The Security Strategies in IoT – A Road Map

Bobby. S[1], AmalRedge. G[2]

[1]Assistant Professor, Department of Computer Science,
St. Joseph's College of Arts and Science for Women, (Hosur, Tamil Nadu, India).
angelbobby2@gmail.com

[2]Assistant Professor, Department of Computer Science,
St. Joseph's College of Arts and Science for Women, (Hosur, Tamil Nadu, India).
g.amalredge@gmail.com

ABSTRACT – ***The Internet of Things (IoT) is the escalation production of the Computer Science and Communication technology. The phrase IoT was originally proposed to connected objects with RFID technology. Presently, researchers relate IoT with sensors, actuators, GPS devices and Mobile devices. IoT has provided a capable prospect to build powerful industrial systems and applications. Recently large number of IoT applications have been developed and deployed. The significance of the security in the IoT is gradually budding and IoT is one of the most promising network technologies in the new network. This paper is a survey of the basic concept of IoT, background architecture and analyzes the security problems of IoT. And also we provide the requirements of embedded security, the solutions to resist different attacks and the technology for defying rage proofing of the embedded devices by the concept of trusted computing. Addressing this concern is equivalent to addressing the security issue of the hardware platform.***

Keywords – Internet of Things, Security, Architecture, Embedded Security

1. INTRODUCTION

The Internet of Things (IoT) gives connectivity for anyone at any place to anything at any place. The expansion in technology we are moving towards a society where everything and everyone will be connected [1]. The basic idea of IoT is to allow sovereign and secure connection and exchange of data between real world devices and applications [2]. The IoT connects real life and physical activities with the virtual [3]. The IoT is a kind of intelligent system, which uses intelligent objects with perception, communication and computing ability to capture different information in physical world and interconnects the physical objects which can individually addressing. Consequently overall perception, reliable transmission, and intelligent disposal is realized and the interconnection between people and things as well as among things constructed [4]. One main objective of IoT at work is ensuring elasticity and security in running applications that support adaptive and agile manufacturing scenarios.

Wireless and mobile communication technologies are previously mostly and their capabilities are forever growing, such as WiMAX, ZigBee, wirelss Mesh Networks and 4G Network emerge giving rise to the notion of ubiquitous computing. The computer of the 21st century according to which "the most deep technologies are those that disappear; they weave themselves in to the fabric of everyday life until they are indistinguishable from it is today a reality[13].ubiquitous computing as:" any computing movement that permits human interaction away from a single workstation.[14]. Since then there have been great advances in mobile and wireless technologies toward supporting the envisioned ubiquitous applications that are intended to utilize the foregoing technologies have emerged and are constantly permeate our life[15]. We can observe that from cars to smart phones, refrigerators to multimedia players rooted computing increasingly encompass our lives. Security issues are nothing new for embedded systems. However as more embedded systems are connected to the internet, the possible compensation from such vulnerabilities scale up radically. Unfortunately security techniques developed for enterprise and desktop computing might not satisfy embedded application requirements. Internet connection exposes application to intrusions and malicious attacks. System designs for embedded devices are complicated including multiple independent processor cores secondary bus masters such as DMA engines and large numbers of memory and peripheral bus slaves. In addition to these functional components there is typically a parallel system infrastructure that provides invasive and non –invasive debug capabilities as well as component boundary scan and Built-In-Self-Test (BIST) facilities.

In reality it is a new dimension that designers should consider throughout the design process along with other metrics such as cost, performance and power. The diverse security requirements are especially apparent in embedded systems where increased connectivity, portability, and pervasive networks have led to widespread use of increasingly diverse application. Many of these embedded system applications handle sensitive data or perform critical functions and the use of security protocols is imperative to maintain confidentiality integrity and authentication of these applications. Evolution of embedded systems towards devices connected via internet, wireless communication or other interfaces as well as the trend towards always growing numbers of devices (IoT) requires a re-consideration of embedded systems engineering processes. Typically embedded systems have low computing power and finite energy. Thus design of secure embedded systems is guided by factors: small form factor, Good performance, low energy consumption and robustness to attacks.

2. BACKGROUND

The Internet of Things (IoT) can be considered as a global network infrastructure composed of numerous connected devices that rely on sensory, communication, networking and information processing technologies [5]. Many other technologies and devices such as barcodes, smart phones, social networks and cloud computing are being used to form an extensive network for supporting IoT [6]. Figure 1 shows the technologies associated with IoT.

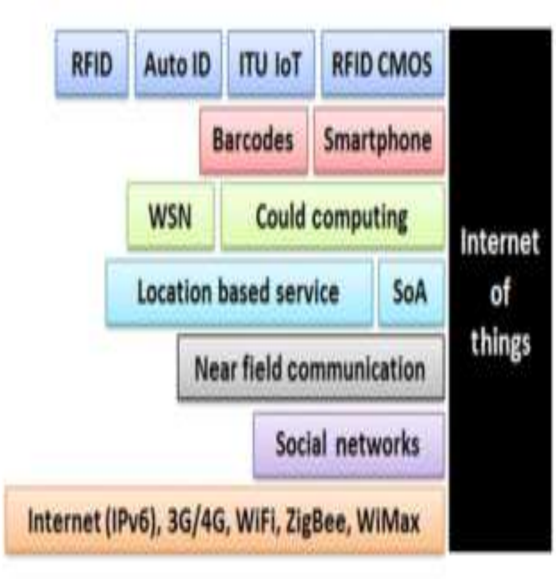

Figure 1: Technologies associated with IoT

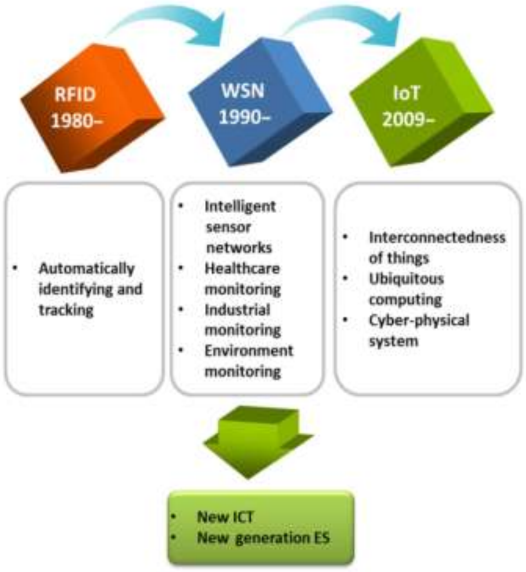

Figure 2: IoT related technology and their impact

IoT has gaining attraction in industry such as logistics, manufacturing, retailing and pharmaceutics. With the advances in wireless communication, smart phone and sensor network technologies, more and more networked things or smart objects are being involved in IoT. These IoT related technologies have also have also made a large impact on new information and communications technology (ICT) and enterprise system technologies. Figure 2 shows the IoT related technologies and their impact on new ICT and enterprise systems.

3. ARCHITECTURE AND SECURITY ISSUES

IoT application infrastructure contains Perception layer, Network layer and Application layer, depending on the three basic characteristics.

3.1 Perception Layer

The perception layer, ties between physical world and the virtual world is the basis of the IoT, whose main task is to achieve reliable sensing. The perception layer locating in the lowest level of IoT construction is the source of access to information throughout the IoT. The main security issues include physical security of sensing devices and the security of information collection. Due to the diversity, simple, energy limited and weak protective capability of sensing node, and mostly deployed in unmanned harsh environment without a special standard, the IoT cannot provide a unified security protection system and is vulnerable to the invasion and attack, which affects the security of the wireless sensor network, M2M terminal and RFID.

3.2 Network Layer

The network layer provides ubiquitous access, information transmission, processing, storage and the bearer of the core business. IoT faces the risks in existing communication network, including illegal access, data eavesdropping, confidentiality, integrity, destruction, denial of service attacks, man-in-the-middle attacks, virus attacks, and the use of factory explores the variety of attacks outside the tools and system vulnerabilities. moreover, it exist across the network construction network interconnection, inter-network authentication and other security issue, and it may be subject to Dos attacks, man-in-the middle attack, asynchronous attack, conspiracy attack and so on.

3.3 Application Layer

The Application layer analysis and process the received information to make the right decision and control for intelligent management, applications and services. The widespread applications of IoT are the result of closely integration between computer technology, communication technology and industry professional, which can find applications in many aspects. Besides the business in the traditional communication network abuse such as, replay attacks, applications of information security issues such as eavesdropping and tampering, the applications face many extra security issues and become particularly prominent, including cloud computing, middleware, data mining, data storage and backup, management and authentication mechanisms, information disclosure, intellectual property rights, and privacy protection security issues.

4. SECURITY ARCHITECTURE ELEMENTS

Security architecture for IoT enabled automation systems needs to be based on an equivalent defense in depth strategy and a single security mechanism is not sufficient to protect open automation environments supporting dynamic plug & work scenarios. Multiple layers of security controls are necessary to provide adequate and flexible security architecture. The architecture elements from a network and device view only which are:

4.1 Secure Device Identifier

Devices shall provide a cryptographic secure identifier that is bound to the device in such a manner that it is hard to manipulate or clone the identity. A secure device identifier is an identifier based on authentication credentials that cannot be easily removed or copied for unauthorized access are to attack the operations of a network. Secure identifiers are a prerequisite for the objectives of IoT at Work to enable secure communication and secure plug & work and are an enabler for various (security) services like: Secure authentication, Access control and policy checks, Auto-configuration, Authorization, Secure inventory, Localization, Anti counterfeiting.

4.2 Secure Credential Management

The automation environment shall provide components and mechanisms to manage credentials. Security mechanisms providing authorization, integrity protection and confidentiality may require additional credentials. The process to efficiently install required security credential especially considering the huge number of devices in industry environment and internet of things scenarios is challenging. Security credentials are, like other type of data or equipment, part of a lifecycle .they are created, applied, and destroyed and need to satisfy a certain security policy. The typical life cycle of security credentials is depicted in the following figure 4.

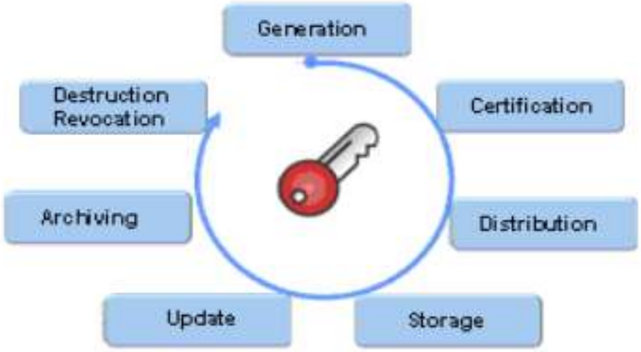

Figure 4: Security Parameter Lifecycle

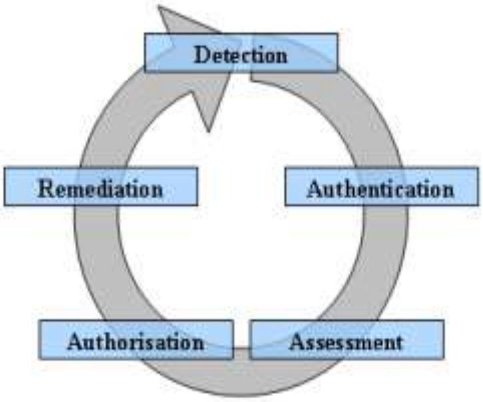

Figure 5: Network Access Control Steps

- **Generation**: Device keys can be created on the device itself or they may be created externally and installed on the target device.
- **Certification**: typically done for asymmetric keys through a certificate authority. depending on the key generation, this can be part of the key generation in a trust center or may be done on information sent in a certificate signing request (CSR).
- **Distribution**: In case of off-device key generation, the device key has to be installed on the target device.

- **Storage**: The private/secret device key can be stored in secured memory (eg., Flash) or in a separate hardware module (eg., smart card or a trusted platform module).

The above steps are essential to initialize security on a device. The following steps occur during the lifetime in the operational phase and are not discussed in this document.

- Update of operational keys.
- Archiving of long term (secure or private) to enable access to encrypted data.
- Destruction and revocation of session keys or long term keys.

4.3 Secure Network Access of Devices

A device shall be authenticated before access to the operational network is granted. Network access control is a well-known approach improving network security in enterprise and Office domains and implemented by many network component, operating system and security vendors (e.g.[10]). Standardization activities in this area have been mainly driven by the trusted connects (TNC) work group [11] and the NEA working group of the internet engineering task force (IETF) [12]. Figure 5 shows the network access control steps:

4.4 Device And System Integrity Assurance

The integrity of devices of an automation environment shall be verified regularly during operation. The collection and communication of device attribute are security sensitive steps. If an attacker is able to manipulate or forge attributes as part of the assessment results, the primary goal of the system integrity assurance component to observe the integrity of automation devices has failed. Therefore, it is necessary that some major security requirements are addressed by the system integrity assurance architecture:

- **Integrity of attributes**: It needs to be assured that the integrity of the device attributes cannot be modified by unauthorized devices.
- **Authenticity of attributes**: It needs to be assured that the attributes originate from a specific device.
- **Confidentiality of attributes**: It needs to be assured that no sensitive information is accessible by unauthorized devices.
- **Replay protection**: It needs to be assured that attributes of past assessments are not re-used for or replayed in future assessments.

The verification of device integrity, that means device attributes map to the expected attributes, is divided into two phases:

- Collection of device attributes.
- Verification of device status that is the comparison of the collected attributes to the expected ones.

4.5 Policy Enforcement For Devices

The compliance of a device to given policies shall be assessed during network access and regularly during normal operation. These architecture elements address or enhance major technical security controls of current industry best practices as described in documents like [7-9]. Examples are identification and authentication, access control, network security, intrusion detection are monitoring for malicious actions.

5 EMBEDDED SECURITY REQUIREMENT IN IOT

The start of controlling computing and communication gadgets and tools, the possibility of attack on our daily life is increased many fields. We are encountering a third wave of hacking one that encompasses not only wired computers and networks but intelligent devices: wireless phones, routers, and switches printers SCADA (Supervisory Control And Data Acquisition) systems and even medical devices. Devices and systems used for banking, energy metering and wireless mobile communication signalling the increasing importance of this area.

Another testing area which fixed systems needs good amount of thought is in –vehicular security. Many analyses [16] can verify the safety and reliability of vehicle networks beside random failures. Analyses that consider also intended malicious manipulations. Security for these systems is an open question and could prove a more difficult long-term problem than security does today for desktop and enterprise computing. Unfortunately security [17] techniques developed for enterprise and desktop computing might not satisfy embedded application requirements. Non-invasive techniques consist of software attacks and attacks based on the statistical analysis of operational characteristics of the device to extract secret information. When a system is under attack [18], is the extraction of secret information the second one is trying to put the system out of order.

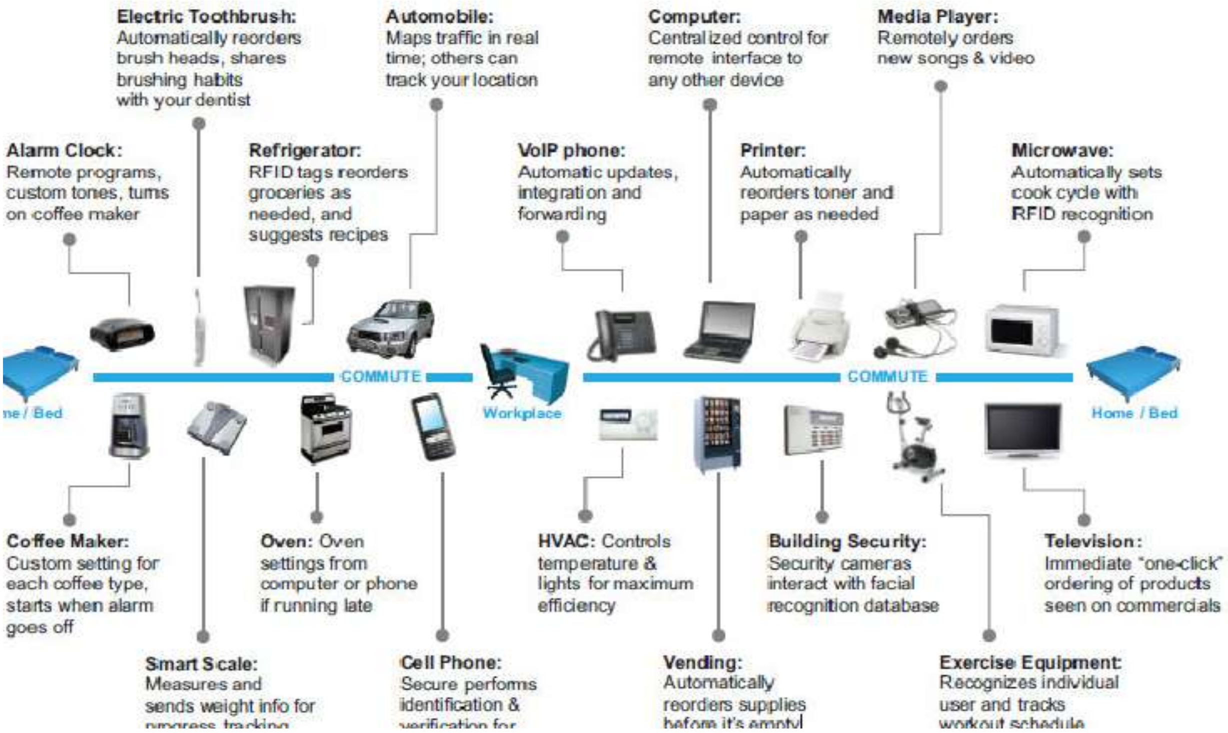
Electric Toothbrush: Automatically reorders brush heads, shares brushing habits with your dentist
Automobile: Maps traffic in real time; others can track your location
Computer: Centralized control for remote interface to any other device
Media Player: Remotely orders new songs & video
Alarm Clock: Remote programs, custom tones, turns on coffee maker
Refrigerator: RFID tags reorders groceries as needed, and suggests recipes
VoIP phone: Automatic updates, integration and forwarding
Printer: Automatically reorders toner and paper as needed
Microwave: Automatically sets cook cycle with RFID recognition
ne / Bed
COMMUTE
Workplace
COMMUTE
Home / Bed
Coffee Maker: Custom setting for each coffee type, starts when alarm goes off
Oven: Oven settings from computer or phone if running late
HVAC: Controls temperature & lights for maximum efficiency
Building Security: Security cameras interact with facial recognition database
Television: Immediate "one-click" ordering of products seen on commercials
Smart Scale: Measures and sends weight info for progress tracking
Cell Phone: Secure performs identification & verification for
Vending: Automatically reorders supplies before it's empty
Exercise Equipment: Recognizes individual user and tracks workout schedule

Figure 6: IoT architecture

6 EMBEDDED SECURITY SOLUTION

There are many existing solutions to counter different attacks. Encryption of information is used for confidentiality. System design for embedded devices are difficult including multiple independent processor cores, secondary bus masters such as DMA engines and large numbers of memory and peripheral bus slaves. In addition to these functional components there is typically a parallel system infrastructure that provides invasive and non-invasive debug capabilities, as well as component boundary scan and Built-In-Self-Test (BIST) facilities [19]. Due to this kind of importance complexity as well as the pervasive deployment of embedded device from home to big issue. Many research initiatives have been undertaken to counter the issues of security in embedded systems. We find great treatment on the issues of embedded systems security [20] in where authors have described security requirements, design challenges, basic concepts, and different security protocols like Secure Socket Layer (SSL) [21]. The SSL protocol is typically layered on top of the transport layer of the network protocol stack, and is either embedded in the protocol suite or is integrated with application such as web browsers.

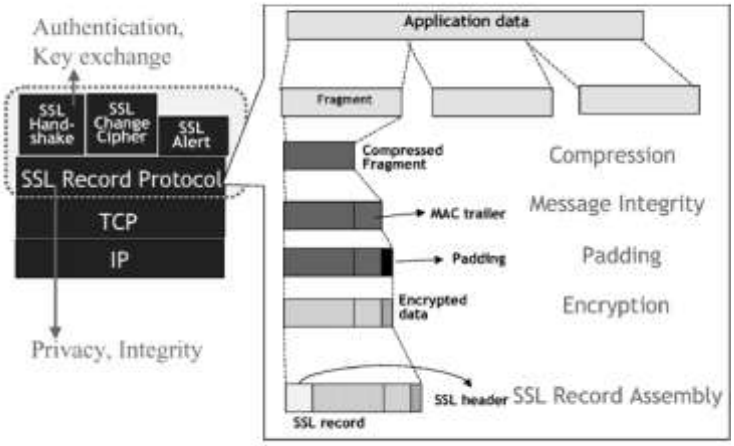

Figure 7: SSL protocol, with an expanded view of the SSL record protocol

7 ATTACKS ON IOT SYSTEMS

The domain of security attacks on embedded device is increasing day by day.

- **Physical Attacks**: These types of attacks meddle with the hardware components and are relatively harder to perform because it requires high-priced material. Examples are de-packing of chip, layout reconstruction, micro-probing and particle beam technique.
- **Cryptanalysis Attacks**: These attacks are focused on the cipher text and they try to break the encryption, i.e finds the encryption key to obtain the plain text. Examples are cryptanalysis attacks include Cipher text-only attack known-plain text attack, chosen- plain text attack, Man-in-the middle attack etc.
- **Side Channel Attacks**: These attacks are based on “side channel information” that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the cipher text resulting from the encryption process. Examples are side channel information are timing attacks, power analysis attacks, fault analysis attacks, electromagnetic attacks, environment attacks [22].
- **Software Attacks**: Software Attacks are the major source of security vulnerabilities in any system. This kind of attack includes exploiting buffer overflows and using Trojan horse programs, worms or viruses to deliberately inject malicious code in to the system.

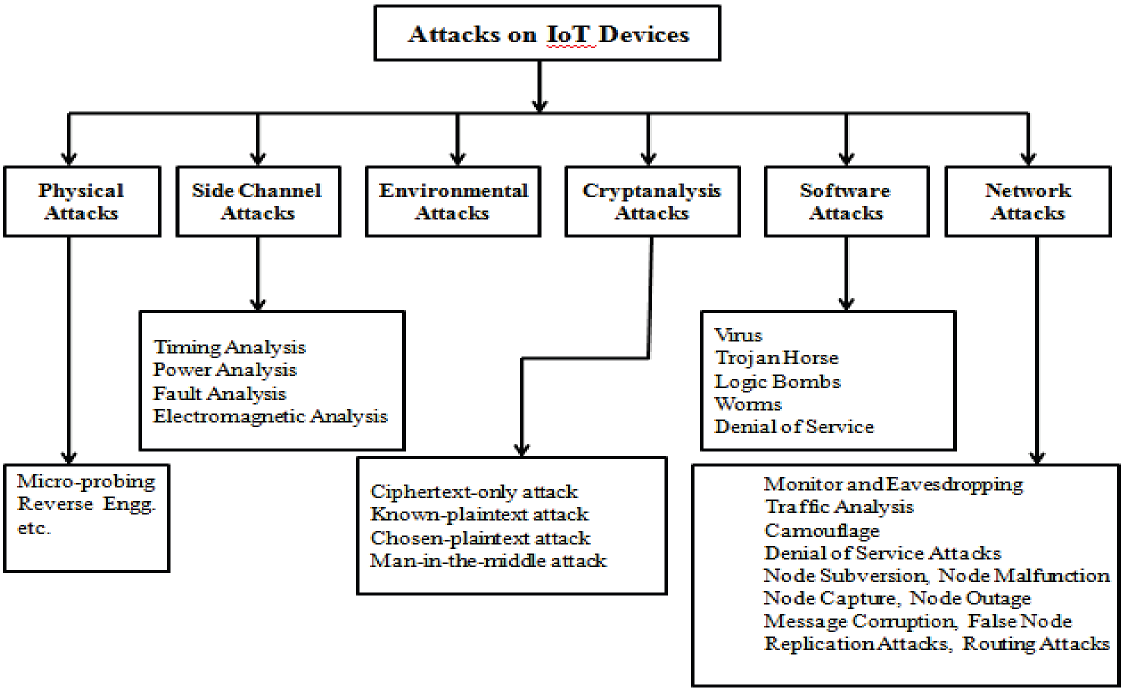

Figure 8: Attacks on IoT

- **Network Attacks**: Wireless communication systems are vulnerable to network security attacks due to the board cast nature of the transmission medium. Examples of passive attacks include Monitor and Eavesdropping. Examples of active attacks include denial of service attacks , Node subversion.

Few types of attacks in the security domain. The security in the case of IoT system must deal with several additional resource constraints and a need of strongest resistance against attacks.

8 PROPOSED EMBEDDED SECURITY FRAMEWORK

- **Environment factor**: with respect to the environment in which the devices operate determine the assumptions, threats, vulnerabilities, attack and required policies for secure functioning.
- **Security Objectives**: determine your device’s security objectives.
- **Requirements**: Determine your functional security requirements.

The basic idea for framing the security architecture for IoT is utilizing security mechanisms protocol effectively. It takes security consideration from the requirements gathering to maintenance.

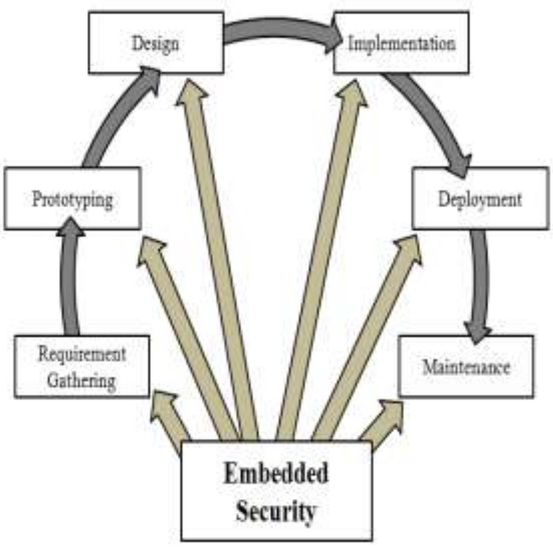

Figure 9: Embedded security and design steps.

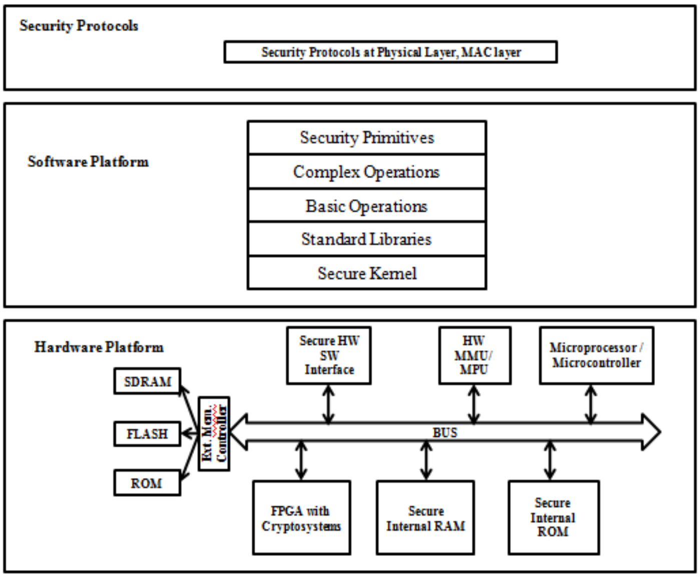

Figure 10: Embedded Security Framework and architecture

For building the embedded security framework for IoT. We also need to look at all of the tradeoffs between performance, cost, and security. Unfortunately these three concepts are almost always directly at odds with one another. More performance means the cost goes up lowering the cost means lowering security and presentation and implementing higher security means performance will decrease.

The key features of the security framework and architecture:

- **Lightweight cryptography**: Optimized Cryptographic algorithms and hardware architecture for extreme low power memory and processing requirements.
- **Physical Security**: Trusted platform module which will take into account the vulnerabilities of the hardware device at physical level.
- **Standardized Security Protocols**: Development of standardized protocols which are both lightweight with respect to communication and cryptographic computations.
- **Secure Operating Systems**: Rich operating systems with a secure kernel which will ensure a secure communication inside the processor by providing secure runtime execution environment, secure booting, secure content, etc.
- **Future application Areas**: Understanding the technical, economical, social context of a given application area in order to develop security solutions which are appropriate and acceptable.
- **Secure Storage**: Protect the sensitive information stored in RAM/ROM and secondary storage.

The architecture can be divided in to hardware and software level with lightweight standardized protocols supporting at the physical and MAC layer. The level of security within the device will vary depending on the nature of the protected content and kin of application. The architecture should provide physical protection to secret keys by keeping the components like secure ROM, which is handling the secret keys, inside the secure SoC. The Secure Boot loader should ensure that the device boots up with the genuine OS or firmware with right process privileges secure ROM, secure runtime execution environment, secure memory management unit are the prime focus for inbuilt security. Also rich operating systems with necessary security functionality, secure kernel interface and compatible standardized security protocols for IoT system will contribute towards the secure security architecture and framework for IoT.

9 CONCLUSION

Along with the rapid development of the IoT industry, the importance of the security in the IoT is gradually emerging and IoT is one of the most promising network technologies in the new network. In this paper, security issues on the IoT construction layers are analysed. In addition to the theory, we also have a survey about embedded Systems. As most today’s and next generation computing applications involve embedded systems in this work, we have presented the requirements, issues, designs and solutions of embedded design to counter the different attacks. Several issues, however, still remain open to find a holistic solution to the problem of embedded system security. IoT mainly consist of tiny devices with limited processing power. As the attackers become sophisticated, it becomes necessary to dedicate entire co-processor with high scalability to offer entire security features that an embedded system may require. Embedded security for IoT will be crucial and important with strong security mechanisms which will prevent damages and economical losses offering new business opportunities.

10 ACKNOWLEDGEMENT

First of all, I am glad to thank THE LORD ALMIGHTY for giving me the fortitude in finishing this paper. I express my sincere gratitude to my husband and my parents for their continuous guidance, support and encouragement in all my endeavors. I would like to thank my colleagues for their constant support they provided throughout my preparation.

11 REFERENCES

[1] J. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. Mouftah, “The Internet of Things,” in IEEE Communications Magazine, Volume:49 , Issue: 11, pp:30-31, 2011.E.Fleisch, and F.Mattern, Das Internet der Dinge, Springer, 1 edition, July 2005.

[2] T. Fan and Y. Chen, “A Scheme of Data Management in the Internet of Things,” in 2nd IEEE International Conference on Network Infrastructure and Digital Content, Sept. 2010.

[3] Y. Huang and G. Li, “A Semantic Analysis for Internet of Things,” in International Conference on Intelligent Computation Technology and Automation (ICICTA), May 2010.

[4] WU Gongyi, WU Ying. Introduction to the Internet of things engineering [M]. Beijing: china machine press, 2012.

[5] L. Tan and N. Wang, “Future internet: The internet of things,” in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), Chengdu, China, Aug. 20–22, 2010, pp. V5-376–V5-380.

[6] X. Jia, O. Feng, T. Fan, and Q. Lei, “RFID technology and its applications in internet of things (IoT),” in Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet), Yichang, China, Apr. 21–23, 2012, pp. 1282–1285.

[7] IEC/TR 62443-3-1,” industrial communication networks- network and system security – part 3-1: security technologies for industrial automation and control systems”,2009.

[8] NIST SP800-82, “ Guide to industrial control systems(ICS) security “, june 2011.

[9] ISO/IEC 27002, “Information technology – security techniques – code of practice for information security management”, june 2005.

[10] Enterasys, network access control, March 2010, http://www.enterasys.com/company/literature/nac-wp.pdf.

[11] Trusted computing group, trusted network connect specifications, http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications.

[12] IETF NEA Working group status page, http://www.tools.ietf.org/wg/nea/.

[13] Mark weiser, “the computer for the twenty first century, “scientific American, pp.94-104, September, 1991.

[14] A. Dix, J. Finlay, G.Abowd, and R.Beale, “Human-computer interaction, “prentice Hall, 3e, 2004.

[15] G.D.Abowd, G.R.Hayes, G.lachello, J.A.Kientz, S.N.Patel, and M.M.Stevens, “prototypes and paratypes: Designing mobile and ubiquitous computing applications,” IEEE Pervasive computing, vol. 4, no. 4, pp.67-73, 2005

[16] Maxim Raya and Jean-pierre hubaux, “The security of vehicular networks,” Technical report, Laboratory for computer communications and applications (LCA), School of computer and communication sciences, EPFL, Switzerland, March 2005.

[17] P.Koopman, “Embedded system security,” IEEE Computer, vol. 37,issue. 7, pp.95-97, 2004.

[18] T.Messerges, E. A. Dabbish, and R.H. Sloan, “Examining smart-card security under the threat of power analysis attacks,” IEEE Trans.computers, vol.51, pp.541-552,May 2002.

[19] M. Abramovici, C.Stroud, and J. Emmert, “On-Line BIST and BIST-Based Diagnosis of FPGA logic blocks,” IEEE trans. On VLSI systems, Vol. 12, No.12, pp. 1284-1294, 2004.

[20] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, “Security in Embedded systems: Design challenges,” ACM Transactions on Embedded computing systems, vol. 3,no. 3, pp.461-491, 2004.

[21] URL:http://wp.netscape.com/eng/ss113

[22] Bar-E1 ,”An introduction to side channel Attacks “ , White paper, Discretix Technologies limited,