Chapter 7

SECURITY AND PRIVACU ISSUES IN INTERNET OF THINGS

INTRODUCTION

Security phase has been brought up in a multitude of sectors with a myriad of feelings backing it. Those in the IT field will typically harbor mixed emotions about security for a good reason. With the advent of the internet, society has shifted towards dynamic where we want as much information as possible with high speed. With this ideology and the ever-growing field of big-data, we've come to a market-dictated solution known as the Internet of Things or for those more accustomed to the alphabet soup of the IT industry, IoT.

A fundamental element of IoT is simply a device with an internet connection. It generates traffic involving data very personal to the owners. These devices range from Mother, a simple motion tracking object used to help maintain a constant routine, to Alexa, Amazon's Always-listening personal assistant; IoT devices utilized in lifesaving devices such as insulin pumps and pace makers.

These devices integral part to our lives as the internet is, the devices that interact with it have taken a backseat when it comes to security. The IT world is on fire related to security and what it means to security, and with good reason.

The three states of digital data can be useful in defining security requirements for IoT. These three states are data at rest, data in use and data in motion. Data at rest refers to data stored on a device such as a hard drive or offsite cloud backup that is not currently being transmitted, read or processed. Data in use, on the other hand, is data that is in the process of being generated, updated, appended or erased by one more applications. Data in motion is defined as data that is in the process of traveling across a network. Many companies that haven’t yet developed a single IoT application are already exposed to these risks. The Shoran web index, which slithers the Internet searching for associated gadgets, has just listed more than 500 million associated gadgets including control frameworks for industrial facilities, hockey arenas, auto washes, activity lights, surveillance cameras and even an atomic plant. These gadgets were commonly associated with the Internet through an interior application gave by the maker or by outsiders so now and again the proprietor of the gadget may not know that it is associated. As you may expect, these gadgets frequently have just simple security capacities. A significant number of these gadgets require no secret word to associate with them and numerous others utilize "administrator" as their client name and "1234" as

their watchword. 70% of the gadgets convey in plain content so softening up is simple regardless of the possibility that they utilize a safe secret key.

Furthermore, millions of devices are running very old versions of their operating systems with many known vulnerabilities that a hacker could use to gain access to the system. In the first place, associations should fuse security with their contraptions toward the start, instead of as a touch of insight into the past. As a noteworthy part of the security by design process, associations should consider: (1) driving an insurance or security peril assessment; (2) restricting the data they assemble and hold; and (3) testing their wellbeing endeavors before impelling their things. Second, as to staff sharpens, associations ought to set up all specialists for extraordinary security, and certification State-of-the-art IoT platforms provide a highly granular system of permissions and visibility that can be implemented without coding. These platforms make it possible to grant or deny both design time and run time permissions at a range of different levels. In the case of a conflict, the most restrictive security setting is honored. Access control can be granted at the most granular level such as specific read or write access to a single property of a single thing. Or, the ability to read all properties of all things in the system can be granted much more broadly at the collection level. Likewise, multiple property services, subscriptions and events can be combined in a template to which permissions can be granted. Another approach is to structure things and people into hierarchical structures which might be based on organizational units, function, geography or business process and assign permissions and visibility based on this structure.

While Commission staff urges Congress to consider protection and security enactment, we will keep on using our current instruments to guarantee that IoT organizations keep on consider security and protection issues as they grow new gadgets and administrations. Classified information very still ought to be encoded on IoT applications and cloud administrations to avoid information breaks and utmost the downstream effect of a traded off application. Specifically, framework passwords and keys ought to dependably be put away encoded and client passwords must be hashed both at the edge parts and at the IoT stage. Generally, memory preparing on a PC isn't secured for information being used. The alleviating controls ensuring the machine are viewed as satisfactory for information preparing. Cryptographic capacity preparing some of the time keeps running in a Trusted Platform Module (TPM) which is a devoted microcontroller for secure crypto calculation. Your association ought to decide whether the expenses of such an answer are essential for the application that you are planning. Information on movement ought to likewise be encoded so it can't be blocked or controlled while making a trip to its goal. The present business models are AES 128 or 256 for symmetric key encryption and RSA 2048 for lopsided or open key encryption. Information on movement encryption ought to be considered for the information transmitted crosswise over systems and for information inside a system for example between a gadget and door or perhaps between a sensor and gadget. Obviously, there are a few examples where the equipment does not have the handling energy to have the capacity to perform encryption exercises. In these cases, organize observing and other alleviating security controls ought to be set up.

IoT stages created utilizing these structures have a more develop security pose and are more secure as well as can adjust to a consistently changing security scene. For instance, Open SAMM rules give a system to security administration, development, confirmation and organization. Each of these business capacities have a subset of security hones related with them. Confirmation for example incorporates configuration surveys, code audits and security testing. While numerous assessments concentrate on the pen testing part of security testing,

one can perceive how the Open SAMM structure has a significantly more extensive arrangement of contemplations and in this way pushes associations to comprehensively build up their IoT applications. Not exclusively do these systems help to alleviate security issues yet they likewise can bring down advancement costs. It's significantly less costly to settle issues ahead of schedule in the improvement procedure than after the product has been conveyed into the field.

The potential for considerable execution and cost enhancements is rousing numerous associations to create a large number of new shrewd, associated items. With the quantity of associated gadgets and applications expanding at an exponential rate, it's a given that the security dangers related to these gadgets and applications are likewise soaring. The number and assortment of these gadgets exhibit a wide assault surface that joined with the nonappearance as a rule of human administrators postures fundamentally critical security challenges. This white paper has delineated security best practices that can be connected at the gadget and application level by associations that are arranging or planning savvy associated items to guarantee the security of their IoT gadgets and arrangements.

WHY IS IoT SECURITY IMPORTANT?

Internet of Things can be defined as the network of physical devices, home equipment as well as other items that may have software, actuators, sensors and network connectivity embedded in their structure to enable them link and exchange data with one another(Mattern and Floerkemeier). IoT is a means by which technology can manage to integrate the physical world that we experience into computer-based systems. The term “things” in IoT can refer to a wide range of devices like automobiles, field operation devices, air purifiers, cameras, mobile phones and heart monitoring implants among many others.

With IoT spreading its use and influence to almost all sectors of human life, it is important to ensure that all IoT devices are guided with a number of elements (Noto La Diega and Walden). These key elements increase the quality assurance of the IoT devices as well as safeguard the interests of the users. When a client is making decisions to make use of an IoT device, there are a number of things that they consider from cost, return on investment and the security, privacy and ethical considerations by the manufacturer (Singh, Pasquier and Bacon).

Key Elements of IoT

There has been consumer concerns raised that most IoT devices are developed in a rush without careful considerations for their privacy and security elements (Singh, Pasquier and Bacon). According to a survey carried out by Business Insider Intelligence, in the last quarter of the year 2014, 39% of the survey respondents felt that security was their biggest concern when considering using new IoT technology. Security and privacy are part of the key elements that determine the effectiveness of IoT devices.

Security: Consumers have expressed concerns mostly about the handlers of big packets of data. This data is harvested in large quantities and stored over a long period of time. In case of

a high profile hack, it is possible that consumer details could be brought to light and used inappropriately. Most IoT devices are sold to customers with unpatched software and operating systems. Aside from this overlooked mistake, some consumers forget to change the original password after purchasing their smart devices**.**

***Privacy*:** IoT privacy involves protecting consumer information from exposure in the IoT environment (Rouse, IoT Privacy). Data transmitted from more than one endpoint when collected and analysed can give rise to sensitive information. Consumer concerns on privacy have been plagued with notions that it would be impossible for infrastructures that deal with big data like IoT to consider privacy. Some of these IoT devices have been labelled to invade public space.

As technology advances, we as a society are using the information generated by the technology to improve our lives. While the notion and ideology is sound, but we have to tackle potential of the abuse. The methods we use to enrich our lives should be tried, tested, and secured. Several companies have started shifting their models to accommodate for this change in ideas, but as it stands; the IT community still lives in a ‘wild west' mentality.

In just 2016, Cyber attacks in the healthcare industry have risen over 60%. Credit card processing systems, as well as 3.6 million patient records of Banner Health, 3.4 million patient files, were taken from Newkirk Products, and even a worst case that the FBI had to alert 21st Century Oncology of their breach, which affected 2.2 million people.

These are three of the biggest incidents to happen in 2016. Three compromises of the integrity of three companies put millions of people at risk. Now the inability to secure the IoT environment vastly expands the ability for malicious intent. We've started to see just a glimpse of the harm that could come from the lackadaisical approach to the development of the Internet of Things, such as the attack on the ISP Dyn late 2016.

In October of 2016, hackers initiated a DDoS or Distributed-Denial-of-Service attack in which multiple compromised network-connected systems try to take a service offline by bombarding it with traffic, directed at that facility's resources; against the Internet Service Provider (ISP) Dyn. The devices responsible devices compromised by using malware Mirai, which allows the compromise of old Linux and turning them into bots that can perform large-scale network attacks. The DNS server was knocked out; it affected customers ranged from private individuals to big-name players such as Amazon, Spotify, Netflix and Paypal.

TECHNICAL ANALYSIS

Data protection has been an issue since the first two computers were connected. As the Internet evolved, concerns for security also grew to include personal privacy, and threats from cyber theft. In the case of IoT security is synonymous with safety. With a regular computer device, when you get hacked you might lose some money. There's no doubt that can have devastating effects. However, when there is interference with a pacemaker, or a nuclear reactor, it poses a threat to human life.

The evolution of security has grown in parallel with networks. First there was the packet filtering firewalls in the late 1980s. From there they progressed to the more sophisticated firewalls that were protocol and application aware whiach are introducing intrusion detection

and prevention systems and security incident and event management solutions. These were designed to attempt to keep malicious activity off of a network. However, if they did gain access, these controls would detect them if a firewall was breached by malware, antivirus, using signature matching and blacklisting to identify and fix the problem.

As malware grew and detection techniques advanced, blacklisting was replaced by whitelisting techniques. Correspondingly, many different access control systems were developed as more and more devices started coming onto corporate networks. These systems authenticated devices and users as well as authorizing those users for specific actions.

Concerns over software authenticity and intellectual property protection, resulted in various software verification and attestation techniques, sometimes referred to as trusted or measured boot. Data confidentiality has always been the primary concern. Controls like physical media encryption and VPNs were created so that data in motion could be secured.

With all these security controls and techniques, one would think it wouldn't be too difficult to apply variant of them to in the IoT world. However, in order to do that, considerable re-engineering would be required in order to address device constraints. For example, blacklisting which is very successful on a regular network requires too much disk space to be a practical solution for IoT application. IoT devices often have limited connectivity and are designed for low power consumption. Customarily, their processing power and memory is limited to only as much as they need to perform their task. To add to the challenge, most are "headless" devices, meaning that there is no human operating them. this eliminates the possibility of someone inputting authentication credentials or decide if an application should be trusted. In our absence, the device must decide on its own whether to accept a command or execute a task.

Because there are numerous IoT applications, there are just as many security challenges to go with them. For example, the control systems for nuclear reactors are attached to infrastructure. These systems need consistent updates and patches in a timely manner to work properly, but how can they receive them without impairing functional safety. As another example, consider smart meters for your home. These meters collect data like energy usage to send to the utility company. But that information must be protected. The data showing that power usage has dropped could indicate that a home is empty, making it a target for burglars.

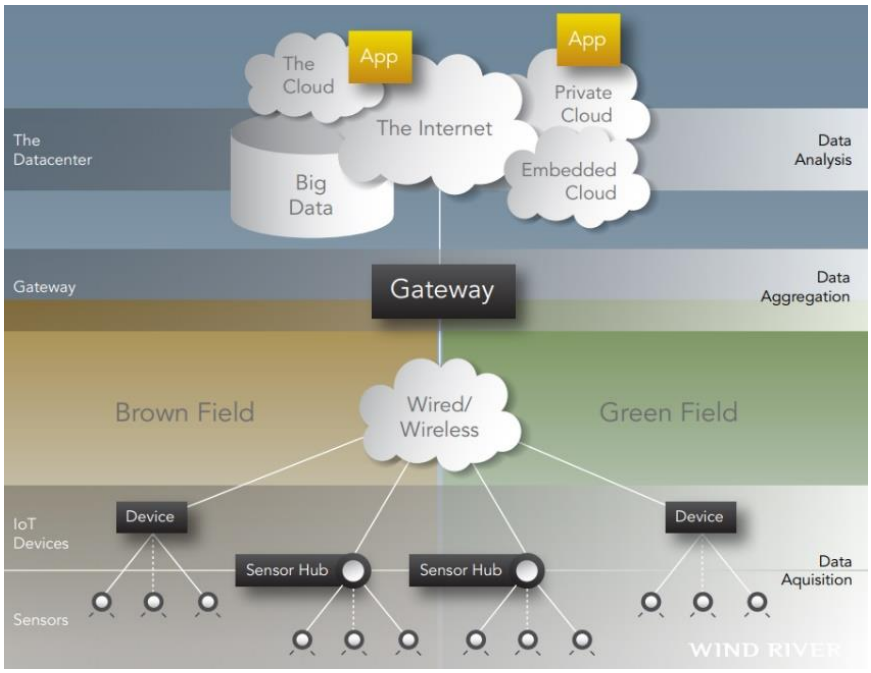

Figure 1: IoT syatem Infrstructre

With so many different challenges to overcome, it's no wonder why this problem has yet to be solved. However, many people have ideas on how to address this. The most popular solution proposed is a multi-layered approach that starts from the bottom up. This approach would start with secure booting. When the device is first given power, the software on the device is verified for authenticity and integrity using cryptographically generated digital signatures. A digital signature looks something like this:

In the case of IoT security, the digital signature would be attached to a software image and then the device would verify it to make sure the software has been authorized to run on that particular device, and signed by the entity that authorized it, can be loaded. This establishes a foundation of trust to start.

The next step would be applying different forms of access control. These controls would be built into the operating system and could be either role-based or mandatory. These controls limit the privileges of device applications and components so that they only access the resources they need to do their jobs. In the event that a component is compromised, access control can ensure that the intruders' access is minimumized to other system parts.

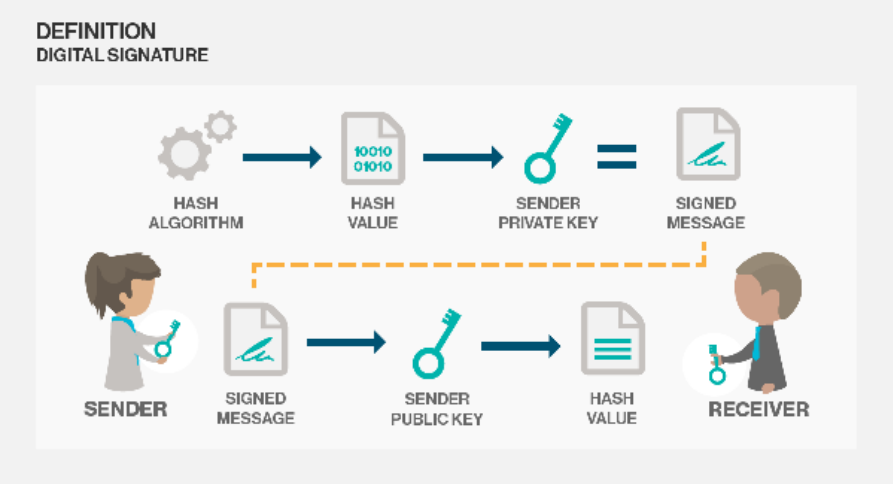

Figure2: A typical digtal signature

After access control, the next step would be Device authentication. This means that prior to receiving or transmitting any data, a device should authenticate itself as soon as it is plugged into the network. Similar to user authentication which allows a user on a network based on credentials that user provides, device authentication works the same with a set of credentials stored in a secure storage area.

After device authentication, firewalls and IPS are the next layer to securing IoT devices. These firewalls will inspect and control traffic that is destined to end at the device. These are necessary even though network-based appliances are in place because deeply embedded devices are unique to themselves, independent from enterprise IT protocols. Industry specific protocol filtering and deep-packet inspection capabilities are important to have in order to identify malicious payloads hiding in non-IT protocols. With these in place, a device won't have worry about filtering higher-level common internet traffic, but it does still need to filter the specific data destined to terminate on that device.

The last layer in this solution is simply updates and patches. The patches that operators need to roll out should be authenticated by the device in a way that doesn't harm the functional safety of the device or consume bandwidth.

This solution starts at the very beginning. Security should not be an afterthought adds on to a device, but an integral part of a devices functioning. The solution does not start at any one place but should be implemented up through the layer to be effective. The internet of things may never be 100 percent secure but through collaboration across stakeholders in hardware, software, network and cloud, we can be prepared.

Economic analysis

The security of the Internet of Things is a huge issue. While the devices you have in your home pose a certain security risk, the repercussions of those devices getting hacked would be significantly less devastating to the population than a device in the electrical grid. Attacks in the last few years on places like the Ukrainian power grid, have highlighted the increasing need for security.

One of the biggest challenges in security is money and the questions is always who should be responsible for the costs. Back to the example of power grids, should private owners be responsible for the major investments? It is, after all, to their advantage to invest in security, at least up to the point of their own losses, mostly loss in revenue. However, there is also a much greater cost to our society if there were to be a major electrical outage. This justifies much greater spending to manage the security risks of a sophisticated attack. For these types of attacks, it is possible that private investments will not be enough. It's because of this reason that the government wants to institute some form of security oversight on critical infrastructures. This asymmetry of cost means that we cannot put too much faith that a free market system will optimize the outcome.

Cost asymmetry is part of a larger field commonly referred to as security economics. New to the economic discipline, it focuses on understanding security incentives and the cost misalignments. There are a few different elements with this field. Software being at the center of the cybersecurity problem Non-adhesion contracts absolves a vendor from any liability, such as security vulnerabilities. These contracts are wide-spread, giving the software vendors very little incentive to concern themselves with security.

Though some liability should be attached to security failures if we want better security outcomes, it's unreasonable to expect vendors to shoulder the blame and full cost of every security failure. With the technology we have today, no product can ever be 100 percent secure. Having said that, there are many best practices that can greatly reduces vulnerabilities. It is true however, that security can slow down software development making vendors risk the speed of innovation with the added expense.

At this point the question becomes how we find a middle ground between no liability and full liability so that we can improve the outcome for the entire system, and not just software companies' share price. A great example that could be used as a model is the automotive industry. As the technology for self-driving cars becomes more prevalent and mainstream, many have questioned its liability. Automotive manufactures have always been held to a higher standard than software companies due to the nature and dangers their product bring. To ensure the safety and security of their product, automotive manufacturers are working side-by-side with regulator and security companies like BlackBerry to ensure that their systems are adequately secure. This partnerships regulations and industry practices could be used as the example to establish liability guidelines for other IoT devices.

In today's market, being a first mover in a burgeoning market means some significant advantages for the seller. These first movers often gain a foothold in such markets and experience exponential customer growth, which gives them the dominant position in that market. In this case, time-to-market is vital to the success of the business.

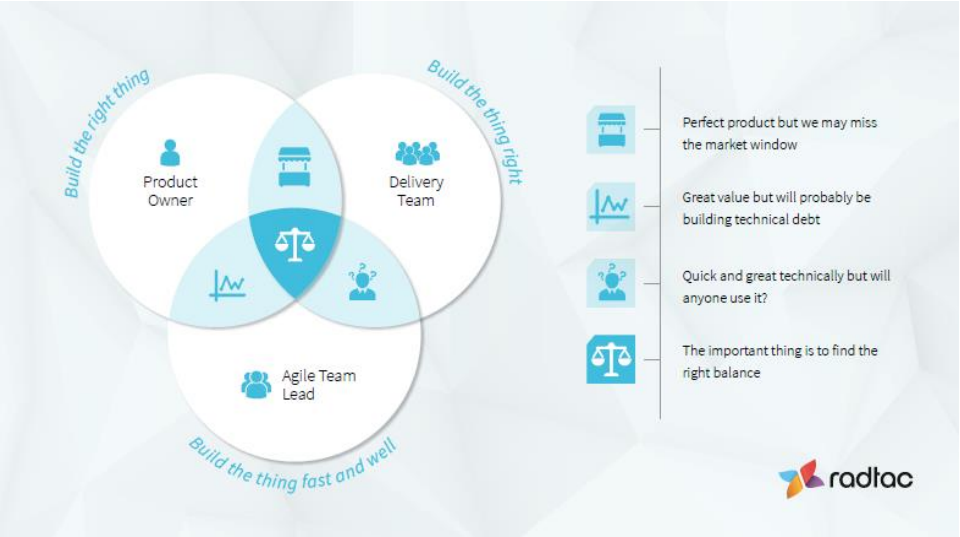

Figure3: Time to market conisderation

The lack of liability and the hazy nature of security during the buying process has generally lead to the shipment of products with all the required features first, leaving security to be worried about later. Historically, this has caused companies that delay time-to-market for the sake of security to be penalized. This dynamic, however, is unnecessary in the IoT market. Operating system defects and design issues are responsible for many security concerns. With the new IoT devices, many of these issues are invisible to the user. It is for this reason that leveraging third-party embedded system platforms as a starting point for product development could be advantageous for vendors. This would allow their products to be more secure and stable as well as allowing a faster time-to-market.

While the technology and processes for security in the Internet of things will be important in the coming years, some of the battles fought on this subject won't be about technology at all. Instead they will be about the economics of security incentives. Who is liable and who's not. Economics will be a driving force in the evolution of security in IoT.

VAULT 7: FBI'S ARMAMENT UNLEASHED

On March 7th, 2017 WikiLeaks posted individual activities and capabilities of the Central Intelligence Agency in the areas of Cyber warfare. Of these files were details of homegrown software capabilities, attack vectors against operating systems of many smart devices including the compromises that can compromise standard operating systems such as Current versions of Microsoft's Windows, Mac OS X, and certain distros of Linux.

The release from WikiLeaks came in 10 parts:

Year Zero – Lays out over 7800+ web pages detailing exploits and capabilities of software supposedly written by the Center for Cyber Intelligence.

Dark Matter – Documented the CIA's efforts to hack iOS and macOS at both the software and hardware level.
Marble – Contained a little fewer than 700 source code files for the framework designed to obfuscate to evade current malware detection techniques.
Grasshopper – Framework used in building persistence malware payloads for Microsoft's Windows operating systems geared towards avoiding standard antivirus solutions including Microsoft's own Security Essentials Suite.
HIVE – This acts as a CIA malware suite with a public-facing HTTPS interface. Using a masking agent to maintain its presence behind public domains (program dubbed "Switchblade") allows the transfer of information and opens the compromised devices up for directions for tasks.
Weeping Angel – Joint product ventured by CIA and MI5, allows televisions with built in microphones and possibly video cameras to record and transmit even when they turned off.
Scribbles – Contained source code of a tool that generates documents with web-beacon tags dedicated to tracking document leaks (How Ironic).
Archimedes – Redirected browser sessions to a different computer (MITM or Man in the Middle).
After Midnight & Assassin – Malware disguised as DLL's that upon reboot, allowed sets up a connection with the host. Assassin does something similar but disguises itself as a windows process.
Athena & Hera – This two hijack both remote access service and DNS caching service. Both affect all current versions of Windows 10 and could potentially affect Windows Server 2012.

The majority of these were zero-day exploits, meaning that these were not previously known vulnerabilities. The CIA had these leaked and already developed behind closed doors. The idea is that the devices that we utilize on a day to day basis could use, exploit and compromise to the extent that you wind up on the 11 o'clock news.

Wannacry

On Friday, 12 of May 2017, first mass weaponized attack from the Vault 7 leak. The WannaCry ransomware crypto-worm utilizes EternalBlue, an exploit in SMB protocol. The popularity of the incident went viral when discovered from a weaponized exploit that the NSA had, but didn't report it to Microsoft; within less than four days, 230,000 machines infected in over 150 countries.

WannaCry was just one worm that comprised of several exploits that affected windows machines. Roughly 11% of medical devices are windows based, and of that 11 %, almost 99% of them are running on an XP system.

The idea is that we're going into an age where security needs to be an after-thought. It's come to the point where we need to set standards for IoT that can allow peace of mind, but this can easily attribute to a mindset. Producers have to inspect their products better, before releasing it to the public.

The next step analysis of the situation shows us analogy “be the calm before the storm”. IoT holds a pretty significant chink in the armor that we try to uphold in the everyday struggle of information technology. Since the beginning, we installed the devices to maintain the CIA triad: Confidentiality, Integrity, and availability. There is a multitude of pros and cons to each

subject of the Triad. The mindset has to start at the beginning of the project with incentives to upgrade and to keep things at the standard required for the internet of things.

Many organizations utilize the CIA model when creating their information security policies as a method of staying ahead of the evolving cyber-threat. Following the payment card industry, security standards council is a sure-fire way to get started to changing the mindset of your organization to prepare yourself against cyber threats.

PCI sets the baseline of technical and operational instances that practice a "defense-in-depth" approach, especially to cardholder data but can be implemented in all areas of a business to protect a multitude of assets. Maintaining PCI compliance addresses confidentiality through the scrutinization of insecure protocols and the assets it encounters; protocols and services like FTP, Telnet, and various email protocols (PoP3, IMAP, and SNMP).

The idea is to understand what's going in and out and being able to minimize the risk by doing as much as you can to mitigate the worst-case scenario. It becomes a mindset as it sets a standard that to follow, repeat, and secure. This applies to IoT from the beginning of development to software to the services that run on the device.

The Mindset securing the Internet of Things will require the thorough knowledge and strenuous testing of possible vulnerabilities following the OSI model. Here is a brief reminder of the seven-layer system.

Layer 1: Physical – How could the device be physically compromised?
Layer 2: Data Link – how could the connection between two devices be compromised?
Layer 3: Network Layer – How could the machine be compromised from a Network perspective?
Layer 4: Transport Layer – How are we securing the data transmitted between connected devices?
Layer 5: Session Layer – How are we handling remote access?
Layer 6: Presentation Layer – Could the device's interface be abused?
Layer 7: Application Layer – How could someone abuse the service we provide for malicious intent?

Cisco's Idea

Cisco is proposing their framework that allows for the development of a policy to address their perceived threats involving IoT. They developed an encompassing strategy revolving around Authentication, Authorization, Network Enforced Policy, and Secure Analytics.

Authentication

At the core of this framework is Authentication. IoT infrastructure can be accessed with a trust established between devices; an example would be Active Directory Authentication. There are other protocols laid out in IEEE 802.1X utilized as a standard for CPU and memory allocation for credential storage. With this distribution, it allows the ability to establish through X.509 certificates, further advancing cryptographic capabilities for low-grade public-key operation.

Authorization

Using current policy mechanisms, we can control a device's access throughout a network; it works pretty well through enterprise networks by segmenting the traffic which is simple with technology, already implemented in most corporate environments. Trusts could potentially formed from exchanges between devices. Cisco uses cars for their example. Say a car builds a trust with a shop, the car could share its authorization to an on-site worker for readings of the odometer, last maintenance records, etc.

Network Enforced Policy

Once again established policies are well suited to elements involving routing and transportation of traffic securely over the infrastructure.

Secure Analytics Visibility and Control

Secure analytics laid out the services that utilized in an IoT ecosystem. Network analytics used for monitoring a deployment of a massive parallel database that allows for the processing of large volumes of data in near real time. Threat mitigation could vary from shutting down to isolation for further investigation.

Is this a silver bullet? No, in the IT world there isn't a clean cut answer for everything as there are all kinds of variables that have to work around. It's up to us to remain as secure as possible.

Recommendation

Most IoT devices will require the collection, analysis and transmissions of sensitive data. It is of the most importance that this data is adequately protected at all times, also that users are aware of what private data is being processed. I have compiled a list of concerns that should ultimately be applied to devices.

- Device should be designed with security, appropriate to the threat and device capability.

Security architectures for devices, and networks should be developed at the same time as the device rather than implemented later.

- Offer appropriate protection for all devices

Sensitive data may also be exposed in other connected systems. Consider how the security of the data will be covered throughout the network.

- Be sure users are informed of what private data is required for the device to operate.

Many users want to take advantage of the opportunities offered by IoT but they also want to ensure their privacy is taken into consideration and protected.

- Audit security products to be sure sensitive data is being protected.

Implement local security policies for handling private data.

- Manage encryption key securely

Consider the lifecycle of encryption keys, decommissioning when necessary.

Data needs to be protected from tampering or modification while in motion from one location to another. If it is not, you may have a malicious attacker lying in wait for that data to come across. It is too late at that point. Security conditions to consider include the following:

- Be sure your software is verified (e.g. Secure boot)

This ensures that only known and trusted software are allowed to run on the device.

- The device or system should only use a hardware-rooted trust chain

This protects against sophisticated low-level software attacks.

- Data must have authentication and integrity protection.
- Remove any compromised or malfunctioning devices.

If a hacker recognizes any device that is malfunctioning, it is then much easier for them to take over the system and in many instances, take over a network since they would have a way in the front door.

- Minimize which systems have access to important data.
- Test system integrity on a regular basis.

In order to avoid any vulnerability exploitation of device due to operation of device under an out-of-date Software upgrading software is a must and can be done within different scenarios.

- Vendor update and management process

Security patches/updates should be applied as soon as they are available.

- Only install patches/updates from the manufacturer or another authenticated source allowing unauthorized patches/updates could potentially pave the way for hackers.

CONCLUSION

Information technology is a mindset that has to be compatible across all facets of IT. The methods we use to design, implement, and maintain our networks are supposed to be transparent, easily navigated, and appropriately managed. The Internet of Things (IoT) is another hurdle thrown at users, and it's up to users to analyze the problems with this innovation, adapt to the issues, and overcome them with well thought and documented solutions. Internet of things is a pretty substantial hurdle that has given the potential outcomes. It's up to users to alter the mindset towards IoT security, and the IT community has to adapt to these security issues. Researched ideologies have a pretty good grasp on their benefits and effects in the corporate environment, but some professionals deal with this on a day-to-day basis. The struggle is, educating the populace who don't interact and deal with technology every day. Lack of awareness of security threats is the main reason for policy existence, and the policies hold some pretty good ideas to persuade the issues.

REFERENCES

Borza, M. (2017, May 16). How PCI compliance is the first step in achieving the "CIATriad". Retrieved from http://www.bobsguide.com/guide/news/2017/May/16/how-pci-compliance-is-the-first-step-in-achieving-the-cia-triad/

Cisco. (2016, December 16). Securing the Internet of Things: A Proposed Framework. Retrieved from https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html#9

Drolet, M. (2016, June 20). 8 tips to secure those IoT devices. Retrieved June 01, 2017, from http://www.networkworld.com/article/3085607/internet-of-things/8-tips-to-secure-those-iot-devices.html

Foxhoven, P. (2016, November 08). Security risks from the internet of things. Retrieved from http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Security-risks-from-the-internet-of-things

HAJDARBEGOVIC, N. (2015). Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns. Retrieved from https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things

Industry News. (2017, January 25). 3 Big Information Security Stories In 2016. Retrieved from https://www.capella.edu/infosec/year-in-review-sixteen/

INFOSECINSTITUTE. (2015, November 30). Security Challenges in the Internet of Things (IoT). Retrieved from http://resources.infosecinstitute.com/security-challenges-in-the-internet-of-things-iot/

Losey, R. (2014, April 28). The CIA Cyber Security Triad and 9ec4c12949a4f31474f299058ce2b22a. Retrieved from https://e-discoveryteam.com/2014/04/27/the-cia-cyber-security-triad-and-9ec4c12949a4f31474f299058ce2b22a/

Rouse, Margaret. "IoT Privacy." 2015. Prin

Samani, R. (2016, June 06). 3 key security challenges for the Internet of Things. Retrieved August 21, 2017, from https://securingtomorrow.mcafee.com/business/3-key-security-challenges-internet-things/

Singh, Jatinder, et al. "Twenty Cloud Security Considerations for Supporting the Internet of Things." *IEEE Internet of Things Journal* (2015): 1. Print.

Vault 7. (2017, May 31). Retrieved June 02, 2017, from https://en.wikipedia.org/wiki/Vault_7

Bauer, Harald. "Security in the Internet of Things." McKinsey & Company, McKinsey & Company, 1 May 2017, www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things.

Schneier, Bruce. "Schneier on Security." Schneier on Security, 1 Feb. 2017, www.schneier.com/blog/archives/2017/02/security_and_th.html.

"SECURITY IN THE INTERNET OF THINGS ." WindRiver, www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf .

Rouse, Margaret. "What Is IoT Security (Internet of Things Security)? - Definition from WhatIs.com." IoT Agenda, TechTarget, Sept. 2015,

internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security.

Network, CIO. “Security Surprises Arising from the Internet of Things (IoT).” Forbes, Forbes Magazine, 8 May 2017, www.forbes.com/sites/ciocentral/2017/05/08/security-surprises-arising-from-the-internet-of-things-iot/#401fc4d42495.

“The Internet of Secure Things – What Is Really Needed to Secure the Internet of Things?”The Internet of Secure Things – What Is Really Needed to Secure the Internet of Things? | Icon Labs, Icon Labs, www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things.

HAJDARBEGOVIC, NERMIN. “Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns.” Toptal Engineering Blog, Toptal, www.toptal.com/it/are-we-creating-an-insecure-internet-of-things.

Dickson, Ben. “Why IoT Security Is So Critical.” TechCrunch, TechCrunch, 24 Oct. 2015, techcrunch.com/2015/10/24/why-iot-security-is-so-critical/.

J.M. Porup (UK) - Jan 23, 2016 3:30 pm UTC. “‘Internet of Things’ Security Is Hilariously Broken and Getting Worse.” Ars Technica, 23 Jan. 2016, arstechnica.com/information-technology/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

Schneier, Bruce. “The Internet of Things Is Wildly Insecure - And Often Unpatchable.” Wired, Conde Nast, 3 June 2017, www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

“Securing the Internet of Things.” Securing the Internet of Things | Homeland Security, www.dhs.gov/securingtheIoT.

Talluri, Raj. “The Fight to Defend the Internet of Things.” Network World, Network World, 22 June 2017, www.networkworld.com/article/3202767/internet-of-things/the-fight-to-defend-the-internet-of-things.html.

Meola, Andrew. “What Is the Internet of Things (IoT)?” Business Insider, Business Insider, 19 Dec. 2016, www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8.

Dhanjani, Nitesh. Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts. 1st ed., O'Reilly, 2015.

“The Cost of Connectivity: How Will Security Economics Influence IoT Security?” Inside BlackBerry, blogs.blackberry.com/2016/03/the-cost-of-connectivity-how-will-security-economics-influence-iot-security/.