SECURITY CHALLENGES AND CRYPTOGRAPHY IN EMBEDDED SYSTEMS

Meeta Gupta
Ph.D Scholar, Computer Science and Engineering Department, JIIT, Noida, (India)

ABSTRACT

Embedded systems now days are integral part of our lives. They are used for various industrial automation purposes, service oriented applications like power, water distribution, healthcare and low cost systems like smart cards and PDA's. Today, already more than 98% of all manufactured microprocessors are employed in embedded applications rather than in traditional personal computers. Embedded processors are already an integral part of many communications devices and their importance will continue to increase. Embedded systems exchange data and information both locally and globally using networking and wireless communication, thus making them vulnerable to various kinds of active and passive attacks. In this paper we provide an overview of the security requirements, security challenges and need of light weight cryptography in embedded systems.

Keywords: Security, Attacks, Cryptography, Light Weight Cryptography

I. INTRODUCTION

Embedded devices are increasingly integrated into personal and commercial infrastructures. Security has emerged as a prime concern in the design and development of embedded systems. Today security[1] is a requirement for an increasing number of embedded systems ranging from low end systems such as PDA's, wireless handsets, networked sensors and smart cards to high end embedded systems such as routers, gateways, firewalls, storage servers and web servers. Embedded systems are used to capture, sense, store, process, transmit private, and vital data in computing systems like in automobiles, planes, trains, consumer electronics, medical equipments, network appliances, smart cards, cell phone, PDA's, time limited and on demand digital services etc. The users are endless so the numbers of new applications, both are increasing in this new world of pervasive computing. Security concerns are not new for embedded systems, but internet and wireless connectivity makes them more vulnerable to attacks. Security in embedded systems is usually considered as an afterthought, as security is not an economic priority for companies and users also pay more attention to saving money, and adding more features and functionalities. But as more and more security breaches have reported, the awareness and importance of security is raised and there is a need to incorporate security from the beginning of the design of embedded systems to the throughout entire life cycle[2]. The security attacks on embedded systems [3][6] target the weaknesses in the implementation of embedded systems, which mainly occur due to the following reasons:

- Network connectivity: embedded systems are now a days have networking capabilities including wireless, which makes them vulnerable to many sources of attack.

- Dynamic and configurable environment*:* Embedded systems are generally deployed in environments that are highly dynamic and configurable.
- Software induced vulnerability: third party software downloaded from internet on embedded devices are used in launching security attacks.
- Complexity : advances in embedded systems hardware and software technology enable the development of increasingly complex embedded systems

The security techniques developed for enterprise and desktop computing cannot be directly applied to embedded applications because of the strict design constraints of embedded systems such as cost, battery, size, processing power and changing functional requirements of embedded systems with time. The software security techniques developed mainly focus on detection and prevention, but do not focus on recovery from failures. Embedded systems deployed in mission critical applications have chances of failure so recovery from failure is important in embedded systems.

The paper is organized as follows. Section 2 presents the security requirements of embedded systems. Section 3 presents the attacks on embedded systems. Section 4 discusses the cryptographic requirements in embedded systems and section 5 conclusion.

II. SECURITY REQUIREMENT OF EMBEDDED SYSTEMS

Embedded systems are employed in emerging applications in everyday life and are used in services that need security. Security has long been a concern in computing and communications systems, and substantial research effort has been devoted to addressing it. Especially the connectivity of embedded systems to networks or to the Internet, places a significant requirement on the security. Considering the different types of attacks that have been developed for the overall system and the context of the system use, the term security is used to indicate different properties and services. To specify the requirements placed on systems for security, one needs to identify the areas of applications and services where embedded systems are used. The requirements for security should be considered from all perspectives, vendors, providers and customers [4]. Applications define the security requirements, which need to be met through appropriate security mechanisms and policies. Thus it is essential for embedded device to secure sensitive information, ensure availability and provide a secure communication system. The common security requirements of many embedded systems are:

- ***Confidentiality:*** Ensures the protection of stored or transmitted sensitive data from accidental for deliberate disclosure.
- ***Integrity:*** verifies the correctness and ensures that stored and transmitted sensitive data is protected against corruption.
- ***Availability:*** ensures that system can perform its intended function and service users at all the times.
- ***Dependability:*** ensures that the system is fault tolerant and can run continuously for years without errors and faults.

Cryptographic algorithms, including symmetric ciphers, public-key ciphers, and hash functions, form a set of primitives that can be used as building blocks to construct security mechanisms that ensures authentication, confidentiality and integrity of communicated data [3][5]. These mechanisms are known as functional security mechanisms, since they only specify what functions are to be performed, irrespective of how these functions are implemented. In order to provide complete security, one need to consider other factors such as profile of attackers and the available resources for the provision of secure applications, as well. Dependability is basically a system requirement providing reliability, Availability, safety and maintainability in the event of accidental and non malicious failures.

III ATTACKS ON EMBEDDED SYSTEMS

Attacks on embedded systems can be broadly categorized in two categories:

3.1 Hardware Attacks

The hardware attacks on embedded systems can be classified in two categories:

(a) ***Physical Attacks:*** refer to the attacks that require physical intrusion into the embedded system to observe, manipulate, and interfere with the system internals. For an embedded system on a circuit board attacks can be launched by using probes to eavesdrop on inter-component communications. However, for a system-on-chip, sophisticated microprobing techniques are used . The physical attacks are also known as invasive attacks. Because invasive attacks typically require relatively expensive infrastructure, they are much harder to deploy[1].

(b) ***Side Channel Attacks:*** attempts to exploit weakness in the implementation of design. They are also known as non-invasive attacks. They are based on observing properties of the system while it performs cryptographic operations. In the case of side channel attacks[7], the attacker treats the embedded system as a black box and analyzes the inside of the system by feeding it various types of inputs and then observing the behavior of the system and its output. These types of attacks are normally used to extract some secret information from the embedded system. Generally, side channel attacks are mounted against hardware implementations of various encryption algorithms so as to infer the secret key stored inside the hardware security modules. The side channel attacks are of four types:

- ***Timing analysis:*** tries to infer the cryptographic key, by observing the execution times of cryptographic computations on different data sets.
- ***Power Analysis:*** tries to infer the key used in cryptographic algorithm, by power consumption statistics of cryptographic hardware over a wide range of data sets. Power analysis attacks are of two types: Simple power analysis (SPA) attacks and Differential power analysis (DPA) attacks.
- ***Electromagnetic radiation analysis (EMA):*** attacks try to infer sensitive information by measuring the electromagnetic radiation emitted by a device. Two classes of EMA attacks are: Simple EMA and Differential EMA.
- ***Fault induction:*** the hardware module under attack is falsely activated or damaged and output pattern for a given input is obtained. Fault injection attacks rely on varying the external parameters and environmental conditions of a system such as the supply voltage, clock, temperature, radiation, *etc.*, to induce faults in its components. These attacks can be used to corrupt the secure or non-secure code or data stored in components such as memories. Fault injection techniques are also useful as a pre-cursor to software attacks.

3.2 Software Attacks

The software attacks refer to the attacks which are launched through software agents such as viruses, Trojan horses, and worms and can compromise the security of the system from all stand points – confidentiality, Integrity and Availability . These attacks exploits weakness inherent in the design and algorithm of the embedded system. The software attacks are very cheap and does not requires any big infrastructures like physical attacks. The buffer overflow problem is a common problem in operating system and application software, which can be exploited during software attacks. The buffer overflow effects can include overwriting stack memory, heaps, and function pointers. The attacker can use buffer overflows to overwrite program addresses stored nearby. This may allow the attacker to transfer control to malicious code, which when executed can have undesirable effects. Software attacks can also be mounted by exploiting weakness in the end system architecture. These are knows ass software vulnerabilities, which allows attacker to gain direct access to the end system or may provide an entry point to indirectly exploit to gain access.

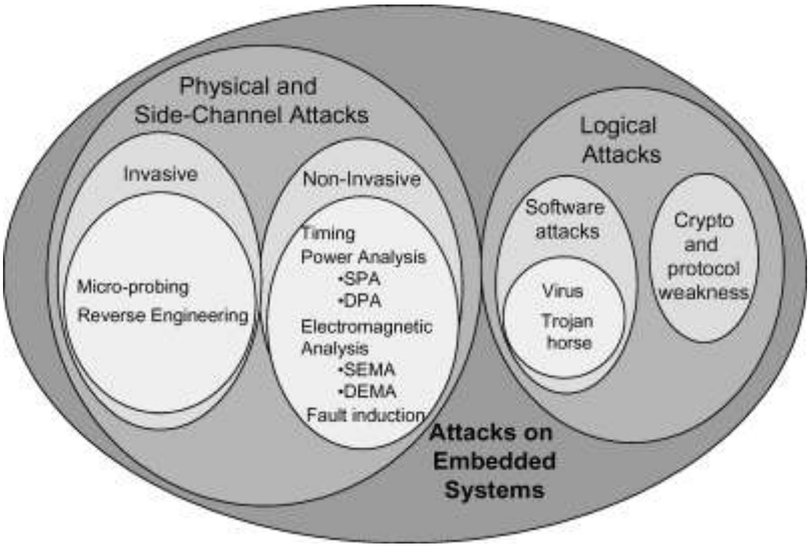

Fig-1 Attacks on embedded systems [1]

IV. CRYPTOGRAPHY IN EMBEDDED SYSTEMS

The advent of worldwide communication system like Internet has made all companies, government agencies and home users largely dependent on digital information and if security system is not implemented, then users have a fear that their sensitive information can be monitored and stolen. Data security plays a central role in the design of systems dependent on embedded systems. Specifically, unauthorized access to information must be prevented, privacy must be protected, and the authenticity of electronic documents must be established. Thus there is a need to develop security systems and the cryptographic algorithms are the core of such security systems. [8]The field of cryptography started as a simple encryption technique, now can be used for confidentiality, integrity, authentication and non repudiation of information. Cryptographic algorithms are cost and computation power intensive, hence the cryptographic techniques applicable to desktop computers cannot be directly applied to resource constraint embedded systems. The cost is one of the important aspect in design of cryptography in embedded systems, therefore specialized implementations are done on embedded systems.

There are two major classes of algorithms in cryptography: Private-key or Symmetric-key algorithms and Public-key or asymmetric algorithms. Symmetric algorithms are much faster to execute than asymmetric ones. Symmetric ciphers serve mainly for message integrity checks, entity authentication, and encryption, whereas asymmetric ciphers additionally provide key-management advantages and nonrepudiation. Asymmetric ciphers are computationally far more demanding, in both hardware and software. Most often these two techniques are used together, the encryption key is used to encrypt the actual message using a symmetric algorithm and an asymmetric algorithm is used to exchange the encryption key. The cryptographic algorithms can be implemented in hardware as well as software. Hardware based implementations have high performance but have less flexibility and high cost. On the other hand software based implementations are very flexible. The main challenge is to design cryptographic techniques which can be efficiently executed on various platforms and gives performance and cost tradeoffs.

- *Symmetric key algorithms :* two distinguished categories of symmetric key algorithms are stream and block ciphers. The various symmetric key algorithms that have been implemented on 8 and 16 and 32 microcontrollers and microprocessor platforms are DES, 3DES, AES, IDEA, BLOWFISH, RC4, RC6 etc. These have been implemented with variable length key sizes like 112 and 12 bit both in hardware as well as software. The performance evaluation [9] of the algorithms shows that encryption throughput is highest for AES. One major issue with symmetric ciphers is the secure key exchange .

- *Asymmetric key algorithms:* the various asymmetric or public key algorithms implemented in embedded systems can be categorized in three families. The first category includes RSA algorithm based on integer factorization problem, the second category includes Diffie-Hellman key exchange algorithm based on discrete logarithm problem and last category includes elliptic curves algorithm(ECC). The performance investigation of public key algorithms RSA (both 256 bit and 2048 bit) and ECC on 8 bit and 32 bit embedded platform [10][11] using a separate coprocessor shows that ECC gives same security as RSA with less key size.

- The upcoming era is of pervasive computing[12], where there is an increasing demand for security in applications such as smart cards and RFIDs to mobile devices. These devices have tight cost constraints leading to the demand of efficient hardware and software implementations of cryptographic algorithms. The existing methods of security [8]are very complex and expensive requiring more resources and time, hence cannot be directly applied to these low cost and highly constraint pervasive devices.

- *Light Weight cryptography :* is one which can perform computationally intensive operations with limited memory and power at an acceptable speed and without compromising on security emerges as a strong security solution for pervasive devices like smart cards and RFIDs. The light weight cryptographic solutions have to optimize the three design goals security, cost and performance. Several light weight cryptographic variants of already existing algorithms have been proposed[12] and several new lightweight cryptographic algorithms have also been proposed. Under light weight symmetric key algorithms are the hardware implementation of DESL , DESXL, Present and Hight. And under light weight asymmetric key algorithms is the hardware implementation of low area, stand alone coprocessor for ECC. The research is going in this area for designing new ciphers with low implementation cost and providing acceptable level of security.

V. CONCLUSION

We have introduced the basic security requirements and challenges of embedded systems and its applications . It has been shown that embedded systems are essential parts of most communications systems today and wiill be integral part of most of future IT applications, thus making then attractive as a potential platform for hardware and software attacks discussed here. Thus data security plays an important role in the design of future embedded systems and a platform for implementing cryptographic algorithms. We have shown that previous implementations of symmetric and asymmetric algorithms are not efficient on resource constraint embedded systems used in pervasive devices as they are very arithmetic intensive and expensive. The pervasive devices is an upcoming field having tight cost and power constraints, thus there is a need to develop lightweight cryptographic algorithms for these devices. Several light weight variants of already existing cryptographic algorithms have already been proposed, but still more research needs to be done in this area.

REFERENCES

[1]. Srivaths Ravi , Anand Raghunathan , Paul Kocher , Sunil Hattangady, *" Security in embedded Systems : Design Challenges*" ACM Transactions on Embedded Computing Systems (TECS), v.3 n.3, p.461-491, August 2004.

[2]. S. H. Mirjalili and A. Lenstra, "*Security Observance throughout the Life-Cycle of Embedded Systems*," ESA 2008, pp. 186-192.

[3]. Ravi, S.,Raghunathan, A., And Chakradhar,S,"*Tamper resistance mechanisms for secure embedded systems*", In Proceedings of the International Conference on VLSI Design. 605–611,2004.

[4]. Dimitrios N. Serpanos, Artemios G. Voyiatzis, *"Security Challenges in Embedded systems*",ACM Transactions on Embedded Computing Systems (TECS), v.12 n.1, March 2013.

[5]. Bruce Schneier, "*Applied Cryptography: Protocols, Algorithms, and source code in C",* 2nd edition", Wiley October 1995.

[6]. Somesh jha,"*Software Security Issues In Embedded Systems",* In Proceedings of the ARO Planning Workshop on Embedded Systems and Network Security, North Carolina, February 22-23, 2007

[7]. Muhammad Farooq-i-Azam, Muhammad Naeem Ayyaz, "*Embedded System Security*", In book "Cyber security standards, practices and Industrial applications", Junaid Ahmed and Athar Mahboob, chapter 10.

[8]. S. Sadanandan and R. Mahalingam,"*Light weight cryptography and applications*," Novel Algorithms and Techniques in Telecommunications , Automation and Industrial Electronics , 2008, pp. 484-488

[9]. Ondrej Hyncica, Pavel Kucera, Petr Honzik, Petr Fiedler,"*Performance evaluation of symmetric cryptography in Embedded systems*", in IEEE 6th international conference on Intelligent data acquisition and Advanced computing systems(IDAACS),2011,pp 277-282.

[10]. HoWonKim, Sunggu Lee, "*Design and Implementation of a private and public key crypto processor and its application to a security system*", IEEE transactions on consumer electronics, vol.50, No. 1, Feb 2004.

[11]. Wang Long, Zhao Hue, Bai Guoqiang, "*A Cost-efficient Implementation of Public-key Cryptography on Embedded Systems*", Proc. of International Workshop on Electron Devices and Semiconductor Technology, Beijing, China, 2007.

[12]. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel,"*A Survey of Lightweight Cryptography Implementations*", IEEE Design and Test , vol. 24, no. 6, Nov. 2007, pp. 522-533.