Chapter 7: Environmental Threats to the Applications in Embedded Systems

The previous chapter discussed how applications can be empowered to safeguard themselves against prying eyes and hackers looking to exploit security loopholes. While last chapter was targeted at securing the application architecture to safeguard the applications and the user, this chapter presents various other threats that can compromise the environment in which the applications run and user interacts with them.

7.1 Known Security Exposures of Mobile Devices

7.1.1 Malware

A malware is really a program that performs unexpected or unauthorized, but always malicious actions. It's a general term used to consult viruses, Trojans, zombies, logic bombs, trap doors and worms. These threats are usually split up into two classes: people who demand a host program and which have been independent. The first sorts are fragments that cannot exist independently of some actual application program, utility or system program. The second are self-contained programs which can be scheduled and run from the operating system.

Malware, according to the type, occasionally includes replicating and non-replicating malicious code. Although some people might payloads can display messages or images, many may be destructive - they can destroy files, reformat the hard drive, cause trouble by consuming storage space and memory or reduce speed on the operating system.

7.1.2 Viruses

A virus is usually a program or part of code that is loaded onto laptop/desktop or mobile devoid of the user’s knowledge throughout the internet or another system.
disks. Virus can infect other programs by modifying them. A virus carries rolling around in its instructional code the recipe to create perfect copies of it. Lodged within a host, the typical virus takes temporary management of the operating system. Then when an infected machine is confronted with an uninfected software application, a fresh copy from the virus passes to the new program. Thus, the infection might be spread from one device to other by unsuspecting users who either swap disks or send programs to each other on the network.

A virus is capable of doing whatever other programs do. The sole difference is who's attaches itself to a different program and executes secretly in the event the host program is running. Once a virus is executed, it could possibly perform any function, like erasing files and programs. The important thing to its operation is usually that the infected program, when invoked, will first execute the virus code and execute the initial code of the program.

### 7.1.3 Worms

A worm is a program that spreads copies of itself through a network. The primary distinction between the virus and a worm is the fact a worm program use network connections to spread from system to system, plus a virus can spread through any medium, but usually uses copied program or documents. A worm doesn't need a host as well as doesn't should attach itself to another program. With the ability to send copies of itself being a stand-alone program to machines on the network, whereas the virus spreads copies of itself being a program that attaches to or embeds in other programs.

Once active inside a system, a network worm can behave as working virus or bacteria, or it might implant Trojan programs or perform many disruptive or destructive actions.

To replicate itself, a network worm uses some form of network vehicle: by employing e-mails, network program and creating of the company's own server sockets, by cracking the passwords and signing in as a regular user using a remote machine, or by using of the back doors of an operating system.
7.1.4 Trojan Horses

A Trojan is really a malware packaged that has a useful program, usually free for download, for example a screen saver or a game, but carries viruses, or destructive instructions, that perpetrate mischief invisible for users. Trojan program hidden in the primary program runs secretly commands, which steal passwords, some private data, play sounds, videos or display images, shutdown the device randomly, scan e-mail addresses and use them for spam, get a back door on a pc system. Unlike viruses and worms, Trojan horses do not possess replication abilities.

7.1.5 Spyware

Spyware is misleading software that's secretly attached to your an application over the web - it usually is attached with free programs that user downloads, its sole purpose is to gather data from the device and forward it to some location devoid of the consent or expertise in the pc’s owner. This includes monitoring key strokes, collecting confidential information (passwords, plastic card numbers, PIN numbers, etc.), harvesting e-mail addresses or tracking browsing habits. Spyware is just like Trojans. However, malicious functions are executed by Trojans are hidden and also by spyware these destructive functions unlike Trojans are known in the application description. Too much spyware can reduce the operation speed of any machine.

7.1.6 Hoax

A hoax can be a fake warning with regards to a virus or other part of malicious code. Typically, a hoax takes the type of an e-mail message warning the reader of your dangerous new virus and suggesting how the reader passes on the content to everyone they are fully aware or at least to numerous other people. This forwarded email can decrease or even stop a mail server, fill peoples' mailboxes and, certainly, frighten them and make them lose time on something, and that is just a hoax. Hoaxes cause no damage by themselves, but their distribution by well-meaning users often causes fear and uncertainty. Most anti-virus vendors include hoax home their internet websites and it's also always advisable to check before forwarding warning messages.
7.2 Wireless Attacks on Mobile Phones

7.2.1 Bluetooth Attacks

To guard systems better, it really is needed to have a greater perception of security attacks hence let us discuss current Bluetooth and WLAN attacks on mobile phones. With proper tools and time, all encryptions can be broken and all sorts of privacy with the network can be lost. Although some other techniques enable hacker to compromise physically the integrity of a wireless network, it concentrates on some of the known non-physical security vulnerabilities in wireless compliant networks. Security attacks affect every of data systems: people, networks, and programs. Risks of wireless networks get addition to classical risks of wired networks new risks introduced by vulnerabilities of wireless protocols.

Attacks around the security of information systems have grown to be a regular occurrence. Attacks have gotten more complex as you move the knowledge required to execute such attacks has decreased. Attacks are directed against all the different parts of a system including people, networks, and applications. Attackers hunt for the weakest links in each component. To guard systems better, it’s must have a much better understanding of security attacks.

7.2.2 BlueSnarfing: (Sniffing)

The BlueSnarf attack can be an OBEX protocol (OBject EXchange communications protocol which allows the exchange of binary objects between devices) which allows hackers gain access to the mobile phone’s calendar, pictures, phone book secretly, however even changing a pin code without owner’s knowledge may be possible. While using OBEXAPP application it is possible to generate a reference to a target phone
7.2.3 BlueJacking

This trick was discovered through flirting habits of Bluetooth phones owners. It uses the likelihood to switch the phone completely to another name as well as to send a profitable business card (vCard). After renaming the naming of his phone, the hacker can force the victim to simply accept the Bluetooth connection. Usually, the specific phone would be the name on the manufacturer and mobile type. When the hacker changes the phone’s name towards the string “get more information at free cash”, the victim will usually click the pop-up frame mistakenly and accept the call. This permits the hacker to get in touch to the device. BlueJacking can be employed by hackers to infect phones, to exhibit obscene movies, etc.

7.3 WLAN Attacks

7.3.1 Rogue Access Points: (Man in the Center Attack)

Wireless access points (WAP) are super easy to install, however many employees install access points into their companies, without informing the network administrator for making their work easier. Usually the reference to these access points is not protected by password or encryption. An attacker can easy gain access to the organization network through such access point. Otherwise an assailant can purchase a so-called rogue access point that pretends becoming a corporate access point, but usually it really is at bay with the attacker. In the event the attacker can install an access point which has a stronger signal than the valid one, the perspective’s mobile device automatically connects on the attackers AP. Then this attacker is able to see each of the traffic that goes through this AP. This attack is difficult to avoid, because many wireless systems automatically fix the text without asking the user.

7.3.2 Wireless Zero Configuration

Each time a device connects a wireless access point, it generally stores the details of that connection locally. So when the mobile phone is started up, the wireless network
card immediately searches for the call and re-establishes the text without asking the user.

To find the last used AP, the wireless network card sends a request while using Service Set Identifier (SSID) in the desired access point. The AP sees this packet and sends back a remedy. Because SSID is sent like a plain text, anyone with a sniffer can see it. An assailant can configure an AP with the same SSID. This AP will likely then answer as an original access point. Some programs can automatically establish a reference to a wireless user, and control you their web connection, email and much more.

7.3.3 War Driving

The process of seeking open wireless LANs by driving around a unique area is referred to as War Driving. The name derives from the idea of “war dialing”, and that is an existing attack method that requires repeatedly dialing different numbers to search for modems as well as other network places. The war driver only needs a Notebook which has a wireless network card and a few free software from the net. Using a GPS System (GPS) receiver will be able to develop a map of open wireless networks of the city by driving across streets. Simple War driving uses information that's offered by the system like software name, version, network address, Service Set Identifier (SSID), Network name, equipment manufacturer and whether encryption is needed.

7.3.4 Securing the Network and Operating Systems

The most beneficial defense against network attacks is always to update the system while using the latest patches. Good network security applications are also important. These applications include intrusion detection system (IDS), firewalls and antivirus programs.

The wireless network must be checked for known vulnerabilities. Security functions like access controls and checks for rogue access points need to be implemented inside the network. Static IP addresses (not Dynamic Host Configuration Protocol “DHCP”) in small networks ought to be used. Ethernet MAC Access Control Lists (ACLs) to
avoid access of foreign clients should be also implemented. Service set identifier (SSID) broadcast by access points should be disabled plus the SSID ought to be changed through the factory default settings. Automatically, when wireless access points are delivered, their security functions are switched off. This means that an attacker can easily hook up to the access point and configure the router because he wants. The URL of your website System (DNS) server name could be changed with an IP which is owned by the attacker so that all requests to websites will result in attacker’s page where he can steal passwords. Uploading a hacked firmware version for the router could put the attacker completely control of the results. He can install undetected sniffing programs around the router.

Moreover, they work extremely well by attackers to launch virus or spam attacks. The operating system ought to be secured too. Just about the most serious security flaws in programs is usually a buffer overflow. The software industry knows about this vulnerability for over three decades, but it really still exists.

A buffer overflow in operating memory is due to incorrect memory usage when developer writes their programs with languages without built-in memory management. Overflowing a buffer often ends up with a program crash. However, a carefully constructed exploit might run a program from the attacker or crash the complete operating system. One treatment for prevent this issue is by using languages that do better memory management. Languages for example Java and C# give you a safe alternative to popular C and C++.

7.4 Antivirus Programs

Antivirus software detects and protects the smartphones from some of the viruses, worms, Trojan programs, and backdoors, as well as blended threats, which combine issues with different threats. Some antivirus programs may also assist to block well-known joke or hoax e-mail messages, spyware programs and program exploits. To secure mobile devices, the leading antivirus software manufacturers like avast, F-Secure or Kaspersky offer solutions for the most mobile operating systems.

Most antivirus software includes three basic sorts of scanning: real-time, manual, and heuristic. Real-time scanning may be the main line of defense. This can be the scanning, which is done about the fly as you move the device is utilized. The manual
scan is a scan run to confirm the files which might be already around the mobile tool. These scans might be initiated by user if something suspicious seems to be occurring; however they also need to be run periodically to ensure that no malware got at night real-time scanners. It is additionally feasible that an infected file is likely to make its way onto the mobile OS prior to the antivirus software vendor updated their software to detect it. The third way of detection a part of most antivirus software program is called heuristic detection.

The standard malware scanning relies upon signatures or pattern files employed to identify known threats. However, until a threat is discovered and researchers identify its traits that they use to detect it, the conventional malware scanning won't detect the brand new threat. Heuristic detection won't seek out specific malware threats. Heuristic detection uses general characteristics of typical malware to recognize suspicious network traffic or e-mail behavior. Based on known traits from past threats, heuristic detection attempts to detect similar traits to identify possible threats.

7.5 Firewalls

Firewalls are widely-used to be able to protect networks externally attacks. Typically, firewalls are available in three categories: static packet filters, state full packet filters and application level gateways. Static packet filters have static rules that describe which packets are granted or denied. They filter each packet based only on information in the packet itself (in most cases mix of the packet's source and destination address, its protocol, and also the port number). State full packet filters utilize the information regarding the session state and determined by these records packets could be granted or denied access. Such a type of firewalls can detect as an example packets that begin a new connection and reject them.

Application layer gateways will be the most complex firewalls and can analyze the packets around the application form layer. They will understand protocols (including FTP, Domain Service, or web browsing) and in addition they can detect whether a non-standard port is utilized or whether a protocol will be employed to send prohibited data.
Nowadays, really the only known firewall for mobile devices included mobile phones is offered by the antivirus specialist avast, f-secure. The firewall scans the WLAN traffic for unwanted or dangerous packets.

This chapter enumerated the hostile environment and security measures that can be adopted by the user to safeguard his privacy and threats to his applications. An application is only as safe as the environment in which it exists, a very weak application in terms of security can do very well if the environment and user in which it runs are safe, while the safest of application architectures can be compromised when the user gives unintentional permission to malware like adware and Trojans to run on his machine. Hence this chapter was worthwhile a discussion because no matter what the programmer does, an app has to ultimately run in the user’s machine with his knowledge of environment threats and protection.