats Help Driving Billion Dollar Mobile Security Services Market in 2013, ABI Research.

[5] L. Xie et al. "Designing System-level Defenses against Cellphone Malware". In SRDS 2009.

[6] A. Kim, B. Wampler, J. Goppert, "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," Infotech@Aerospace Conferences, no. 978-1-60086-939-6, pp. 1-30, 2012.

[7] U.E. Larson and D.K. Nilsson, ''Securing Vehicles Against Cyber Attacks,'' Proc. 4th Ann. Workshop Cyber Security and Information Intelligence Research, ACM, no. 30, 2008

[8] N. Ouerdi, M. Ziane, A. Azizi and M. Azizi, "Classification Of Attacks On Embedded Systems ," Journal of Computer Science, Vol. 8, no. 11, pp. 1834-1838, 2012.

[9] K. Ali, "Intrusion detection using feed forward neural networks", thesis master,University of Al-albyte, Computer Sciences, 2008.

[10] S. Parameswaran, T.Wolf," Embedded systems security—an overview " Springer Science+Business Medi,LLC 2008, Vol. 12, no. 3, pp. 173–183, 2008.

[11] S. Ravi, A. Raghunathan, P. Kocher,S. Hattangady," Security in embedded systems: design challenges". Trans Embed Comput Syst 3(3):461–491, 2004.

[12] E. Tromer," Information Security – Theory and Reality", Tamper resistance and hardware security, Lecture 12, 2011.

[13] P. Kocher, R. Lee, G. McGraw, "Security as a New Dimension in Embedded System Design," DAC '04 Proceedings of the 41st annual Design Automation Conference no.1-58113-828-8, pp. 735-760, 2004.

[14] S. Ravi, A. Raghunathan," Security in Embedded Systems: Design Challenges," ACM Transactions on Embedded Computing Systems, Vol. 3, no. 3, pp. 461–491, 2004.

[15] S. Mangard, "A simple power-analysis (SPA) attack on implementations of the AES key expansion". In: Lee PJ, Lim CH (eds) Proceedings of the 5th international conference on information security and cryptology (ICISC 2002). Lecture notes in computer science, vol 2587. Springer, Berlin, pp 343–358, 2003.

[16] D. Boneh, R. DeMillo,R. Lipton,"On the importance of eliminating errors in cryptographic computations". J Cryptol 14(2):101–119,2001.

[17] J. Rao,P. Rohatgi P,"Empowering side-channel attacks". Cryptology ePrint Archive, Report 2001/037,2001.

[18] N. Buard, F. Miller, C. Ruby Gaillard, "Latchup effect in CMOS IC: a solution for crypto-processors protection against fault injection attacks?". IOLTS 07. 13th IEEE International On-Line Testing Symposium, 2007 Volume , Issue , PP.63 – 70, 2007.

[19] H. Choukri, M. Tunstall, (2005),"Round Reduction Using Faults" Fault Diagnosis and Tolerance in Cryptography, FDTC 2005, pp. 13-24, 2005.

[20] P. Sergei Skorobogatov, J Ross Anderson,"Optical Fault Induction Attacks" B.S. Kaliski Jr. et al. (Eds.): c_Springer-Verlag Berlin Heidelberg, CHES 2002, LNCS 2523, pp. 2–12, 2003.

[21] G. Artemios Voyiatzis, N. Dimitrios Serpanos, "A Fault- Injection Attack on Fiat-ShamirCryptosystems" proceedings of the 24th International conference on Distributed computing Systems workshops(ICDCSW '04), 2004.

[22] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and othe systems," Advances in Cryptology – CRYPTO'96, Springer-Verlag Lecture Notes in Computer Science, vol. 1109, pp. 104–113, 1996.

[23] Bin zhou, D. Guo feng, "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing", the Physical Security Testing Workshop, no. 60503014 & 60273027 & 60373039, pp. 1-34, 2005

[24] J. Quisquater, D. Samyde D,"Electro magnetic analysis (EMA): measures and counter-measures for smart cards". In: E-smart, pp 200–210,2001.

[25] J. Han, S. Kywe, Q. Yan, F Bao and R Deng " Launching Generic Attacks on iOS with Approved Third-Party Applications" © Springer-Verlag Berlin Heidelberg CNS 2013, LNCS, no. 7954, pp. 72–289, 2013.

[26] B. Kumar Addagada, "Intrusion Detection in Mobile Phone Systems Using Data Mining Techniques," A thesis submitted to the graduate faculty in partial fulfillment of the requirements for the degree, 2010.

[27] K. Mansfield, T. Eveleigh, T. H. Holzer S. Sarkani, " Unmanned aerial vehicle smart device ground control station cyber security threat model" Technologies for Homeland Security (HST), 2013 IEEE International Conference on, no. 978-1-4799-3963-3, pp. 722 - 728, 2013.

[28] C. Lolita Baldor, «Flashy drone strikes raise status of remote pilots,» www.bostonglobe.com/news/nation/2012/08/11/air-forceworks-fill-need-for-dronpilots/ScoF70NqiiOnv3bD3smSXI/story.html, [Accessed 10 April 2014]

[29] CNN Wire Staff, «Obama says U.S. has asked Iran to return drone aircraft,» 2011. [Accessed 7 May 2014]

[30] A. Kim, B. Wampler, J. Goppert, " Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles," Infotech@Aerospace Conferences, no. 978-1-60086-939-6, pp. 1-30, 2012.

[31] R. Miucic and S. M. Mahmud, "Wireless Multicasting for Remote Software Upload in Vehicles with Realistic Vehicle Movement," Electrical and Computer Engineering Department, Wayne State University, Detroit, MI 48202 USA, Tech. Rep., 2005.

[32] J. Han, S. Kywe, Q. Yan, F Bao and R Deng "Launching Generic Attacks on iOS with Approved Third-Party Applications" © Springer-Verlag Berlin Heidelberg CNS 2013, LNCS, no. 7954, pp. 72–289, 2013.