Chapter 7

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;

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

ration devices,

air purifiers, cameras, mobile phones and heart monitoring implants among many others.

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

In just 20

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 d

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

Figure3: Time to market conisderation

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 sW*n 790.192 reWsfor oTe1 that c-1123(or)6( )-22(al)6(l)5(or)6(pea10(act)5

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 devi Mu spub1he Iel con fu7(y)1-3( )-19il78(of9(JTJub1he)-ns)3(por17(ed)-)-5(7)5(bl)5(on78(of9( )-34

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.

REFERENCES

Borza, M. (2017, May 16). How PCI compliance is the first step in achieving the

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