ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Embedded Systems: Security Threats

Ravindra Kumar Chahar

Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh, India

Email Id: ravindra.chahar@Galgotiasuniversity.edu.in

ABSTRACT: Embedded system is a system that is part of a larger system and executes the specific task. Embedded industries were a booming session in a few years back in many countries. With the growing use of embedded devices in daily lives, security threats also grew proportionally. Nonetheless, ensuring safety in embedded systems has become a big challenge not only for the experts on embedded devices but also for the manufacturers. The problem arises in particular because of the designers ' restricted implementation choices for the hardware and software. At the same time, companies are trying to keep those embedded devices ' operating system vulnerabilities in secret and they are not rapidly relieving any required security updates. In this paper author addressed widely the mechanisms, features and applications of various embedded devices within our daily lives. In addition to this, he also addressed the various causes of security threats and some of our suggested solutions to secure the networks from attackers as well as the ones we identified in our study.

KEYWORDS*:* Cryptography, Firmware, Hackers, Microcontroller, Real-Time Constraints

I. INTRODUCTION

An embedded system can be described as a specific type of computer system executing some particular pre-defined programs that are commonly used within a wider scale of electrical or mechanical system. Commonly, small MP3 players start with largely complex hybrid vehicle systems. Due to the fact that embedded system is a main technology in consumer electronics, automobile, military and aerospace, telecommunications, data communication and office automation industries, it has a large fraction of a digital system branding. All use 32 bit microprocessor in embedded system worldwide[1]. It processor offers special purpose features as compared to software used for general purposes such as desktop users. The embedded processor has far surpassing growth rates than traditional computers. Often defined as real-time systems is the embedded system, which means that they have real-time response such as time analysis, worst case execution time etc. Embedded systems must satisfy the safety, availability, reliability and also performance of some important specifications[2]. Due to small size and flexibility requirement, these systems also require extreme low production costs for small and managed resource consumption and also have restricted hardware power. With increasing complexity of real-time embedded system, demand tends to increase with technological requirements, early detection of errors, high-level design, integration, efficiency, verification and maintenance that increase the value of life-cycle properties such as reliability, portability. Approximately all of the embedded systems nowadays are connected to the Internet[3]. Thus security threats have become a major issue at the moment because most embedded systems lack even more security than personal computers do. Another explanation for this lack of security is the very minimal possibilities of integrating hardware and software for the manufacturers of embedded system companies. Somehow they have to compete with the competitive market price of the other embedded manufacturing companies because they all have to hold the lowest possible price in order to maintain consumer satisfaction and at the same time do not carry out any clear safety testing of their embedded goods manufactured[4].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

II. REQUIREMENT FOR EMBEDDED SYSTEM

Small size, low weight:
Most embedded computers are located in the device in the larger plane. Weight is a vital issue for fuel economy or human endurance in the portable and transportation systems. Mission critical system as an example requires a lot more weight. And stringent size than the others because it uses in flight vehicles, all examples have restrictions of this type[5].
Safety and reliable:
All devices are at risk of failure. Generally, some systems have distributed census protocols or multiplied redundant comports to ensure continued operational redundancy in processing for the fault tolerance technique.
Harsh Environment:
Some embedded system doesn't run in controlled environment. The issue is unnecessary temperature, especially in those combustion applications (e.g., transport). Other issues can be caused by the need to protect against shock, noise, fluctuations in power supply and general physical abuse for embedded computing.
Cost Sensitivity:
Price in embedded computers is always important issue. One explanation why machine price may have an impact on productivity is the role of proportion of cost changes compared to total cost as a contrast with digital cost. Fig.1 shows the VIA VAB-800 10 cm x 7.2cm Pico-ITX embedded ARM board.

Fig. 1: VIA VAB-800 10 cm x 7.2 cm Pico-ITX Embedded ARM Board

III. CHARACTERISTICS OF EMBEDDED SYSTEMS

Embedded systems are usually designed to perform any specific pre-defined function that must meet some real-time constraint. A computer is used to perform multiple user-defined functions, the key distinction between a computer and an embedded device. On the other side, an embedded device is used to perform a specific function which the manufacturers predefined. Meeting all the real-time constraints here is a very significant feature of an embedded system[6]. A restriction on real time is split into two sections. First is a hard real-time system and the other is a soft real-time system. Hard real-time system means that it must fulfill all its schedules with zero degree of flexibility and in the soft real-time system it is acceptable to be lowly flexible. The embedded systems don't always need to be stand-alone. Most of the embedded systems are currently integrated within a broad computerized network. Definitions of standalone embedded devices include devices such as MP3s, cameras, and TV remotes. Embedded devices car and nuclear power plant good examples. GPS, fuel injection controller, anti-lock brake system, transmission controller, cruise control, active suspension, air-bag system, air-conditioner, display monitor-all systems are incorporated into a modern automotive system. The word' firmware' is used to relate to program specifications created for embedded systems. It's located in ROM (Read Only Memory) or in a memory flash chip. Resources such as computer hardware needn't run much. The dedicated user interface is another significant feature of embedded systems. This can vary from no user interface to a complex user interface[7]. No user interface is required for single button and LED device. User

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

interface means that with the on-screen display the function of the button will change and the range depends on the user. A good example of user interface system is handheld device such as joystick that needs to be pointed to with the phone. For an embedded device the size and weight should be smaller. For that purpose, microcontrollers are used for delivering the best performance on demand in embedded devices. Microcontrollers are typically required to perform repetitive functions for long periods of time without failure. In addition, it must be efficient and reliable in case of certain special devices, such as the anti-locking brake system for automobiles and the control systems for nuclear power plants. Compared to those features, embedded systems must also be cost-effective. Manufacturers try to keep their goods to the lowest price. It may also be connected to physical surroundings using sensors and actuators.

IV. APPLICATIONS OF EMBEDDED SYSTEMS

In terms of use, embedded systems have become parts and pieces of our everyday life. Everyday use of are comprehended in the given table. Table.1 shows the embedded system usage in daily life.

TABLE 1: Examples of Embedded Systems Used in Daily Life

Home Applications	Home Security Systems, HVAC, DVD player, Answering Machine, Garden Sprinkler Systems, Lighting Systems, Remote Controls, Air Conditioners, Sprinklers, Dishwasher, Washing Machine, Microwave Oven, Top-Set Box.
Consumer Electronic Products	Mobile phones, cordless phones, cameras, video recorders, DVD players, television sets, calculators, stereo systems, cable TV tuners, digital watches, personal PDA, iPhone.
Industrial applications	Private Smart Phone, Fax Machines, Image Copy Machines, Printers, Scanners, Data Collection System, Stress Control, Voltage, Current, Temperature, Detection of Hazards, Industrial Robot.
Business Equipment	Automatic Toll Systems, Voice Recognizers, Smart Vendor Station, Cash Register, Bar Code Reader, ATM, Cash Registers, Alarm Systems, Card Readers, Finger Print Detectors.
Automobile	Air-conditioner, GPS, Fuel Injection Controller, Anti-locking Brake System, Transmission Controller, Cruise Control, Active Suspension, Air-Bag System.
Communication Systems	Web camera, modem, network cards, teleconferencing system, firewall, server, cell phone.
Aerospace	GPS, Automatic Landing System, Inertial Guidance System for Flight Attitude Controller, Space Robotics, RADAR.
Medical Technology	Digital Pulse Monitor, CT scanner, ECG, EEG, EMG, MRI, Glucose Control, Blood Pressure Monitor, Diagnostic Machine, X-ray machines.
Security Systems	Airport Security System, Alarm System, Digital Access Card, Fingerprint-based Smart Card, Face Recognition System, Finger Recognition, Irish Recognition, Building Security System.
Classroom applications	OCR, Calculator, Smart Cord, Stereo Systems, Projector, Smart Screen, Smart Suite.
Game and Entertainment	Robot, MP3, Mind Storm, Intelligent Toy Video games.

V. CAUSES OF SECURITY THREATS OF EMBEDDED SYSTEMS

In this era of advanced technology, nearly all embedded devices are connected to various network systems like internet. On the one hand, these embedded devices are more related to daily life day by day, while on the other hand, as a proportional pace, their security threats are also rising[8]. Security threats are by no means a new phenomenon in the embedded systems. When internet connections expose applications to intrusions and malicious attacks, the problem arises. Some major causes of security threats to embedded systems are clarified below:

One of the main disadvantages of embedded systems is that they are particularly cost sensitive. In the case of heavy manufacturing products a little change in cost will make a big difference. This cost sensitivity results in producers using a 4-bit or 8-bit processor. Many of those 8-bit microcontrollers can't store bigger cryptographic key. Embedded devices usually have to perform the same function over and over again using loop[9]. With clear real-time constraints

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

speed can easily reach 100 loops in every 5 seconds. Thus a simple pause of even 0.01 second will cause a loss of the reliability of the control loop which means that the system can be vulnerable to attacks designed to destroy the timing of the system. Embedded systems most of the time has no real administrator by which the hackers can easily unleash an internet-connected device via distributed Denial-of-Service (DoS) attacks. Most embedded systems often even by the single engineer are designed and developed by the small development teams. Institutions that produce few kilobytes of code per year normally cannot afford any embedded system security specialist, even though they do not appreciate the security specialists ' requirement as well.

Most embedded systems, such as PDAs or mobile phones, have major battery constraints and are powered by batteries. Many embedded systems will charge fresh batteries daily, while others need to last months or years based on a single battery. An intruder can cause system failure by attempting to drain the battery particularly when system protection is very high or nearly impossible to breach the specific device's security system. This insecurity is very crucial and exacerbates device security[10]. As an instance, it is not easy to ensure enough protection in the battery-powered device using the power-hungry wireless communication system at all. Firmware is being completed day by day, and in the near future will be more complete. This will heighten further vulnerabilities and other security issues. One explanation might be to use more common programming languages like C and C++, as they are very powerful for embedded systems. They can't protect against basic kinds of attacks like buffer overflows though. Although small programs can theoretically prove to be stable, against complex programs it's about impossible.

VI. CONCLUSION

Embedded systems have made lives simpler and more relaxed by meeting almost all of the constraints in real time. Even though it is popular among the mass people, they are quite unconscious of the likely security threats that even the manufacturers and engineers associated with embedded devices have been facing up to now. Expert attackers from the various parts of the world have already identified several security vulnerabilities of the embedded devices and are working on them further. It is therefore very clear that a massive blow to the technology industry could be generated in the near future if the engineers and manufacturers do not take the necessary security solutions as stated in this paper to prevent unauthorized access from unsecured third parties.

REFERENCES

[1] G. Martin, L. Lavagno, H. Hansson, M. Nolin, T. Nolte, and K. Thramboulidis, “Embedded systems,” in *Systems, Controls, Embedded Systems, Energy, and Machines*, 2017.

[2] L. Daqing, K. Kosmidis, A. Bunde, and S. Havlin, “Dimension of spatially embedded networks,” *Nat. Phys.*, 2011, doi: 10.1038/nphys1932.

[3] N. Cowan, “An Embedded-Processes Model of Working Memory,” in *Models of Working Memory*, 2012.

[4] M. Wolf, *Computers as components: principles of embedded computing system design*. 2012.

[5] H. Kaur and J. Singh, “Review on Embedded System,” *Int. J. Innov. Res. Electr. Electron.Instrum. Control Eng.*, 2013.

[6] P. Marwedel, *Embedded System Design Embedded Systems Foundations*. 2010.

[7] A. Barua, M. M. Hoque, and R. Akter, “Embedded Systems: Security Threats and Solutions,” *Am. J. Eng. Res.*, 2014.

[8] K. K. R. Choo, Y. Fei, Y. Xiang, and Y. Yu, “Embedded device forensics and security,” *ACM Trans. Embed. Comput. Syst.*, 2016, doi: 10.1145/3015662.

[9] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, “Cyber Security Threats to IoT Applications and Service Domains,” *Wirel. Pers. Commun.*, 2017, doi: 10.1007/s11277-017-4434-6.

[10] D. Papp, Z. Ma, and L. Buttyan, “Embedded systems security: Threats, vulnerabilities, and attack taxonomy,” in *2015 13th Annual Conference on Privacy, Security and Trust, PST 2015*, 2015, doi: 10.1109/PST.2015.7232966.

- NishaPandey, B. S. Chowdhary , Bhagwan Das , D. M. Akbar Husain , Vishal Jain , Tanesh Kumar, “Design of Data Processing Device on Low Power SPARTAN6 FPGA”, International Journal of Control and Automation (IJCA).
- SujeetPandey, PuneetTomar, LubnaLuxmiDhirani, D. M. Akbar Hussain, Vishal Jain, NishaPandey, “Design of Energy Efficient Sinusoidal PWM Waveform Generator on FPGA”, International Journal of Signal Processing, Image Processing and Pattern Recognition (IJSIP), Vol. 10 No. 10, October, 2017, page no. 49-58 having ISSN No. 2005-4254.
- P. Lavanya, R. Meena, R. Vijayalakshmi, Prof. M. Sowmiya, Prof. S. Balamurugan , “ A Novel Object Oriented Perspective Design for Automated BookBank Management System”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Issue 2, February 2015.