CLM 2016 Cyber Liability Summit
October 5, 2016 in New York City

Internet of Things – Modern Day Warfare and Threats Both Seen and Unseen

I. Understanding the Internet of Things

A. Definition

The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.

The Internet of Things (IoT) is defined as:

> "The Internet enables any-to-any connectivity. Smart Buildings, HVAC and even physical security technologies are now connected, as are handheld smart devices and more. The latest wave of 'things' connecting users, businesses and other 'things' using mixtures of wired and wireless connectivity, includes but is not limited to automobiles, airplanes, medical machinery and personal (implanted) medical devices, and SCADA systems (windmills, environmental sensor, natural gas extraction platforms, hydro systems, you name it)." National Security Telecommunications Advisory Committee. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Meeting%20Discussion%20Aid.pdf

> "The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data:
>
> "if one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security". *Oxford Dictionary*
>
> The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. *Wikipedia*

> "The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes.
> The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. No longer does the object relate just to you, but is now connected to surrounding objects and database data. When many objects act in unison, they are known as having 'ambient intelligence.'" *Techopedia*

Devices

While most think of single purpose devices which use wireless connectivity when thinking of the IoT, the IoT includes a wide range of devices. Those devices can range from PCs, servers, switches to medical machinery, process control kiosks and smartphones. For the most part, it is the single purpose devices that have seen dramatic growth of embedded computing and communications capabilities into things like automobiles, trains, electric meters, vending machines, personal devices and more. The embedded nature of the software causes problems for vulnerability assessment and configuration management processes. For the most part, IoT implementations use different technical communications models, each with its own characteristics. Four common models described by the Internet Architecture Board include: *Device-to-Device, Device-to-Cloud, Device-to-Gateway*, and *Back-End Data-Sharing*. These models show the versatility of IoT devices in connecting and providing value to the user.

Prevalence

As the need and desire for continued connectivity evolves, the number of mobile connections worldwide is set to rise dramatically to reach 10.5 billion by 2020, while the total number of connected devices across all access technologies could reach 25.6 billion, according to the GSMA, Connected Living White Paper issued in July 2014, *Understanding the Internet of Things (IoT).* Per this same publication, the IoT, by enabling devices to communicate with each other independently of human interaction, will open up new revenue streams, facilitate new business models, drive efficiencies and improve the way existing services across many different sectors are delivered.

It is predicted, that the IoT will reflect a demand-side stimulus that helps finance the deployment of mobile broadband networks around the world. Anticipating that the positive impact on the global economy could be as much as $4.5 trillion per year, according to a study by Machina Research.

According to GSMA's January 2014 review, there were 428 mobile operators offering mobile to mobile services across 187 countries, which is the equivalent of four out of ten mobile operators worldwide. The highest proportion of operators offering mobile to mobile services were in Europe, where it was estimated that two-thirds of operators had mobile to mobile offerings. By comparison the US had just under half its operators utilizing mobile to mobile. Market forecasts performed by Machina Research indicate that by 2020, the number of

connected devices in the world will almost tripe from more than nine billion now to 25.6 billion by 2020. Of these, 10.5 billion are estimated to connect using mobile technology with a dedicated SIM and connection to a mobile network.

B. Vulnerabilities associated with the Internet of Things

A study conducted by HP Fortify found that among even among just a small sample of some of the most popular and prevalent Internet of Things (IoT) devices, researchers uncovered 250 vulnerabilities -- many of which were severe and resulted in remote code execution, including vulnerabilities to Heartbleed, denial of service, and cross-site scripting.

The study was meant to demonstrate what may be found when a more comprehensive and disciplined approach is taken to examining this growing new class of devices. For the study, HP Fortify used as a backbone for testing 10 common devices, including a webcam, home thermostat, sprinkler controller, home alarm, and garage door opener.

Among those 10 devices, HP Security Research found an average of 25 vulnerabilities per device. Seven out of 10 of the devices when combined with their cloud and mobile applications gave attackers the ability to identify valid user accounts through enumeration. Nine out of 10 devices collected at least one piece of personal information through the device or related cloud or mobile app; and six of the devices had user interfaces vulnerable to a range of web flaws such as persistent XSS.

Though many IoT devices are marketed to consumers, these rampant vulnerabilities have quite a bit of relevance for enterprises as well. Last year we saw several well publicized hacks involving the IoT that raised awareness of the issue. They were:

(1) Internet-Enabled Automobiles. 2014 Jeep Grand Cherokee remotely hacked by WIRED, which led to the recall of 1.4 vehicles.
(2) Medical Devices. Students at the University of Alabama hacked a pacemaker implanted in iStan- a robotic dummy patient used to train medical students. They were able to speed and slow the heartrate eventually killing iStan, theoretically.
(3) Lots of other stuff. Hello Barbie had a smart phone app with led to interception of the audio recorded by the doll. Samsung's "Smart fridge" which allowed gmail credentials vulnerable.

II. Internet of Things Educational Scenarios:

A. Common Cloud Sharing

Cloud computing is such a popular topic because it can be a substantial benefit in conserving resources and saving money. Moving software, storage, e-mail, etc. to the cloud, helps organizations dedicate only the resources necessary to these services. Storage space, computing power, memory, and even licensing can be avoided in some cases, saving costs.

By outsourcing IT services to cloud providers, organizations are able to free up IT staff to other business uses rather than spending time supporting services that cloud providers can take over.

With the cost saving possibilities, it is difficult to understand why organizations are hesitant to move data, software, and other services to the cloud. But, if you consider the security risks that are involved, some organizations won't make the move. According to most polls, security is the main reason why a move towards cloud-based solutions is not initiated. A recent LinkedIn survey showed that 54% of the 7,053 respondents claimed that security is the top concern when it comes to migrating to the cloud.

There are security vulnerabilities that attackers look for in the cloud, not unlike other IT services. Education and understanding of the vulnerabilities can enhance security in the cloud making it a safer place. In fact, cloud based services has improved security according to 57% of the participants of a Mimecast survey.

In various cloud models, and the hybrid cloud model to a lesser extent, many different customers share resources using virtualization. This computing platform presents the following potential weaknesses:

- Communication between different virtual machines or between a virtual machine and the host through shared disks, virtual switches, or virtual local area networks (VLANs) and a shared I/O or cache.
- Generic drivers that emulate hardware.
- Vulnerabilities in the hypervisor that allow the execution of arbitrary code on the host with the privileges of the hypervisor that allow an attacker to control all virtual machines and the host itself.
- Virtual machine-based root kits that allow for modification of the hypervisor system calls to the host operating system to run malicious code.
- An exploit, known as *virtual machine escape*, where a program in one virtual machine is given unrestricted access to the host through shared resources.
- Denial-of-service attacks run on one virtual machine that bring down the others running on the same host.

If a secured environment is necessary due to laws, standards, or industry regulations, then the approach to security needs to reflect these requirements. The preferred method is a private cloud solution or even a hybrid solution with sensitive data, transactions, and services hosted in the private section to give your organization greater control over security and access. Performing an assessment of the cloud provider is essential. Request information about vulnerability protections and virtualization software. Also, one should know that patching and upgrading is done and whether the cloud host uses a trusted platform module.

B. Medical Equipment Interface

Implantable medical devices are forecast to grow about 7.7% through 2015, and more than 2.5 million people already rely on them to keep various illnesses at bay, according to a study by Freedonia Group.

Today's medical equipment involves everything from Wi-Fi to Bluetooth communication in an effort to increase the flow of patient medical information to medical staff. But, these devices are not properly secured. Most are preconfigured with default passwords such as "password" or "admin," making them vulnerable to attack.

The US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) cited 300 medical devices from 40 companies that had unchangeable passwords. Any attacker who possessed these passwords could log in and change critical settings, with dire results. Manufacturers of these devices have difficulty issuing security patches to this software, because most medical equipment requiring a software upgrade must be resubmitted for FDA approval.

Unauthorized access to an implantable medical device is taken seriously by the US Department of Homeland Security takes very seriously. Over 300,000 Americans receive wireless IMDs each year, including pacemakers, neuro-stimulators, and drug delivery pumps. AT current, attackers could hack the bodies of hundreds of thousands (if not millions) of people who rely on these devices to stay alive.

These devices have what looks like any other IP address, so not a stretch to imagine an attack scenario that involves remotely taking control of an implanted defibrillator. The battery life needed to regulate heartbeats could easily be depleted, thus requiring emergency medical intervention. Also, the communication technologies used by IMDs are often not regulated and are insecure. Advanced tools can easily take advantage of vulnerable security mechanisms and either change the default settings of such devices or provide remote commands.

Network-enabled hospital equipment such as infusion pumps can also be subject to cyberattacks because of software vulnerabilities. This has been the focus of the FDA. Specifically, the Infusion Pump Improvement Initiative was specifically aimed at manufacturers to facilitate device improvements through software upgrades and to mitigate risks that might make them vulnerable to outside interventions.

It's not fantasy to imagine a cyber attack on a hospital's Wi-Fi network whereby a hacker can gain access to all stored medical data. With the interface, life saving equipment could be compromised.

III. Prophylactic Measures

There is widespread agreement that companies developing IoT products should implement reasonable security. What constitutes reasonable security for a given device depends on a number of factors, including the amount and type of data collected. The FTC commissioned a workshop on this issue and in that workshop they urged companies to consider adopting the best practices as follows:

a. build security into their devices at the outset, rather than as an afterthought.
b. As part of the security by design process, companies should consider:
    (1) conducting a privacy or security risk assessment;
    (2) minimizing the data they collect and retain; and
    (3) testing their security measures before launching their products.
c. companies should train all employees about good security and ensure that security issues are addressed at the appropriate level of responsibility within the organization.

d. companies should retain service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers.
e. When companies identify significant risks within their systems, they should implement a defense-indepth approach, in which they consider implementing security measures at several levels.
f. companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.
g. companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

Additionally, data minimization is another tool recommended by the FTC to reduce security risks involved in the IoT. Data Minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. While data minimization could limit the innovative uses of data, companies should consider reasonably limiting their collection and retention of consumer data.

Data minimization can help guard limit security risks involving the IoT in two ways. First, larger data stores present a more attractive target for hackers and also increases the potential harm to consumers from such an event. Second, maintaining large amounts of data increases the risk that the data will be used in a manner that departs from consumers' reasonable expectations.

As is the case anytime personally identifiable or sensitive data is store, the best defense is a good offense and a breach response plan should be in place prior to a breach.