American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-03, Issue-12, pp-119-123
www.ajer.org
Research Paper Open Access

Embedded Systems: Security Threats and Solutions

Anik Barua[1], Mohammad Minhazul Hoque[2], Rubina Akter[3]
[1, 2, 3] *(Department of ICT, Mawlana Bhashani Science and Technology University, Bangladesh)*

ABSTRACT : *With the increasing use of embedded devices in our daily life, security threats have also been increasing in a proportional rate. However, ensuring security in the embedded systems has become a great challenge not only for the embedded device experts but also for the manufacturers. The problem especially arises because of the limited hardware and software implementation options for the designers. At the same time, companies are trying to keep the vulnerabilities of the operating system of those embedded devices in secret and they are not relieving any necessary security updates quickly. It has become very urgent to ensure proper security of the embedded systems to save it from any major technological disaster near future. In this paper, we have broadly discussed the structures, characteristics and applications of different embedded devices in our daily life. Beside this, we have also discussed about the different causes of security threats and some of our suggested solutions to protect the systems from the attackers as well that we have found in our research.*

KEYWORDS: *cryptography, firmware, hackers, microcontroller, real-time constraints*

I. INTRODUCTION

An embedded system can be defined as a special type of computer system that performs some specific pre-defined programs which is generally used within a larger scale of electrical or mechanical system. Generally, it is started from small MP3 players to largely complex hybrid vehicle systems. Some other examples of frequently used embedded systems in our daily life are keyboard, mouse, ATM, TV, PDA, cell phone, printer, elevator, smoke detector, DVD player, refrigerator, camera, GPS navigator, radio, TV remote, telephone, game controller, monitor, digital image processor, bar code reader, SD card, washing machine, anti-lock breaking system, blender etc. We use embedded systems especially because of its dependability, efficiency and it meets the real-time constrains.

Examples of the embedded system show that it has become a part and parcel of our daily life in term of use. We are very familiar with the term ‘Smart Home’ because of the deployment of smart embedded system in our home. Now-a-days almost all of the embedded systems are connected with the internet. So security threats have become a major issue at present because most of the embedded systems lack security even more than personal computers. One of the reasons for this lack of security is the very limited hardware and software implementation options for the manufacturers of embedded system companies. Again they have to deal with the competitive market price of the other embedded manufacturer companies because they all have to keep the lowest possible price to maintain the customer satisfaction and at the same time they do not conduct any specific security research of their manufactured embedded products. This leads to the security threats for the embedded devices because ensuring advance security techniques for embedded systems means the higher cost of that embedded products. Customers also don’t want to be more expensive usually when buying an embedded device and they are not concerned also about the probable security threats of their products. Lack of security analysis and low-cost market product mentalities of the manufacturer companies lead the hackers the exact environment they are expecting for. Many embedded systems hacking tools are easily available in the internet. Hacking in the PDAs and modems are very common example of embedded systems hacking.

Recent development trends of the embedded systems protocol are going to be convergence because of its applications in TCP/IP protocol for the purpose of inter-media interfacing. In this case, using IPv6 will cost much more for the development of the embedded applications at least for the next few years. As a result IPv4 is going to dominate in the applications of embedded systems. This IPv4 is much more challenging for its internal security problems in terms of authentication, integrity and confidentiality.

II. STRUCTURE, CHARACTERISTICS AND APPLICATIONS OF EMBEDDED SYSTEMS

Although there are many types of applications, the principle of the embedded device structures is typically the same in terms of system components and design methodologies. Complex applications such as chemical plants may need standard I/O (Input / Output) devices but this is not mandatory for the most of the other embedded systems. At present, most of the embedded systems are microcontroller based that means memory and other specific devices are integrated with the Central Processing Unit (CPU). In general it can be divided into three categories: small, medium and large. Small such as TV remote needs 4-bit microcontrollers. 8-bit or 16-bit microcontrollers are well enough for medium size systems such as automated data acquisition systems and 32-bit or more needed for the high–end large scale computer system such as plant monitoring and central control system.

Embedded systems are not standalone always rather than in the most of the time it is used as a part of a larger complex device. Here performance based real-time constrains must be met for the usability and safety of those devices. Graphical user interface is not always mandatory for the small scale device such as simple button or LED (Light Emitting Diode). But it is a must for the bigger and complex devices such as nuclear power plant systems along with the networks, data bus connections, screen-edge systems etc.

Figure 1: VIA VAB-800 10 cm x 7.2 cm Pico-ITX embedded ARM board

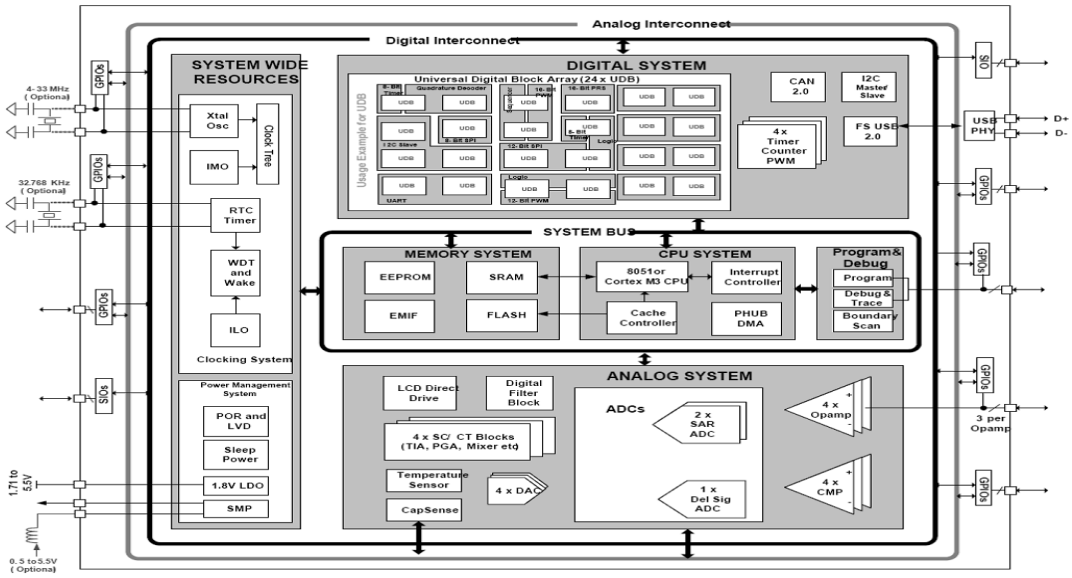

Figure 2: Block diagram of Cypress PSoC 5 (32-bit ARM Cortex-M3 processor) embedded ARM board

The term 'PSoC' stands for Programmable System on Chip. It is a programmable embedded design platform which integrates discrete, analog and programmable logic with a memory and a microcontroller. PSoC 5 is based on 32-bit ARM Cortex-M3 processor. It allows the designer to make flexible changes during design, validation and production. It is easy to reconfigure and implement using fewer system components. A single PSoC device can integrate about 100 peripheral functions. It also offers single-chip integration of multiple buttons, sliders, touch pads and proximity detectors with requiring no external components for sensing.

Characteristics of Embedded Systems:

In general, embedded systems are designed to perform any particular pre-defined task that must meet any real time constraint. The main difference between a computer and an embedded system is a computer is used to perform multiple tasks defined by the user. On the other hand, an embedded system is used to perform a specific task that is pre-defined by the manufacturers. Here, meeting all the real-time constraints is a very important characteristic of an embedded system. A real-time constraint is divided into two parts. One is hard real-time system and the other is soft real-time system. Hard real-time system means it must meet all its deadlines with a zero degree of flexibility and it is acceptable to be little flexible in the soft real-time system. It is not necessary to be standalone always for the embedded devices. Actually most of the embedded systems are integrated within a large computerized device. Devices such as MP3s, cameras and TV remotes are the example of standalone embedded devices. For the example of integrated embedded devices car and nuclear power plant are some good examples. GPS, fuel injection controller, anti-locking brake system, transmission controller, cruise control, active suspension, air- bag system, air-conditioner, display monitor-all the devices are integrated in a modern car system.

The term 'firmware' is used to refer the program instructions written for embedded systems. It is stored in ROM (Read Only Memory) or in a flash memory chip. Resources like computer hardware do not need much to run. Another important characteristic of embedded systems is the dedicated user interface. It may range from no user interface to complex graphical user interface. For simple button and LED system, no user interface is needed. User interface means the task of button can change with the on-screen display and the selection depends on the user. Handheld device such as joystick which needs to be pointed with the screen is a good example user interface system. Size and weight should be less for an embedded device. For that reason, microcontrollers are used in embedded devices to deliver the best performance on demand. Generally, microcontrollers are required to perform repeated functions for long time without any failure. Beside this, it must be reliable and safe in case of some special systems such as car's anti-locking brake system and nuclear power plant controlling systems. Adding to those characteristics, embedded systems must be cost efficient also. Manufacturer companies try to keep the lowest price of their products. Using sensors and actuators it may be also connected with physical environment.

Applications of Embedded Systems:

As we describes earlier, embedded systems have become parts and parcels of our daily life in term of use. From the following table we can easily understand our daily use of embedded systems.

Table 1: Examples of embedded systems used in our daily life

Home Applications	Dishwasher, Washing Machine, Microwave Oven, Top-set Box, Home Security Systems, HVAC system, DVD player, Answering Machine, Garden Sprinkler Systems, Lighting Systems, Remote Controls, Air Conditioners, Sprinklers.
Consumer Electronic Products	Cell phones, Cordless Phones, Digital Cameras, Video recorders, DVD players, TV set, Calculators, MP3 Players, Stereo Systems, Cable TV tuners, Digital watches, Personal PDA, iPhone.
Industrial applications	Personal Smart Phone, Fax Machines, Photo Copy Machines, Printers, Scanners, Assembly Line, Data Collection System, Monitoring Systems on Pressure, Voltage, Current, Temperature, Hazard Detecting System, Industrial Robot.
Business Equipment	ATM, Cash Registers, Alarm Systems, Card Readers, Finger Print Detectors, Automatic Toll Systems, Voice recognizers, Smart Vendor Machine, Cash Register, Bar Code Reader.
Automobile	GPS, Fuel Injection Controller, Anti-locking Brake System, Transmission Controller, Cruise Control, Active Suspension, Air- bag System, Air-Conditioner.
Communication Systems	Router, Hub, Cell Phone, Web Camera, Modem, Network Cards, Tele-conferencing System.
Aerospace	GPS system, Automatic Landing System, Flight Attitude Controller Inertial Guidance System, Space Robotics, RADAR.
Medical Technology	CT scanner, ECG, EEG, EMG, MRI, Glucose Monitor, Blood Pressure Monitor, Diagnostic Device, X-ray machines, Digital Pulse Monitor.
Security Systems	Face Recognition System, Finger Recognition, Irish Recognition, Building Security System, Airport Security System, Alarm System, Digital Access Card, Fingerprint based Smart Card.
Classroom applications	Smart Board, Smart Room, OCR, Calculator, Smart Cord, Stereo Systems, Projector.
Game and Entertainment	Video games, Robot, MP3, Mind Storm, Smart Toy.

III. CAUSES OF SECURITY THREATS OF EMBEDDED SYSTEMS

In this age of advanced technology, almost all of the embedded systems are connected to different network systems such as internet. At one side, these embedded devices are being more connected to our life day by day whereas on the other hand its security threats are also increasing as a proportional rate. Security threats in the embedded systems are not a new concept at all. As an example, in the year of 2001, Peter Shipley and Simson L. Garfinkel claimed that they have found an unprotected modem line to a system that could control a high voltage power transmission line. Internet enabled home applications are very available now. However the problem arises when internet connections expose applications to intrusions and malicious attacks. Some major causes of embedded system security threats are explained below:

One of the major limitations of embedded systems are they are very cost sensitive. A little change in cost can make a big difference in the case of heavy manufacture devices. This cost sensitivity leads manufactures to use4-bit processor or 8-bit processor. Bigger cryptographic key cannot be stored by many of these 8-bit microcontrollers. Embedded devices have to perform same task again and again usually by using loop. Here, speed can easily reach to 100 loops in every 5 seconds with strong real-time constraints. Therefore, a single delay of even 0.01 second can cause a loss of control loop stability which means the system can be vulnerable to attack that is designed to destroy the system timing. In the most of the time, embedded systems have no real administrator by which an internet connected device can be easily launched by distributed denial-of-service (DoS) attacks by the hackers. Many embedded systems are designed and developed by the small development teams even by the single engineer sometime. Organizations that write few kilobytes of code per year usually cannot afford any embedded system security specialist even they do not understand the importance the necessity of the security specialists as well.

There are many embedded systems that have significant battery constraints and powered by battery as well such as PDAs or cell phones. Some embedded systems can get fresh battery charge daily but other must last months or years depending on a single battery only. An attacker can create system failure by seeking to drain the battery especially when the security of the system is very high or almost impossible to break the security system of that particular device. This vulnerability is very much critical and worsens the security of the device. As an example, ensuring enough security in the battery-powered device is not easy at all that uses the power-hungry wireless communication system. Firmware is being completed day by day and will be more completed in near future. This will increase more bugs and other security problems. One reason may be the use of more popular programming languages such as C and C++ as they are very efficient for embedded systems. However they cannot protect against the simple kinds of attacks such as buffer overflows. Although small programs can be theoretically prove as safe but it is about impossible against complex programs.

IV. SOLUTIONS OF SECURITY THREATS IN EMBEDDED SYSTEMS

Security requirements of embedded devices can vary from different aspects. As an example of a cell phone system, end user may be concerned about his private data protection while content provider may be concerned about copy protection of the multimedia contents delivered to the cell phone and manufacturers may be concerned about the proprietary firmware that has been used in that cell phone. Here the system of attack may also vary for users, content providers, manufacturers etc. We have already described different challenges of embedded systems in term of security and in this section we will describe some probable solutions also to get rid of those problems also. Modern cryptography techniques provide strong defiance against the conventional attacks. However, much more effort and care is still required in the software design to make the system more protected from bugs and design flaws. Designers should be emphasizing more on Software Development Life Cycle (SDLC). Different secure level practices should be applied which can be classified into three. They are the design level, the implementation level and the testing level. Tamper-resistance techniques should be strengthening more to protect the system against different software and hardware attacks. These techniques can be used for attack detection, recovery and prevention as well.

To prevent side-channel attacks, different hardware and software level approaches have been proposed to identify symptoms that allow the leak of the system's side-channel information like power dissipation, timing and electromagnetic radiations. Software based countermeasures include randomization instruction sequence, introducing dummy instructions, bit splitting and balancing hamming weights of internal data. Randomization can also be applied on the clock signal or the power consumption. It has been experimented that software based countermeasures are most efficient although they slightly decrease the performance of cryptographic algorithm in terms of memory, energy and execution time.

Security solution in the architectural level should also be improved that means consider the mapping of adopted algorithms and protocols more efficiently. One solution to overcome the limitation of software based efficiency is to implement the resource-greedy cryptographic computations on a dedicated hardware using Application Specific Integrated Circuits (ASICs). Therefore 'hardwired algorithm' approach may be followed for its proven performance although it's costly.

Beside those solutions, some extra added modules such as SSL and SSH may also be implemented. It would be the best solution to protect many attacks such as denial of service (DoS) attack, spooling, hijacking and sniffing although implementation of such value added module is not mandatory because of the lacking of hardware resources available.

V. CONCLUSION

Embedded devices have made our life more easy and comfortable by meeting almost all the real-time constraints. Although it is very popular among the mass people but they are quite unconscious about the probable security threats till now even the manufactures and the engineers associated with embedded devices. Expert hackers from the different parts of the world have already found many security pitfalls of the embedded devices and they are further working on it. So, it is very clear that it could create a huge blow in near future for the technological industry if the engineers and the manufactures do not take the necessary security solutions as proposed in this paper to protect the unauthorized access from the unsecured third party. We heartily believe that more concentration on cryptography, tamper-resistance techniques, advanced microcontroller and algorithms can mostly make the embedded devices secure enough. At the same time, it is also important for the manufacturer companies to design and implement the whole embedded system with much more security concern.

REFERENCES

[1] Sudhakar Singh, Prashant Mor and Gajendra Singh, Application of Embedded Systems in Modern Society, VSRD International Journal of Electrical, Electronics & Communication Engineering, 2 (6), 2012, 373-384

[2] Jesús Lizarraga, Roberto Uribeetxeberria, Urko Zurutuza, Miguel Fernández, Security in Embedded Systems, Computer Science Department, Mondragon University, Spain

[3] Lyes Khelladi, Yacine Challal, Abdelmadjid Bouabdallah, and Nadjib Badache,On Security Issues in Embedded Systems: Challenges and Solutions, International Journal of Information and Computer Security, 2(2), 2008, 140-174

[4] James O. Hamblen, Introduction to Embedded Systems Using Windows Embedded CE, School of Electrical and Computer Engineering, Georgia Institute of Technology, USA, 2007

[5] Philip Koopman, Embedded System Security, Associate Professor,Department of Electrical and Computer Engineering, Carnegie Mellon University, 2004

[6] Bergman, P., Berman, S., The Criminal Law Handbook: Know Your Rights, Survive the System

[7] Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan and Srivaths Ravi, Security as a New Dimension in Embedded System Design, NEC Laboratories America, Princeton, NJ

[8] Bleichenbacher, D., and Nguyen, P. Q. 2000, Noisy polynomial interpolation and noisy Chinese remaindering. Advances in Cryptography, EUROCRYPT 2000

[9] Kaufman, C., Perlman, R., Speciner, M. Network Security: Private Communication in a Public World, Second Edition.

[10] Morrose, F., Reiter, M., and Wetzel, S (1999), Password hardening based on keystroke dynamics. ACM Conference on Computer and Communication Security

[11] National, R. C., (2002), Cyber Security Today and Tomorrow: Pay Now or Pay Later, National Academy Press, Washington, D.C.

[12] Massey, J. L. 1969, Shift register synthesis and bch decoding. IEEE Transactions on Information Theory vol. 15, no. 1, pp. 122-127

[13] Smeulders, AWM 2000, Content based image retrieval at the end of the early years', IEEE Transactions on pattern analysis and machine intelligence, pp. 1349-1380

[14] Phrack Magazine 2014, Hacking with Embedded Systems, www.phrack.org

[15] Embedded Insights Inc. 2012, Security and Encryption, www.embeddedinsights.com

[16] Embedded Systems, www.wikipedia.org