ISSN: 2393-8528

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 7 Issue 1; January-February 2020; Page No. 01-04

An Analysis of Efficient Security Framework for Embedded Systems and Internet of things

K D Gupta

Apex Institute of Management & Science College Jaipur, Rajasthan, India.

ABSTRACT

Internet of Things is interconnection of intelligent and self configuring nodes or devices that gather useful data. This data is then processed and transformed into information that is then finally used in useful areas such as smart cities, smart home, automation, transportation etc. In this paper, we only discuss the embedded device security. We are assuming that network security is already there. The devices connected in IoT are very vulnerable to different security attacks, so it is very important to discuss the security issues faced by these devices. In this work, we provide the requirements of embedded security, the solutions to resist different attacks and the technology for defying temper proofing of the embedded devices by the concept of trusted computing.

Keywords: IoT

INTRODUCTION

Mobile and wireless communication technologies are increasing day by day. Recently there are technologies such as WiMAX, 4G, mesh networks are emerging into the market. These are all examples of ubiquitous computing. “Any computing activity that permits human interaction away from a single workstation” is called ubiquitous computing. There have been tremendous advances in technologies to support ubiquitous computing. We can feel that in our everyday life embedded devices are everywhere to support human life. So security of these systems will play an important part in our everyday life. The more embedded systems connected to internet the more security issues will be there. Because in internet connect there can be very malicious attacks. There is a difference between security techniques in enterprise computing and embedded devices.

Embedded system devices are very complicated in design. They have DMA’s, bus slaves, processor cores etc. because of the pervasive deployment of embedded devices, as they are from home to big enterprises, security in embedded devices is a big issue. Many researcher are working on the issues of security in embedded system devices. When security feature is added to the embedded systems, many features are added to them as some algorithms and protocols. But it should be noted them rather than adding extra design features, researchers should think about the security in the whole design or throughout the system design process. Security should be considered as a metric along with other metrics such as cost, performance, and power. The challenges that are different in embedded systems require new approaches to security covering all aspects of embedded system design from architecture to implementation. The diverse security requirements are especially apparent in embedded systems where increased connectivity, portability, and pervasive design objectives are need to be considered. In fact, pervasive networks have led to widespread use of embedded systems, like cell phones, PDAs, RFIDs etc., in increasingly diverse applications.

Mainly devices in embedded systems have low computing power and they have fixed energy supply based on a battery, and these things don’t work properly with the computationally intensive nature of the cryptographic algorithms underlying many security protocols. And also the secure embedded systems are vulnerable to attacks, like physical tampering, malware and side-channel attacks. Thus, design of secure embedded systems is guided by the following factors: small form factor, good performance, low energy consumption (and, thus, longer battery life), and robustness to attacks.

Corresponding author: K D Gupta

SECURITY REQUIREMENT IN INTERNET OF THINGS AND EMBEDDED COMPUTING

When the research in powerful computing and communication gadgets and tools is on peak, the possibility of breach of security in our daily life is increased many times. Now, when the use of IoT is increased (as shown in Fig. 1), our society is 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 systems, and even medical devices. This new hacking wave is not like the older amateur "street-creed" phase and these are well-honed, massively coordinated and sophisticated attacks. This third wave will also include terrorist cyber-strikes against the utility and industrial infrastructure. This is really a danger to our daily use devices and for our daily lives. One of the most common attacks on internet of things is "war driving," in which hackers drive around a neighborhood and they hunt for unsecured wireless nodes. The latest version of war driving approach is a security expert cruised around Fisherman's Wharf, he was armed with a cheap RFID scanner and a low-profile antenna, and he has cloned half a dozen electronic, wallet-sized passports in an hour. Ross Anderson discussed the basic security issues in the devices and systems.

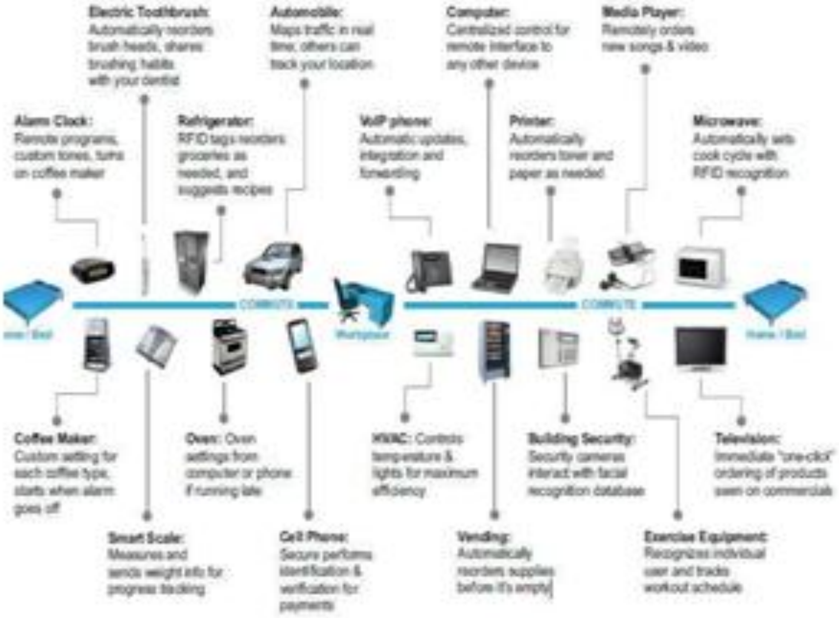
Electric Toothbrush: Automatically reorders brush heads, shares brushing habits with your dentist
Automobile: Maps traffic in real time; others can track your location
Computer: Centralized control for remote interface to any other device
Media Player: Remotely orders new songs & video
Alarm Clock: Remote 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
COMMUTE
Workplace
COMMUTE
Home / Bed
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 payments
Vending: Automatically reorders supplies before it's empty
Exercise Equipment: Recognizes individual user and tracks workout schedule

Fig. 1. IoT architecture

Vehicular security is also an area in which attention is needed among all embedded security aspects. From the first day when electronic devices were installed into cars, they have been a feasible target for malicious attacks. Some of the already common attacks are mileage counter manipulation, unauthorized chip tuning or tachometer spoofing. We can observe in our daily life that there are a lot of application that are affecting our lives are smart phones, refrigerators, multimedia players. All of these use embedded computing. But they are unsecured in nature. Security for these systems is really important aspect and could prove a more difficult long-term problem than security does today for desktop and enterprise computing. Security issues are not new for embedded systems. Because they are connected to internet so they are more prone to intrusions and malicious attacks. Unfortunately, the security techniques implemented in enterprise and desktop computing might not satisfy the security requirements of embedded applications. With the advent of Internet of Things in embedded computing, breach of security for network, data, hardware and software are in rise. Many embedded systems are very much susceptible to a type of non-invasive attacks called side-channel attacks. These types of attacks consist of software attacks and these attacks use the statistical analysis of operational characteristics of the device to extract secret information. In these attacks some goals on the devices are fixed; the first kind of attack is the extraction of secret information, the second one is trying to put the system out of order.

SOLUTIONS FOR EMBEDDED SECURITY

When we talk about the solutions of security attacks then There are many existing solutions available for different types of attacks. When confidentiality is required the encryption of information is used. The cipher algorithms that used are: RSA, ECC, AES, 3DES.the integrity of a message is checked by The hash of information by providing a signature which is unique for each message. The algorithms used are MD5 and SHA. Some of the communication protocols are also used for non-repudiation, availability and authenticity. These algorithms are computationally intensive processes. That's why Digital Signal Processors are required in these systems. These are dedicated and special types of processors. So that security primitive instructions are implemented easily. An analogy can be done with DSP through its multiplication-accumulation instruction for digital signal processing. In most cases, security processors are dedicated to one class of ciphering algorithm (symmetric or asymmetric). Some of the authors propose processors with instructions for symmetric ciphering algorithms. Researchers discussed an analysis of a 0.25um physical design that runs the standard Rijndael cipher algorithm (3DES) 2.25 times faster than a 600MHz Alpha 21264 processor. Some specific instructions are defined For processors dedicated to asymmetric ciphering algorithms. "For instance to efficiently compute the modular exponentiation is used in ECC and RSA. However, there still exists significant difference between requirements of security processing and the capability of an embedded processor. This difference is termed security processing gap".

CONCLUSION AND FUTURE WORK

Security feature is very much important aspect for today's computer generation of technologies. As pervasive nature of computing is becoming very popular for the wide range of applications. As embedded system devices are involved in almost all today's and next generation computing applications. In this paper we have discussed the use of embedded systems in applications of Internet of things. Applications of IoT and embedded systems are also discussed. Vulnerability to security attacks in these types of systems is the main point of analysis. The analysis is based on the attacks and the solutions of those attacks. As in general purpose and desktop computing a lot of security frameworks are already available. But in embedded systems, these security frameworks are very intensive. So future works can be the implementation of an efficient security algorithm that can be used in the devices having less computing power.

"IoT mainly consists 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. It is very crucial to reduce susceptibility to side-channel attacks through the use of hardware techniques that reduce correlation between data values and side-channel information, like power, time, etc".

REFERENCES

1. Mark Weiser, "The Computer for the Twenty First Century," Scientific American, pp. 94-104, September, 1991.
2. A. Dix, J. Finlay, G. Abowd, and R. Beale, "Human-Computer Interaction," Prentice Hall, 3e, 2004.
3. G.D. Abowd, G.R. Hayes, G. Iachello, 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.
4. P.Koopman, "Embedded system security," IEEE Computer, vol. 37, issue. 7, pp. 95-97, 2004.
5. Ross J. Anderson, "On the security of digital tachographs," 5th European Symposium on Research in Computer Security (ESORICS '98), pp. 111–125, Springer-Verlag, London 1998.
6. Richard Evans and Jonathan D. Moffett, "Derivation of safety targets for the random failure of programmable vehicle based systems," In SAFECOMP, pp.240–249, 2000.
7. 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.
8. 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.
9. K. Lemke, C. Paar, and M. Wolf (Eds.), "Embedded Security in CarsSecuring Current and Future Automotive IT Applications," Springer-Verilag, 2006.
10. 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.

11. T. Alves and D. Felton, "TrustZone: Integrated Hardware and Software Security, Enabling Trusted Computing in Embedded Systems," ARM Whitepaper, July 2004.
12. H. Nahari, J. Ready, "Employ a secure flavor of Linux," Embedded Systems Design, pp. 20 - 29, Oct, 2007.
13. "Attacks on Mobile and Embedded Systems: Current Trends," Mocana whitepaper, www.mocana.com, 2009.
14. D. Dagon, T. Martin, and T. Staner, Mobile Phones as Computing Devices: The Viruses are Coming!, IEEE Pervasive Computing, vol. 3, no. 4, pp. 11- 15, 2004.
15. L. Wu, C. Weaver, and T. Austin, "CryptoManiac: a fast flexible architecture for secure communication", Proceedings of the 28th annual international symposium on Computer architecture (ICSA'01), vol. 29, issue. 2, May 2001.
16. H. Eberle et al, “A Public-Key Cryptographic Processor for RSA and ECC,” Proceedings of the Application-Specific Systems, Architectures and Processors (ASAP’04), 2004.
17. S. Ravi, A. Raghunathan, N. Potlapally, and M. Shankaradass, "System design methodologies for wireless security processing platform," in Proc. Design Automation Conf., pp. 777-782, June 2002.
18. E. Rippel, “Security challenges in embedded design," www. discretx.com, 2009.
19. A. P. Fuchs, A. Chaudhuri, and J. S. Foster, "SCanDroid: Automated Security Certification of Android applications”, http://www.cs.umd.edu/~avik/papers/scandroidascaa.pdf, 2009.
20. R. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems," Wiley, 2008.
21. 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.
22. J. S. Coron, D. Naccache, and P. Kocher, "Statistics and information leakage," ACM Transaction on Embedded Computer Systems, vol. 3, pp. 492 - 508, Aug. 200