7.4.3 Internet of Things Facts

IoT evolved from machine-to-machine (M2M) communication. It is a sensor network of several smart devices that connect people, systems, and other applications to collect and share data.

This lesson covers the following topics:

- IoT overview
- IoT security
- IoT devices
- Protocols

IoT Overview

The internet of things is a natural extension of SCADA (supervisory control and data acquisition), the gathering of data in real time from remote locations to control equipment and conditions. The evolution of SCADA is such that late-generation SCADA systems developed into first-generation IoT systems. An IoT ecosystem is made of web-enabled smart devices that use embedded processors, sensors, and communication hardware to collect, send, and act on data they gather from their environments.

IoT devices share the data they gather by connecting to an IoT gateway or other edge device where data is sent to the cloud to be analyzed. In certain instances, these devices can communicate with other related devices and act on the information they get from one another. The devices do most of the work without human interaction. The only times humans would need to communicate with such devices would be to do such things as setting them up, giving them instructions, access their data, and so on. The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

IoT Security

The IoT involves billions of data points through all of the devices connected to it. Because of that, security and privacy are major issues that need to be tackled. Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. Manufacturers who don't update their devices regularly—or at all—leave them vulnerable to cybercriminals.

One of the most notorious recent IoT attacks was Mirai, a botnet that infiltrated domain name server provider Dyn and took down many websites for an extended period of time in one of the biggest distributed denial-of-service (DDoS) attacks ever seen. Attackers gained access to the network by exploiting poorly secured IoT devices.

However, hackers aren't the only threat to the IoT; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data. Beyond leaking personal data, IoT poses a risk to critical infrastructure, including electricity, transportation and financial services.

IoT Devices

Device	Description
Thermostat	Smart thermostats learn from your habits and schedule, give you the freedom to control the climate in your home remotely, show you energy consumption in real-time, and can even adjust themselves depending on ambient conditions like humidity.
Switch	A smart switch is a device that allows you to control hardwired lights, ceiling fans, certain fireplaces, small appliances, and even the garbage disposal with an app on your phone or with your voice using a virtual assistant. Smart switches give smart home features to anything you turn on or off with the flip of a switch.
Bulb	Smart bulbs normally work with conventional lighting fixtures and bulb holders. That makes them easy to implement. They also come with wireless communication capabilities packed inside. Some of them use built-in Wi-Fi or Bluetooth which lets them communicate directly with your phone or tablet, eliminating the need for a hub or control device. There are even some higher-end bulbs that change colors, track motion, stream audio over Bluetooth, or double as connected cameras. On a small scale, that kind of plug-and-play simplicity is very convenient, but smart bulbs tend to be expensive so scaling up could be difficult depending on your budget. Also, smart bulbs won't work if the light is switched off; they’re only smart when they’re turned on.
Plug	Smart plugs automate anything with a plug on it. You can remotely turn on and off anything that’s plugged into them using an app. They are an easy solution to making small appliances such as lamps, coffee makers, and toasters smart.
Security Camera	Wireless cameras transmit video through a RF transmitter. The video is sent to a receiver that connects to the viewing and recording device. That device gives easy access to all video footage recorded through the cameras. Many people use cloud storage to save the video footage for later viewing. Modern wireless camera technology tends to implement such features as motion detection, scheduled recording, remote viewing, and automatic cloud storage. But the extent to which these features are implemented may vary by company, model, and brand.

Door Lock	A smart lock is an electromechanical lock that can be locked and unlocked using a smart phone. It uses a wireless protocol and a cryptographic key to execute the authorization process. It can also monitor access and send alerts related to the status of the device.
Speaker/Digital Assistant	Smart speakers/digital assistants work in the following way: ▪ Smart speakers use voice recognition software. Once they're on, smart speakers listen to all speech, waiting for what is known as a 'wake word' or 'hot word'. When they recognize this word, they begin to record your speech and send it over the internet. The speech file is sent to a voice recognition service in the cloud. The voice recognition service deciphers the speech and sends a response back to the smart speaker. ▪ The voice recognition service uses algorithms to familiarize itself with your way of speaking and choice of words. You can also send feedback to the voice recognition service about the accuracy of the responses that the smart speaker provides. When first setting up a smart speaker you are required to do a 'voice training' in which you read 20 to 30 key commands to your device and the voice recognition service starts to learn your speech patterns. ▪ Machines' ability to recognize speech is a complex process, especially when considering the huge variety of different speech patterns. But the simplified explanation of the process is recognizing sections of words known as 'phones'. Those phones build into 'phonemes' which can then be recognized as individual words.

Protocols

Protocol	Description
Zigbee	Zigbee is a standards-based wireless technology that enables wireless machine-to-machine (M2M) and IoT networks. It is designed for low-data rate, low-power applications, and is an open standard. Zigbee is a specification based on IEEE 802.15.4 and the WPANs operate on 2.4 GHz, 900 MHz and 868 MHz frequencies. Its networks are secured by 128-bit symmetric encryption keys. Zigbee has a defined rate of 250 kbps, best suited for intermittent data transmissions from a sensor or input device.
Z-Wave	Z-Waves work in the following way: ▪ Z-Wave was created by a Danish company named Zensys. It is a simpler and less expensive alternative to Zigbee. It uses the same AES-128 symmetric encryption as Zigbee. But, unlike Zigbee that operates on 2.4GHz, which is a major frequency for Wi-Fi, Z-Wave operates on the 800-900 MHz radio frequency range, so it doesn't suffer any major interference issues like Zigbee does. ▪ Like Zigbee, Z-Wave devices all link up together to form a mesh network. There's one central hub that connects to the internet and then the devices themselves don't have Wi-Fi at all, they use Z-Wave connectivity to talk to the hub either directly or through the mesh network. This is called a "source-routed mesh network topology." Z-Wave allows up to 232 nodes on the mesh network.