7.7.3 Embedded Systems Security Facts

In today's world, more and more devices are becoming connected to the world wide web through embedded technology that allows the device to send or receive information via the network or internet. Internet-connected devices are known as smart devices. These devices are part of a growing ecosystem known as the *Internet of Things* (IoT). Environments that contain these types of devices are known as static environments. A *static environment* is one that never changes (or changes very infrequently) and that a network administrator has very little control over. For example, a smart television in an office has embedded technology that might never be updated, which creates a security hole in the company's network.

The following table describes some of the most common static environment categories:

Category	Description
Home Appliances	Many modern home appliances contain integrated technology that allows internet communication. For example, smart laundry appliances are able to send notifications when a load is complete or when laundry detergent needs to be refilled. Other common smart home appliances include the following: - Refrigerators - Dishwashers - Microwaves The first documented Internet of Things (IoT) attack was a phishing email scam that occurred in late 2013. Roughly 25% of the emails originated from smart appliances, including one smart refrigerator. The attackers were able to compromise the appliances because their static environment was easily exploited. This attack coined the term *thingbot*, which is an IoT device that has been compromised by a hacker.
Environment Controls	Many homes and businesses use environmental control devices that are capable of sending real-time information and can be controlled via the internet. These devices can be as basic as controlling a home's HVAC system (a Nest thermostat) or as complex as controlling the humidity, temperature, and other environmental factors in a data center.
Home Automation	Instead of having just a few smart devices, some homes use a network of integrated devices that control various aspects of the home, creating what is known as a smart home. Some of the devices that are integrated with a smart home include the following: - Lighting controls - Security systems - Door locks - Sprinkler systems - Garage doors
Wearable Devices	In recent years, companies have started producing wearable devices that can connect to the internet for a variety of purposes. These devices include: - Watches - Headphones - Fitness Trackers
Media Appliances	Most new media appliances are essentially small computers, complete with a proprietary operating system. These devices are capable of browsing the internet, streaming videos, and making online purchases. Even home routers are capable of more than just routing and can function as a media server or file server. The following are some of the more common smart media appliances: - Smart televisions - Media players (Blu-ray players) - Printers - Game consoles - Home routers
Automobiles	Modern cars use integrated technologies and in-vehicle systems that can perform various tasks, such as: - Starting the car remotely from smart phone - Warning a driver about nearby cars - Automatically applying the brakes to avoid collision - Performing parallel parking autonomously
Industrial Equipment	Even some industrial equipment fits into the category of a smart device. *Supervisory control and data acquisition (SCADA)* devices are special computer systems that are used to gather, analyze, and manage automated factory equipment. For example, a SCADA system could be used to monitor factory pipes and automatically open vents if pressure in the pipe reaches a specific threshold. SCADA is a subset of *Industrial Control Systems (ICS)*, which refers to all types of industrial automation.

Mainframe Computer	A lesser known category of static environments are *mainframe* computers. A mainframe computer is a large, very powerful computer that is capable of processing extremely large amounts of data. Mainframe computers typically run proprietary operating systems. Because these operating systems are rarely updated, they are considered to be a static environment. In addition, mainframe computers often contain large amounts of sensitive data, making them an attractive target to hackers.
Real-Time Operating System (RTOS)	An *RTOS* is an operating system that serves real-time applications without buffer delays. They are generally used in systems that require a response within a strict time constraint. Because RTOS are often used as critical components of an application, a successful attack on the RTOS can do harm to an entire system, including physical machinery.
System on a Chip (SoC)	An *SoC* is an integrated circuit that includes all components of a typical computer system, including digital, analog, mixed-signal, and radio frequency functions. The Raspberry Pi is a common device that uses an SoC. Because of their relatively low cost, SoCs are often used by hobbyists.
Multi-Function Display (MFD)	An *MFD* is a screen surrounded by configurable buttons that can be used to display information in a variety of ways. MFDs are often used on airplanes, helicopters, and ships.
Medical Devices	Much of today's medical technology for daily monitoring and maintenance utilizes embedded systems. Instead of having to visit a physician every day, wearable devices can be used to collect information on heart rate, glucose levels, weight, blood pressure, and several other parameters. This information can then be sent to a doctor automatically or used for self-monitoring.
Unmanned Aerial Vehicles (UAV)	*UAVs* are used for military campaigns, search and rescue, weather monitoring, and recreation. UAVs use embedded computers for collecting and transmitting data and for receiving commands.
Digital Cameras	Most modern digital cameras utilize embedded systems for processing captured images, storing images, and uploading images to a PC or other storage device.
Media Gateways	A media gateway is a translation device that converts media streams so they can be sent network packets using transport protocols.
Wireless Keyboards and Mice	Wireless keyboards and mice use bluetooth or other proprietary radio frequency connections.
Displays	In the past, display devices had a single use as a monitor for a computer. Today's monitors and other display devices are increasingly embedded with smart features and have wireless connections.
Wi-Fi-Enabled MicroSD Cards	Wi-Fi-enabled MicroSD cards can wirelessly transfer their data to and from other devices. Many of them are able to connect directly to the internet.
Printers/MFDs	Printers and other multi function devices (MFDs) are increasingly able to connect to wireless networks and to the Internet for additional functionality.
External Storage Devices	External storage devices such as USB flash drives, HDDs and SSDs can connect to traditional computing equipment as well as to many smart devices.

As with any networked system, there are security risks associated with smart devices. Not only do you have little or no control over the smart technology within static environments, smart device vendors can be slow to take steps to protect their products against security threats. They tend to respond only after an exploit has occurred instead of proactively updating systems. This is why smart devices are attractive to hackers. However, there are some steps you can take to secure a network from these devices and reduce the damage that a compromised device can cause.

- Some static devices (such as home routers, game consoles, and SCADA devices) can have their firmware manually updated. With these devices, it is important to always keep their firmware constantly up to date.
- For devices that cannot be manually updated, the best approach is to minimize the amount of damage a compromised device can cause. This is done by segmenting the network using VLANs or encrypting all network communications.