Erzincan Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
2019, 12(3), 1468-1484
ISSN: 1307-9085, e-ISSN: 2149-4584
Araştırma Makalesi

Erzincan University
Journal of Science and Technology
2019, 12(3), 1468-1484
DOI:10.18185/erzifbed.565044
Research Article

The Security Vulnerabilities on Internet-Enabled Embedded Systems

Ahmet EFE[1*], Melike SARIKAYA[2], Merve ALTINBAŞ[3]

[1*]Ankara Kalkınma Ajansı, PhD, CISA, CRISC, PMP, Ankara, Turkey

[2,3] Department of Computer Science, Ankara Yıldırım Beyazıt University, Ankara Turkey

Geliş / Received: 14/05/2019, Kabul / Accepted: 15/12/2019

Abstract

As technology is improved, mobile and small devices have been started to be used more often in e-government and smart city applications. Although IoT devices are exposed to attack, they do not have security standards and proper built-in measures known by all. It is very difficult to define the security breaches in the embedded systems, and it is a low possibility to detect the vulnerabilities. Remote analysis of embedded systems is very difficult. Embedded systems with the most security concerns are networked embedded systems. This year, the ban on Huawei products by the US and a number of western countries is due to the main concerns in cyber security. IoT and embedded system security vulnerabilities in critical infrastructures can now become an international problem involving the military and governments. For this reason, a study carried out according to the general structure of embedded systems to define and overcome these deficits. In this work, security vulnerabilities in networked embedded systems and security standards against these vulnerabilities are examined within the literature to propose main characteristics of a secure IoT in both government and business cyber environments.

Keywords: Embedded systems, Security standards, Microprocessor, IoT, E-government security

Internet Bağlantılı Gömülü Sistemlerde Güvenlik Açıkları

Öz

Bugünlerde teknoloji geliştikçe mobil ve küçük cihazlar e-devlet ve akıllı şehir platformlarında daha fazla alanda ve daha sıklıkla kullanılmaya başlanmıştır. Bir cihaz ne kadar fazla kullanılırsa hatanın ve güvenlik açıklarının verdiği zarar daha fazla olacaktır. Bu tür küçük cihazlar, bilgisayarların uğradığı saldırılara maruz kalsa da, herkes tarafından bilinen güvenlik standartlarına sahip değillerdir. Gömülü sistemlerde güvenlik açığını yakalamak çok zordur, neden kaynaklı bir açık olduğunu görmek düşük ihtimalli bir durumdur. Gömülü sistemlere uzaktan analiz yapmak zordur. En çok güvenlik açığı çıkan gömülü sistemler internete bağlı ağ bağlantılı gömülü sistemlerdir. 2019 yılında Huawei ürünlerine karşı ABD ve bir takım batı ülkelerinin yasak koyması siber güvenlik alanındaki temel endişelerden kaynaklanmaktadır. IoT ve kritik alt yapılardaki gömülü sistem güvenlik açıkları artık askeriye ve hükümetlerin dahil olduğu uluslararası bir sorun haline gelebilmektedir. Bu nedenle bu açıkları gidermek için gömülü sistemlerin genel yapısına göre bir çalışma yapılmıştır. Bu çalışmada devlet ve iş dünyası tarafından kullanılan ağ bağlantılı gömülü sistemlerdeki güvenlik açıkları ve bu güvenlik açıklarına karşı bulunan güvenlik standartları temel güvenlik niteliklerini belirlemek için literatür üzerinden analiz edilmektedir.

Anahtar Kelimeler: Gömülü Sistemler, Güvenlik Standartları, Mikroişlemci, IoT, E-devlet güvenliği

*Corresponding Author: aefe@ankaraka.org.tr

1. Introduction

The embedded system is an integrated system formed by electronic hardware and software, which takes place in any system and makes that system intelligent to some degrees. The biggest difference from the software in our computers is that they perform a single task and indirectly interact with the user and is under control of users. It is possible to see embedded systems in almost all of our products we use in our daily lives apart from telecommunication and network nodes, the personal computers, printers, scanners, calculators, mobile phones, television cameras, dishwashers, electronic toys and so on.

Figure 1. The Usage Area of Embedded System (Aydın, 2016)

All of these devices benefit from the microprocessor, memory and network communicator and using wireless communication. Devices can be roamed anywhere, providing access to mainstream computers in every environment, proving many services to its users. For example, by connecting to a main server, accessing bank accounts, checking the status of production, shopping is becoming a common practice. These devices, called electronic devices, actually contain embedded designs in a small-scale information system. The electronic intervention of malicious users can cause financial losses during usage of devices so the electronic safety of devices are not fully assured and therefore users' confidence can be shaken. For this reason, it is imperative to know the security vulnerabilities and take precautions against them.

1.1.Research Methodology

This research is based on the assumptions are as follows:

- The IoT based embedded systems usage will dramatically increase as part of the pervasive e-government, smart city and industry 4.0 applications.
- The design vulnerabilities are the most important elements of IoT security

We have developed a research question as such: "*what is the hidden danger of embedded systems and what kind of reasonable measures can be taken by institutions and users*?". In this study, attacks on embedded system whose dimensions and costs are low and only that are programmed to fulfil expected tasks and the precautions to be taken against this attack will be explained. First, the overall design of embedded systems will be discussed. The best way to find security vulnerabilities is to understand design of system. After mentioning the answers to research questions, we will analyze the security attacks on embedded systems and how to protect them from attacks.

The operating principle of the embedded systems will be investigated according to the objects used. The work that describes the operation of embedded systems will be examined. It will be discussed which software is being used, how the techniques are applied, which algorithms are used when these techniques are applied in the embedded systems. Then, research on the algorithms used will be done to assess whether or not these algorithms are secure. At the same time, the issues of security concerns that may arise and when these algorithms are applied to embedded systems will also be investigated. Finally, how these security bugs can be prevented and which methods can be used will be explored and explained in the article.

1.2. Embedded System Designs

The design of the embedded system is of crucial importance for its security architecture. Today, the tendency to control what needs to be smarter than embedded systems with microprocessors is very common and spreads at a great pace (here too, we understand that microprocessors are not just used in computers). Unlike computers, semi-permanent software is used in embedded systems. This software embedded in the device is called "Firmware” which is developed more carefully than the software on personal computers. Because they are the software that appeals to a more specific purpose, and the hardware they run is produced assuming that these software will run without error for a long time until the lifetime of the product itself. However, the embedded system may not be in a place we can reach at any moment (either on a space vehicle or under the oil well). This software is stored in the system memory. Microcontrollers and its entire electrical, electronic and mechanical, etc. connected to it. The microprocessor reads the software from the memory understands what it means and runs it. The number of microprocessors used by an embedded system generally increases according to the complexity of the system or the number of subsystems it has.

Embedded systems with microprocessors contain both software and hardware, so this condition makes complexity to system. The software group and the hardware group must be in communication, both individually and systematically. This means that groups can work together and the programming languages they use need to understand each other. Especially C ++ and special libraries are used for this. Like computer programmers, embedded system designers also use compilers, debuggers, and dialers. Various controls can be used in the software process. One of the most common is to use LEDs. This is the general structure of embedded systems. If the overall structure is well understood, security errors can be found more easily.

1.3. The Reason Why Internet-Enabled Embedded Systems Are Available

The Internet of Things offers the possibility of data transmission over the Internet and communication with other objects. Thanks to interned embedded technology, home appliances at work become integrated with mobile phones, computers and other objects while industrial machines can run with a coordinated way. However, IoT devices that have no security or work with limited or obsolete security methods can have disastrous consequences. It will also be difficult to ensure the security of each tiny IoT device. According to The National Intelligence Council report, IoT will be a destructive technology by 2025 due to the number of the devices are projected to reach 30 Billion.

While IoT offers incredible hope, the use of large-scale IoT brings with it a serious cyber security risk. Countries can face a major catastrophe if they do not take the necessary measures. When IoT becomes widespread, there will be many devices on the network. Since most of these devices will be embedded, there will be very limited security software on them or they will not be at all. Therefore, as well as being an easy entry point into the internal network, the safety of these small devices will be an excellent hiding place for malicious code. Therefore, there will be a back door for attackers who want to infiltrate the network if there is intentional or unintentional vulnerabilities of open backdoors. For IoT security, access to the Internet as in power plants will not be a solution. In terms of design, many IoT devices need communication via cloud technology.

The Internet of Things constitutes one of the key elements of digital transformation in all industry sectors. Our world has already changed in production, agriculture, urban infrastructure, retail and automotive industry. This latest industrial revolution is based on all component parts, from sensors to data centers that offer absolute defense solutions that are connected to each other against cyber threats and malicious attackers.

It is possible to create Thin Client, Model Based Technology Approaches that perform Remote Monitoring and Control using low cost TCP / IP Technology. The use of networked protocols is based on the past. With the success of the Internet, the use of TCP / IP is widespread. Now, the TCP / IP based Internet network is facing the next major development: the connection of many embedded systems with relatively low processing power. They will implement a wide range of monitoring and control applications when communicating over centralized servers over the Internet. Although this is a costly method, the advantages are greater. For example, productivity management can be achieved with remote management or monitoring. Alternatively, manufacturers can take advantage of the ability to charge more for the end product, with added value features enabled by connectivity (Dickie, 2003). In addition to these advantages, the disadvantages should not be overlooked. Setting up a remotely monitored system means that malicious people can review it. If such systems are not equipped with security capabilities, the system can be intervened.

1.4. Literature

In the study of (Karataş, 2016) the security, threats and strategies in mobile devices, vulnerabilities, attacks, and measures taken in mobile applications are described. It summarizes not only end-user recommendations, but also the points that should be considered for application developers. It is evaluated that end users can increase personal security by learning basic information about mobile systems' attack methods. The mistakes made while developing the application are mentioned, and the detection of these errors in the application development stage will make the application safer. It has been a nice work with safety step tests and their problems explained in these tests.

A practical study has been carried out on the security of embedded systems and networked embedded systems by (Özcanhan, 2011). After mentioning the attacks that can be done in general, they have been mentioned about their work. IPsec is a very comprehensive, very complex, and resource-intensive standard because it addresses all security aspects of network communication. In this study, IPsec reference was taken. The basic encryption, hashing and communication keys are determined with negotiation. The study suggests the security covering the entire embedded system simplifying IPsec standard. The security procedures squeeze into embedded systems with accurate simplifications. A subset of an internationally accepted standard has been established without inventing a new method. The study is based on the power of the AES encryption algorithm in particular. If the weakness or security implication of this algorithm is determined, the operation is not unsuccessful. Only the replacement of the encryption algorithm with the new allows the developed security application to continue to be used.

In (Michael, 2016) the secure embedded systems are described. Developers have described a system that seamlessly integrates cyber security into US military system software. However, additional security components may interfere with the functionality of a system. At the same time, a well-defined approach is needed in order to be able to perform a study that is both functional and safe. The Lincoln laboratory uses cryptographic auxiliary processes that provide confidentiality and integrity while maintaining the functionality of the secure embedded system common design methodology. This study describes how these processes are used, secure embedded system designs, threat analysis, and security metrics. We have decided to explore what are the last safeguarding capabilities against security attacks in internet-enabled embedded systems.

Security aspects of embedded systems have been studied by Papp et al (2015). It is said that the embedded systems are the driving force for technological development in many domains such as automotive, healthcare, and industrial control in the emerging post-PC era. As more and more computational and networked devices are integrated into all aspects of our lives in a pervasive and “invisible” way, security becomes critical for the dependability of all smart or intelligent systems built upon these embedded systems (Papp, Ma, & Buttyan, 2015).

Kocher et al (2004) studied design challenges in the embedded systems. Embedded systems, which are said to be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, security is often misconstrued by designers as the hardware or software implementation of specific cryptographic algorithms and security protocols. In reality, it is an entirely new metric that designers should consider throughout the design process, along with other metrics such as cost, performance, and power (Kocher, Lee, McGraw, Raghunathan, & Ravi, 2004).

The construction of security within the embedded system architecture is studied by Ravi *et al*. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are often highly resource constrained, while on the other hand, they frequently need to operate in physically insecure environments. Security has been the subject of intensive research in the context of general-purpose computing and communications systems. However, security is often misconstrued by embedded system designers as the addition of features, such as specific cryptographic algorithms and security protocols, to the system. 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 challenges unique to embedded systems require new approaches to security covering all aspects of embedded system design from architecture to implementation. Security processing, which refers to the computations that must be performed in a system for the purpose of security, can easily overwhelm the computational capabilities of processors in both low- and high-end embedded systems (Ravi, Raghunathan, Kocher, & Hattangady, 2004).

Apostolos et al (2017) have studied microarchitecture of embedded systems against cyber exploits. Cyber-Physical system devices nowadays constitute a mixture of Information Technology (IT) and Operational Technology (OT) systems that are meant to operate harmonically under a security critical framework. As security IT countermeasures are gradually been installed in many embedded system nodes, thus securing them from many well-known cyber-attacks there is a lurking danger that is still overlooked. Apart from the software vulnerabilities that typical malicious programs use, there are some very interesting hardware vulnerabilities that can be exploited in order to mount devastating software or hardware attacks (typically undetected by software countermeasures) capable of fully compromising any embedded system device. Real-time microarchitecture attacks such as the cache side-channel attacks are such case but also the newly discovered Rowhammer fault injection attack that can be mounted even remotely to gain full access to a device DRAM (Dynamic Random, Access Memory) (Fournaris, Fraile, & Koufopavlou, 2017).

2. Security Vulnerabilities on Internet-Enabled Embedded Systems

With the progress of technology every day, information processing and communication tools have started to show themselves more in everyday life. Though life has become easier thanks to their use, there is also an increase in the incidence of security vulnerabilities. We are now faced with a new wave of piracy that includes networked embedded systems, not just wired computers and networks, but also smart devices. It includes wireless phones, routers, switches, printers, and even medical devices. Security issues are not new to embedded systems. However, since more embedded systems are connected to the internet, the damage caused by such vulnerabilities has increased significantly. Internet connections increase the likelihood of attack. Unfortunately, security techniques developed for the desktop computer may not meet the embedded system requirements. With the spread of IOT and embedded information, network, data, hardware and software attacks are increasing. An attacker targets different purposes; the first type of attack is the removal of confidential information, and the second is trying to put the system in order (Ukil, 2011).2.1. *Vulnerability Analysis*

The most security vulnerability is found on network cards. For this reason, the most attacks are made via the network card. After the network card is running the programs and drivers that it manages, it enables the exchange of information through many communication protocols and application software. File and electronic mail exchanges, electronic messaging, remote desktop applications, all kinds of banking transactions are done through this door. All communication of the network card also flows in front of other computers on the network. Nearby attackers can track vulnerabilities in the communication, track and record information. It even communicates with us and secretly examines our device with a higher capacity computer.

Errors are also found in the network card driver and network communication software. A person who specializes in a network communication company knows these exploits and can share them with other people on the Internet. Later, collective attacks make network communication an insecure place. Wireless communication is more insecure than wired communication. In wireless communication, anyone who listens to us while we are broadcasting our close surroundings can record our broadcast. There are more security vulnerabilities in embedded systems. It is expected that embedded systems will have fast access to information, rapid processing and rapid transmission, while the amount of information processed is small. Because the resources are focused only on the services provided and on the acceleration of access to information, sufficient resources cannot be allocated for security measures. Therefore, they cannot have the security to prevent complex and different attacks like computers.

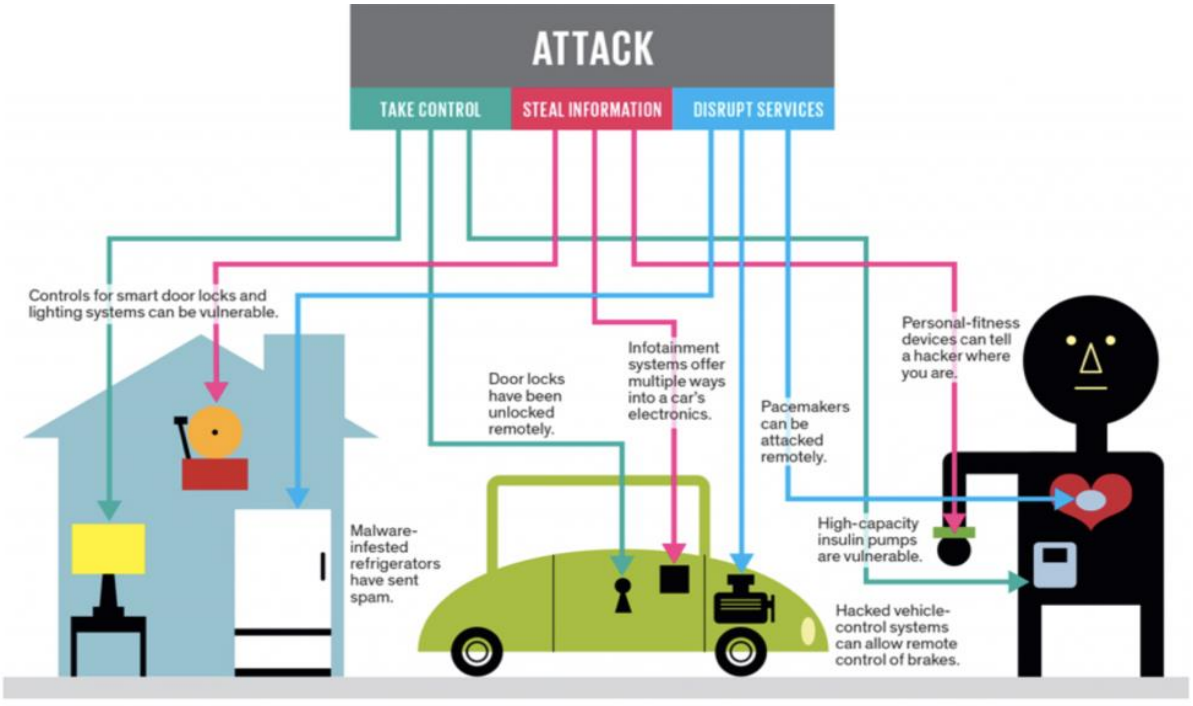
ATTACK
TAKE CONTROL
STEAL INFORMATION
DISRUPT SERVICES
Controls for smart door locks and lighting systems can be vulnerable.
Door locks have been unlocked remotely.
Infotainment systems offer multiple ways into a car's electronics.
Personal-fitness devices can tell a hacker where you are.
Pacemakers can be attacked remotely.
Malware-infested refrigerators have sent spam.
High-capacity insulin pumps are vulnerable.
Hacked vehicle-control systems can allow remote control of brakes.

Illustration: J. D. King

Figure 2. Demonstration of IoT attacks (https://cybersecuritytrends.ro/category/numarul-2/page/5/)

2.1.1. Weak User Information:

Manufacturers who are looking for extremely simple user interfaces can keep the Change Password setting that customers should use to change their incoming password by default. This reason explains why many users use default user information. Probably, if each IoT device had strong, predictable passwords, the above-mentioned Mirai event would not have occurred (Papp, Ma, & Buttyan, 2015).

2.1.2. Unregistered Firmware Updates:

Some IoT authors do not even publish updates or security patches for their device's software. If you have a security vulnerability and the manufacturer does not publish a patch, there is not much you can do to prevent attacks by malicious people.

2.1.3. Lack of Cryptography:

There are numerous IoT devices that do not use encryption to protect the data that they transfer with C2 (Command & Control) servers. This may result in the stealing of the user-defined personal data. Sometimes it is sent from the device from which the user uses the access information to the control server without plaintext, ie, explicit text. In this case, MITM attack will have bad results for the user.

2.1.4. Excessive Allowances:

Some IoT devices require more authority from the user than they normally need. For example, allowing users to shop independently may reduce your credit card's balance. As a result, more IoT devices have more permission.

2.1.5. Violations of Privacy:

IoT devices store a lot of information about the user. If a malicious person seizes one of your smart devices, he or she can access your personal data. Before you buy a device connected to the Internet, check how much information you have on it, and avoid using devices such as smart coffee machines that record your location information.

2.2. Analysis of Security Attacks

Attacks on information devices are generally divided into active and passive attacks. Passive attacks are the seizure of sensitive information by analyzing the vulnerabilities of computer communications. In the case of active attacks, the malicious user systematically implements different attack schemes including communication. While editing these attacks, he uses the information obtained by listening to the attacking system. Active attacks can also involve physical intervention. Most attacks focus around network communication vulnerabilities. The variety of attack types over the network is very high. Replay, reflection, masquerade, DoS, man-in-the-middle, parallel session and insider are some of the attack types. For example, a malicious user could try to access the host server by mimicking our device with his device at a time when our device is off, or it could block our ability to receive service by bombarding our ADSL device with queries. Higher levels of such attacks are attacks on industry bodies and medical devices. There are very serious security vulnerabilities in medical devices. Malicious people can play with human life by disabling medical devices. In recent years, the number of such attacks has increased steadily (Ravi, Raghunathan, Kocher, & Hattangady, 2004)

2.2.1. Using Vulnerabilities:

These vulnerabilities can be found in any software, and even international companies with large resources do not produce flawless code. Attackers can use these software vulnerabilities to deploy attacks. The most common methods used for this are (Fournaris, Fraile, & Koufopavlou, 2017):

Code Injection: This method explains the name itself. Attackers exploit vulnerabilities in the hardware of the software to inject the codes that the device will use to capture and capture the device.

Buffer Overflow: When a smart device tries to store unnecessary data in temporary storage, this redundant data can fill in and overwrite other memory space sections. If this data contains malicious software, it may affect all firmware.

XSS Vulnerabilities: This technique can be applied when a device communicates with a web-based interface. If there is a malicious code embedded in that webpage, it will probably reflect the effects of this malicious code on the connected device.

2.2.2. Malware (make it unusable):

Attacks on IoT devices are not limited to accessing user information, but these are the most commonly used attacks. Cybercrooks is an example of Malware attacks that are exposed to a serious and common problem with malicious software such as Ransomware as a growing trend.

Since most of these devices work on Android, malware written for Android will also work on these devices. This will simplify the job for malicious people. The most targeted IoT devices with this type of malware are smart televisions because they accidentally download applications that contain malicious links or traps (usually sexual content) prepared for the user.

2.3.1. Spoofing*:*

Attackers can try to camouflage their devices as another device used by a victim, and if the attacker can then access the wireless network, he or she will try to duplicate the router to use the scope of access. If this trick works, the fake device can be used to infect the network.

2.2.4. Password Attacks:

This attack method can be divided into brute force and dictionary attacks. The idea of both is to try to guess the login information of the target device by automatically entering many user name and password combinations. Unfortunately, several people use strong passwords, so these attacks are quite effective.

Ideally, the firmware should limit the number of unsuccessful login attempts. Unfortunately, it is a bad situation for all manufacturers not to equip their devices with this critical feature. In addition, it is both necessary and necessary for end-users not to use the default password and usernames.

2.2.5. Botnets:

It is quite difficult to think of a botnet device that has better potential than IoT devices. Malicious people know that these devices are easy to access, and they do not have a way to let their users know they are hacked. Therefore, IoT devices for use on the botnet network are very effective victims. If smart devices join a botnet network, your device can be used to provide access to certain sites or sites without Bitcoin Mining, DDoS attacks, spamming, and information.

ZED attack is the completion of the battery by sending a special signal to the end devices, including the sensors and the application devices, regularly. Keeping these devices in sleep mode when they are not exchanging data is kept active. If there is no message integrity, the ZigBee network is open to DoS attacks even if the transmitted messages are encrypted. An attacker, without knowing the secret key, generates an encrypted random content message and equals the frame of a picture to the maximum value sends this message to the device. The device analyzes this random message that does not make sense for the top protocol layer. In the meantime, the aggressive picture frame counter-frame counter- was able to reach the highest point - high-water mark- maximum (Yanzhen, 2016).

2.2.6. Remote Access:

If someone accesses one of your IoT devices remotely, it may not seem like a terrible thing, you might just think that it will be fun for yourself and not hurt me, but if your car is under the control of an attacker while driving your smart car on a highway, things may be threatening for you. In addition, imagine that the smart locks that you used in your homes were seized. In this case, the thieves can open the door easily and they can go inside and peel the meat.

2.2.7. Protocol Attacks with ZigBee

When we examine the communication protocols used for Internet of Things, IEEE 802.15.4 is a standard that has an important role in the emergence of these protocols. This standard was designed using point-to-point communication and star topology. In this topology there is a coordinating device at the center. The devices connect the coordinator with all other device-to-point communication. Messages are sent via the coordinator device. It is also an ideal standard for low speed and low power consumption environments.

ZigBee is a low-speed wireless personal area network protocol that complies with the IEEE 802.15.4 standard. ZigBee is based on a principle that targets minimal power consumption for low data usage. When there is no data exchange, the devices and the coordinator put themselves to sleep and no large size data is sent, resulting in low power consumption.

For security reasons, two algorithms are used: Advanced Encryption Standard -AES- and Message Control Code -MAC- AES algorithm uses symmetric key algorithm which is frequently used in encryption. That is, the receiver and the transmitter use the same key to encrypt or decrypt the message. This key should only exist in them. In the ZigBee protocol, AES is usually used with a 128-bit key (Charbel, 2016).

AES is based on a replacement - permutation network. The unencrypted message, which is considered to be 16 bytes instead of 128 bits, is encrypted using a certain mathematical formula with the help of a 4 × 4 matrix. Each cycle uses a different loop switch. When analyzing the message, the applied mathematical formulas are applied in reverse. Therefore, encryption and resolution algorithms must be separately coded.

MAC is an algorithm that provides cryptographic control over the information using session key, and detects conscious or unconscious changes in the sent message. The unencrypted message in the MAC is divided into blocks. And the output formed by encrypting a non-secret, random start vector -IV- with the first block and a key is used as the input to be encoded together with the second block. In encryption, the XOR process is used. This is called Block chaining mode. In the decryption process, the same key transactions are applied and the results are checked for the same. If the results are different, it is concluded that the message or MAC value is manipulated.

In addition to these algorithms, ZigBee supports extra security methods. Thus, three different kinds of key points are used to ensure inter-security: master -master-, link-link-, and network -network-switches.

In the process of discovering the network, ZigBee devices send a request to the control light through a channel. As a result, routers and coordinators which receive this request make some important information clear when responding. In this network discovery method, it is possible to install KillerBee software on an AVR RZ Raven USB and simulate it with the RZUSB software installed on the other AVR RZ Raven USB. With the RZUSB software, the package is injected with the KIlerBee software, while the deception is applied. A similar request is generated and important information is obtained about the coordinators and devices using KillerBee's zbstumbler tool. The attacker who captures a channel of the network is now ready to attack to capture packets sent.

Since ZigBee networks do not use encryption, it is possible to obtain network traffic and important information. With KillerBee's zbdumps tool, this traffic is obtained and saved. And so we can access the right to do the operations we want by manipulating the packets obtained in traffic with repetition attacks.

```
# Sudo zbstumpler
```

Apart from these, there is also the possibility of a physical attack on ZigBee. In order to prevent such attacks against ZigBee used in the security of important and critical locations, it should be placed in hard-to-reach places and applications that detect and prevent intrusions should be developed.

2.2.8. BEAST Attack

This attack, which is intended to capture the browser against SSL / TLS protocols, is the case when the message becomes open to the attacker because of an open implementation of the CBC algorithm. This attack is done using the MITM technique on the client-user side. The attacker injects different packages into TLS packages with MITM technique. The attacker predicts the IV-start vector by introducing the injected message into the XOR process. Compares the results of the block he wants to analyze and obtains the block. The attacker seizes the client's browser. This attack is usually applied on the TLS 1.0 version (Yanzhen, 2016).

2.2.9. CRIME Attack

This attack results from an open occurring in TLS data compression. One of the purposes of compression is to reduce the use of bandwidth. DEFLATE is one of the important algorithms used for compression. In compaction algorithms, it is the displacement and compression of repeating characters by pointing to where they were first seen with a marker. For example, the attacker wants to capture the description of the target person. The site on target is using adm as a description. If Cookie: adm = 0 injects the attacker's identifier for the target person's description, by compressing the server 0, the cookie: adm = returns to the target person and this is repeated. The attacker is doing his job by injecting different characters and checking the length of the response. If the length of the response is shorter than the first one sent, that is, the added character is a character of the value and is compressed. If the length of the answer is long, it is not a value of the character definition value. Thus, the target value of the targeted person is determined by brute force operation (Yanzhen, 2016).

3. The Protection Ways against Security Attacks

Embedded system designers should consider some basic steps, which can be thought of as methodology used to improve security, not rule.

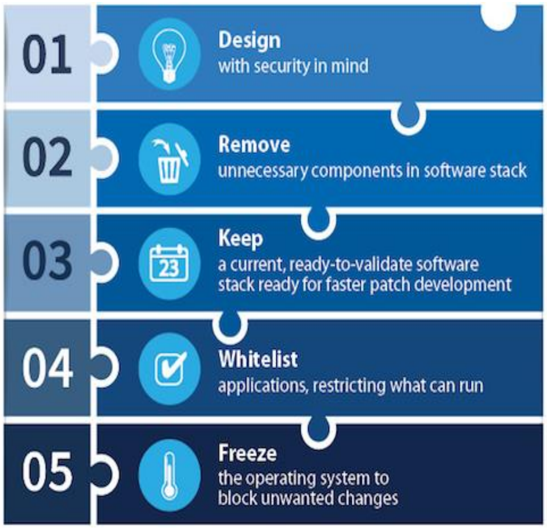
01
Design
with security in mind
02
Remove
unnecessary components in software stack
03
Keep
a current, ready-to-validate software stack ready for faster patch development
04
Whitelist
applications, restricting what can run
05
Freeze
the operating system to block unwanted changes

Figure 3. Basic Steps of Security Embedded Systems (Herger, 2016)

Firstly, threat assessment should be done. Taking into account the elements that can threaten the security of an embedded system is a fundamental step in closing the security vulnerability. All threats must be assessed, and development must begin afterwards. It is even easier to capture security vulnerabilities, especially in networked embedded systems; therefore, this step is very important. At this stage, life cycle analysis of the product should be done first. This analysis should include all steps such as developers, producers, operators, end consumers. Estimating the total number of users of the device to be developed is crucial for information and cyber security. The other analysis is to determine possible access paths for system attacks. Responses to questions such as the possibility of physically accessing the device via USB affect the system's discovery. Risk possibilities should be established. Estimating the likelihood of attacks from channels will help you to take precautions for channels that are more likely. A design that includes security must be defined. It is necessary to make the safety design part of the overall design by specifying the order of priority according to analyzes made.

The second step is to take advantage of existing safety designs. There are a number of technologies and designs available. Commercialized security designs are increasing day by day because advanced security standards are more important nowadays. It is important to take advantage of existing safety designs to reduce costs. Embedded systems are only small pieces that allow you to perform the given function and therefore are not very important to security, but in recent day's virtualization technology have gained popularity. It is a platform that allows multiple operating systems to run on a shared hardware. It is used to get more than hardware and provides flexibility in design. It allows separating the operations of a device into pieces of work in a virtual execution environment. Splitting the application is a useful technique for separating safety criteria. There are some virtualization platforms on the market, and taking advantage of proven security designs such as COTS software is a crucial step in a secure embedded system.

The next step is to determine the appropriate runtime platform. The selection of an appropriate runtime platform is an important aspect of the embedded system. Embedded virtualization is one of the options. Embedded system security can be improved by providing an embedded hypervisor enhanced partition diagrams and multiple operating system capabilities to provide additional system integrity. The other option is the use of real-time operating systems.

The other step is to secure the applications. Modern embedded systems do more than just work with a single working mode, such as that of traditional embedded devices. It usually has more than one function in it and the capabilities of these functions are upgraded with updates. Embedded systems must have secure capabilities to protect against malicious users or data breaches. There are many ways to improve the security of these devices. Whitelisting and Blacklisting are some of these methods. Since black lists are larger lists than white lists, and because they change more often, the capacity of the system may not be enough. For this reason, white lists are preferred (Stroud, 2013).

The last step is to adopt comprehensive life cycle support. The security planning of embedded devices has a significant impact on the lifecycle management of the device. It is also important to take quick action and respond as vulnerabilities arise. There are a few simple ways to do this. Security must be integrated at the end of the product life cycle. Your safety must be kept up to date and adapted to new changes. It is important that the safety design and testing be done accordingly. Safety should be seen as a high priority and should be acted accordingly.

4. A Risk Analysis of Embedded Systems over Huawei Challenge

Huawei is making some of the biggest waves in the wireless industry right now. It's the world's No. 1 telecom supplier and No. 2 phone manufacturer (Keane, 2019) using embedded design architecture. In 2019 a problem raised between USA and China over Huawei products. Beyond its trade and economic aspects there are certain risks and threats that USA take into consideration due to its embedded designs that pose economic, military and governmental concerns.

So far, the US and Australia have banned Huawei from providing equipment for their 5G networks, while Canada’s relationship with the firm is under review. There is also concern among European telecoms network operators, with some considering removing Huawei’s equipment. BT, for example, has removed Huawei equipment from key parts of its 4G network (O'Flaherty, 2019).

The US executive order calls out two threats regarding the embedded designs of Huawei products (Austin, 2019):

- “Risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance” of information and communications technology (ICT) equipment and services in the United States
- “Undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States”.

What are the underlying causes of this problem? Why is Huawei, the Chinese technology giant, disturbing Western countries, especially the United States?

As is known, the United States officially sees Huawei as a security threat. Huawei continues to work for the 5G technology that has just begun to enter our lives, causing America to be uncomfortable about it. In fact, the United States is calling on its allies to keep Huawei out of 5G tenders and is putting pressure on its allies.

The company openly rejects claim that it the Chinese government has collected data using

Huawei.

The fact that the United States and other Western countries wage the war against Huawei has 5 different reasons. If we take a closer look at these reasons:

4.1. Information Collection

All the data that are passed through or analyzed by these embedded structures is potentially vulnerable to the manufacturer.

4.2. Intelligence Laws

In 2017, a law was passed in China. Under this law, Chinese citizens and companies are obliged to support the country's intelligence efforts and to assist where necessary. Although this law was defended by China, Western countries did not like it in any way. Under this law, Huawei lost confidence in the foreign market and could not do anything to secure that trust against both states and customers.

4.3. Back Doors

According to US claims, Huawei is capable of using base stations in Montana as a weapon and controlling a ballistic missile at the air base in the region. And the company will do it using 'back doors'. This claim is completely unfounded and is a 'nonsense' by statements from the Chinese front.

As long as conflict occurs at the nation-state level while critical cyber networks are designed and manufactured internationally, we all must be very careful considering the Turkish Government's strategy on the local and national product development. Currently, Huawei's size and ties to the Chinese government make it the focus of concern. In the future, another supply chain threat will take center stage.

5. Conclusion

Embedded systems are only used to realize the intended purpose of desired functionality of devices. Normally, no qualifications or functionalities are being added to these systems except for their own purposes. This situation is open afterwards and is difficult for interventions in case of problems. In order to intervene with the embedded systems for maintenance and aftersales service delivery, the producers have brought these systems into the form of internet connected systems. Therefore, embedded systems connected to the internet have both advantages and disadvantages. The most important advantage is that if there is a problem, it can be intercepted from the outside to provide solution effectively. However, it also introduces security concerns against internet-connected applications. It is difficult to capture and attack security weaknesses in embedded systems without an internet connection, but it is difficult to control it if an attacker can accomplish this using innovative tools and techniques that are being developed day by day.

The most important task that needs to be done before developing embedded systems with internet connectivity is to analyze this system well. Anticipating the channels where security attacks can be done and making the design accordingly will make the system more secure. Another problem with embedded systems is cost issues. It is preferable to implement security standards to reduce the cost of embedded systems. However, while implementing existing security standards to cover security vulnerabilities, it is not too costly in terms of potential dangers.

As a result of the research from standards and literature, it is possible to say that the characteristics of a secure embedded system should comprise the following provisions:

- Unauthorized Security Management that puts the management functions, management roles, and necessary authentication mechanisms in place.

- Protecting the authentication reference data of the authentication mechanisms and objectives.

- Security Management addressing the threats.

- Logical Data Access that protects the user data from unauthorized access accordingly to the rules defined by the application.

- Data Access Control that protects the data stored and processed on the embedded system from physical probing;

- Confidentiality Protection that protects the confidentiality of the transferred data between internals of the IoT; and so it covers the threat.

- Data Integrity controls that protects the integrity of the data stored and processed on the embedded system from physical manipulation.

- Data Access Control that protects against reading the data prevents the attacker knowing the physical location and content of the data.

Therefore the possible measurements against attacks of embedded systems over internet can be takes as such:

1. Reinforce and protect your Microsoft Windows-based embedded devices and computers with a solution designed to optimize security for low-tech systems with limited memory that do not require ongoing maintenance or Internet connectivity.
2. Set up device policies that enable administrators to perform certain security policies, such as multifactor security levels or locking methods. It also provides the ability to lock content on the device, protect company privacy, e-mails and files when needed. Two-step authentication is the only proven way to make user login secure.

3. Most of the time, small and medium-sized businesses have the highest level of security, while almost all SaaS solutions do not have the resources to invest in a powerful security system. If possible, it is recommended that medium-sized companies use SaaS (software as a service) solutions rather than their own software.
4. Integrating existing security systems or creating a new security structure using direct integrated security systems increases network visibility for security professionals and helps to monitor potential attack risks on a larger surface.
5. Using security-embedded applications for enterprise operations, or incorporating powerful security features

embedded in an enterprise-specific application, enhances security.

6. Some employees may not be convinced about the importance of data security, or do not have the necessary capabilities to comply with the necessary cyber security measures, they may face serious security risks. For this reason, regular training to both IT security personnel and all employees connected to the enterprise network on a regular basis minimizes the possibility that business data will become vulnerable to attacks due to ignorance and / or carelessness.

7. Regular penetration tests by IT staff enable the identification of potential safety weaknesses and provide valuable opportunities for enterprises to take more advanced safety measures.

8. The sharing of information about identified or actual risks across the enterprise ensures that all employees are more conscious in the future if they encounter a similar threat in the future.

6. References

Austin, G. (2019, May 16). *US ban on Huawei likely following Trump cybersecurity crackdown – and Australia is on board*. Retrieved from Theconversation: http://theconversation.com/us-ban-on-huawei-likely-following-trump-cybersecurity-crackdown-and-australia-is-on-board-117250

Aydın, H. (2016, January 24). *GÖMÜLÜ SİSTEMLER(EMBEDDED SYSTEM)*. Retrieved from https://yazilimdnyasi.wordpress.com/2016/01/24/gomulu-sistemler/

Dickie, J. (2003, March 31). *The How And Why Behind Internet-Enabled Embedded Systems*. Retrieved from Electronic Design: http://www.electronicdesign.com/embedded/how-and-why-behind-internet-enabled-embedded-systems

Fournaris, A. P., Fraile, L. P., & Koufopavlou, O. (2017). Exploiting Hardware Vulnerabilities to Attack Embedded System Devices: a Survey of Potent Microarchitectural Attacks. *Electronics, 6(3), 52; https://doi.org/10.3390/electronics6030052*.

Herger, A. (2016, February 4). *Embedded Systems Engineering*. Retrieved from Designing with Embedded Security in Mind: Starting Early and at the Edge: http://eecatalog.com/IoT/2016/02/04/designing-with-embedded-security-in-mind-starting-early-and-at-the-edge/

Karataş, G. (2016). Mobil Cihazlarda Güvenlik-Tehditler ve Temel Stratejiler. *Istanbul Commerce University Journal of Science*, 55-75.

Keane, S. (2019, Seb 3). *Huawei ban: Full timeline, plus Huawei accuses US of cyberattacks to disrupt business*. Retrieved from CNET: https://www.cnet.com/news/huawei-ban-full-timeline-accuses-us-cyberattacks-threats-fbi-disrupt-business/

Kocher, P., Lee, R., McGraw, G., Raghunathan, A., & Ravi, S. (2004). Security as a new dimension in embedded system design. *ACM DL, doi>10.1145/996566.996771*, 753-760.

Michael Vai, D. J. (2016). Secure Embedded Systems. *Lincoln Laboratory Journal* , 110-122.

O'Flaherty, K. (2019, Feb 26). *Huawei Security Scandal: Everything You Need to Know*. Retrieved from Forbes: https://www.forbes.com/sites/kateoflahertyuk/2019/02/26/huawei-security-scandal-everything-you-need-to-know/#3e1c09aa73a5

Özcanhan, H. (2011). Gömülü Sistem Uygulamalarına Yapılan Saldırılar ve Ağ Bağlantılı Gömülü Sistemlerin Sağlanması. *Elektrik-Elektronik ve Bilgisayar Sempozyumu*.

Papp, D., Ma, Z., & Buttyan, L. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. *IEEE, DOI: 10.1109/PST.2015.7232966*.

Ravi, S., Raghunathan, A., Kocher, P., & Hattangady, S. (2004). Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems (TECS), doi>10.1145/1015047.1015049*, 461-491 .

Ukil, A. (2011). Embedded Security for Internet of Things. *2nd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS).* Shillong, INDIA.

Stroud, R.“The Convenience/Privacy Trade-off on the Internet of Things, "Wired Innovation Insights Blog, 17 Aralık 2013, http://insights.wired.com/profiles/blogs/the-convenience-privacy-trade-off-on-the-internet-of-things?xg_source=activity#axzz3MNq2UmCe

Charbel, A., (2016). “Vulnerability Analysis and Security Framework for Zigbee Communication in IOT”. Las Vegas: Nevada Üniversity.

Yanzhen, Q., Chan, P. (2016) “Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network Based IoT Systems”. New York: IEEE.