Evan Wilcox

Professor Joe Stanley

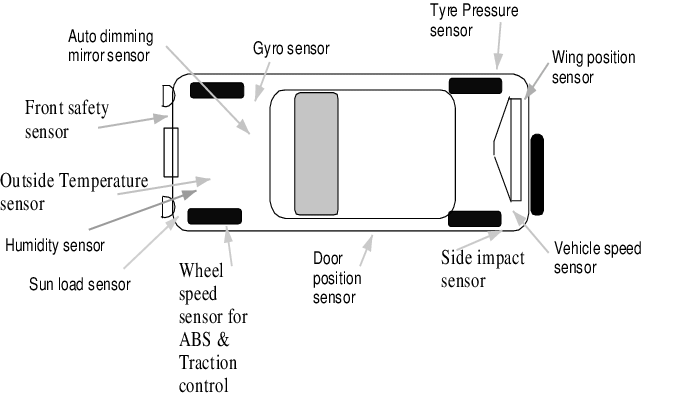
Computer Engineering 3150

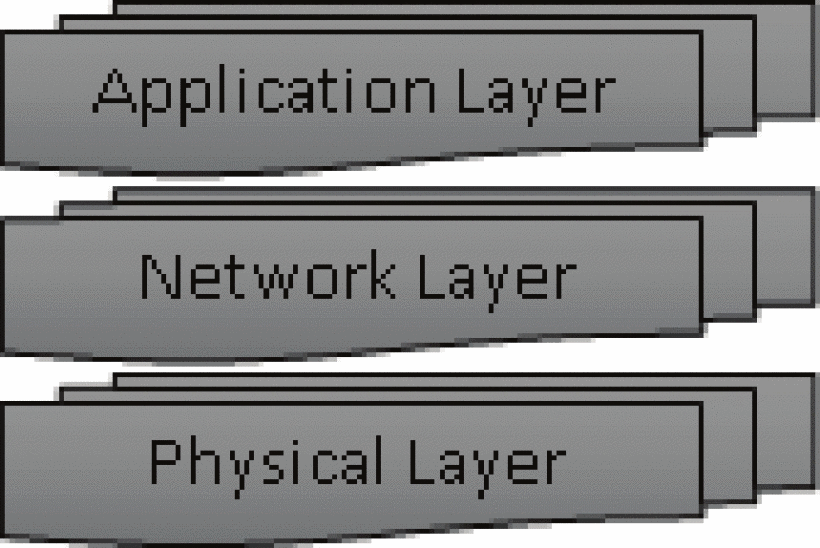
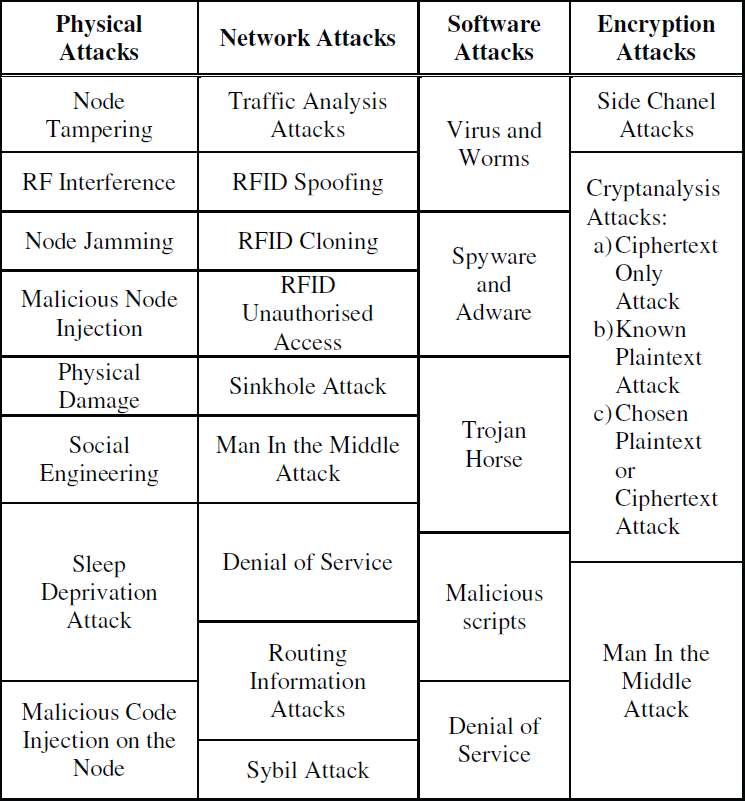
11/7/2019

The Internet of Things

Recently, many common household objects have been integrated with new features giving them access to greater functionality than before. For example, a refrigerator with a built-in touch screen that tells what foods your out of and allowing you to order more from right there at the refrigerator. Or a voice activated coffee maker than allows you to program it to start brewing before you even get out of bed. Or even being able to lock and unlock your car from anywhere using your smart phone. All of the things listed before take advantage of a system call the Internet of Things. “The IoT embeds some intelligence in Internet-connected objects to communicate, exchange information, take decisions, invoke actions and provide amazing services” (Future Internet, 2012). The internet of things connects everyday objects to the internet to give them added functionality that they wouldn’t before. Generally, this functionality makes the device smarter than it was before in that it now has access to significant processing power. This processing power is not contained in the device itself, it only contains a basic microcontroller. The microcontroller sends the data from the user to the cloud where processing power is abundant, and then receives the final product. This off loading to the cloud for data processing is vital for many devices in the internet of things because most devices aren’t capable of such processing because they only have simple microcontrollers.

Smart Internet of Things devices are beginning to make they way in to out daily lives. In Barcelona, they have installed sensors in all the trash cans that detect how full they are. “The sensor measures the container filling level using ultrasonic technology, and periodically transmits all captured information to the Urbiotica Software Platform, where the data is processed and distributed to a third-party application where route planning optimization is made” (Rowley, 2016). Spain is using microcontrollers imbedded in their trash cans to become more efficient at waste disposal. “In Barcelona alone, more than $4 billion in savings is expected in the next 10 years, due to the adoption of IoT-aided waste management technology” (Rowley, 2016). The reason that microcontrollers work well for Internet of Things uses is that they are generally low powered allowing some to be powered by batteries and they are cheap to produce. Internet of Things devices have also made their way in to our vehicles. Some newer vehicles can contain hundreds of sensors that work to make sure the car is operating correctly and to keep the user informed of any possible danger.

(Vasamsetti, 2017)

 Because of the simple and low powered nature of Internet of Things devices, they are susceptible to some security vulnerabilities and challenges. The Internet of Things consists of three layers: the Application Layer, the Network Layer, and the Physical Layer. The physical layer is the hardware of the device including the processor chip, any sensors, and the physical network interfaces. The physical layer is responsible for device identification (UUID). The network layer includes network interfaces, communication channels and any network management tools required to connect to the network or other Internet of Things devices. The application layer is the software or database that the devices connect to in order to relay their data to. This is usually in the cloud or a central hub that all devices are connected to. Each layer is susceptible to different security flaws and challenges. Due to the nature of hardware, if someone has access to the physical layer they can modify or tamper with the device. This attack is the generally the easiest to execute if access is available but also the easiest to prevent when planning ahead. The network layer is prone to multiple attacks including man in the middle attacks and spoofing. an in the middle attacks work by intercepting the flow of data from point to point. This attack only works if the data is not encrypted from point to point. There is nothing to intercept if the data is encrypted. Spoofing works by convincing a device on the network that you are something you’re not by either spoofing your MAC address or RFID signal. The application layer can be attacked using DoS or DDoS attacks. Denial of Service attacks render a machine or service unviable by repeatedly requesting or sending it data. So much that data that it can’t process it all causing the service to slow or completely crash. A Distributed Denial of Service attack is the same as a DoS attack except distributed across multiple machines to increase the number of requests hitting the service. Despite their simplicity, this is only a short example of security risks faced by Internet of Things devices.

(I. Andrea, 2015)

(I. Andrea, 2015)

A recent new use for Internet of Things devices has been home automation. Imagine waking up in the morning to your lights simulating the rising of the sun and as you walk down the hallway towards the bathroom, the lights turn on automatically when they detect your movement. Or getting daily updates from your home security system about any recent movement around your house. How about being able to lock and unlock all doors and windows using a voice command. All of these are possible with home automation using Internet of Things devices. Many IoT devices have been created recently to enable people to make “smart” homes that act and react how they design them to. Such as razing the blinds at a specified time of day or turning on certain lights to simulate someone being home even when you’re not. Most of these home automation attempts require a hub that all the devices connect to. A lot of devices are designed with the idea of integration in mind so they can connect and work with other home devices even if they were not designed to work together initially. Home automation is not only for convivence but are extremely useful for handicapped individuals. “Voice recognition based home automation systems are most useful for handicapped and elderly persons, who wants to control home appliances by speaking voice commands” (Asadullah, 2016). Home automation can also make your home more efficient by automatically turning off lights, fans, TV’s, and regulating your heating and cooling. Home automation is one of many examples where the Internet of Things has helped to improve our lives.

The Internet of Things connects many devices together in order to improve the lives of everyone who uses them. These devices tend to be smaller microcontrollers because they can fit almost anywhere they are needed. Internet of Things devices can be found everywhere in our daily lives, in our cars, houses, and work. These devices change how we interact with the world. They connect everything we do to the internet. The Internet of Things was created out of necessity as more and more devices were created that need to interface with each other and the internet.

**Bibliography**

Asadullah, Muhammad & Raza, Ahsan. (2016). An overview of home automation systems. 10.1109/ICRAI.2016.7791223.

I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 2015, pp. 180-187.

R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," 2012 10th International Conference on Frontiers of Information Technology, Islamabad, 2012, pp. 257-260.

Rowley, Melissa Jun. “How the Internet of Things Is Aiding the Garbage Crisis.” The Network | The Network, 18 Apr. 2016, https: //newsroom.cisco.com/feature-content?articleId=1757267.

Vasamsetti, Subrahmanyam. (2017). Future Automobile an Introduction of IOT. 10.13140/RG.2.2.15587.40484.