ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

Security in Internet of Things (IoT)

Nimesh Kumar Dwivedi[1], Tanushree Solanki[2], Rashi Jain[3]

UG Scholar, Computer Science Engineering Department, Gyan Ganga College of Technology, Jabalpur, India[1,2,3]

Abstract: The "Internet of things" (IoT) is becoming an increasingly growing topic of conversation. It's a concept that not only has the potential to impact how we live but also how we work. In IoT, the tens of billions of devices that have sensing or actuation capabilities are connected to each other via the Internet. The IoT includes everything from wearable fitness bands and smart home appliances to factory control devices, medical devices and even automobiles. Security has not been a high priority for these devices until now. And this has led to some destructible cyber-attacks aimed through IoT devices seeking authentications, private data, privileges etc. Many cyber security experts have already warned that connecting real world products and appliances to the internet is setting us up for a disaster. This paper is aimed to discuss the security issues of IoT, recent attack scenarios and possible solutions to establish 'Internet of Secure Things'.

Keywords: Intrusion through IoT, Botnets, Distributed-Denial-of-Service (DDoS), IoT Design Issues.

I. INTRODUCTION

British entrepreneur Kevin Ashton in the year 1999 coined the term 'Internet of Things (IoT)', defined as "the infrastructure of the information society". Everything that can be embedded with electronics, software, sensors, actuators, and the network connectivity, enabling collection and exchange of data, can be a part of IoT. Thus, the IoT is a giant network of connected "things" (which also includes people). Expert estimate that IoT will consist of almost 50 billion objects by 2020. The new rule for the future is going to be, "Anything that can be connected, will be connected."

However, concerns have been raised that the IoT is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. In particular, as the IoT spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat. With billions of devices being connected together, what can people do to make sure that their information stays secure? Will someone be able to hack into your toaster and thereby get access to your entire network? The IoT also expedite security threats for companies all over the world. Then we have the issue of privacy and data sharing. This is a contentious topic even today, so one can only imagine how the conversation and concerns will escalate when we are talking about many billions of devices being connected.

II. RESEARCH OBJECTIVE

- Discuss some security threat incidents & vulnerability trends.
- Highlight common threats and identify attack patterns.
- Review some solutions and suggestions proposed bysecurity experts and cyber security firms.

III. IOT ATTACK SCENARIO

Here are some recent incidents of cyber-attacks through IoT devices:

A. Security Team Exposes Vulnerabilities in Drones

The benefits and commercial uses of drones (unmanned aerial vehicles or UAVs) have attracted a massive interest among hobbyists and businesses. And despite their relatively recent introduction in the market, it's been reported that drone sales have already tripled in 2015.

According to the Federal Aviation Administration, drone sales are projected to grow from 2.5 million this year to seven million in 2020. Sale of drones utilized by businesses, is expected to triple over the same period, from 600,000 to 2.7 million.

However, new research from John Hopkins University Baltimore, Maryland has raised concerns over the security of drones after one of its security teams managed to hack and take control of a drone. As part of a capstone project, led by Professor Lanier A. Watkins, team of security informatics graduates, developed an exploit that can wirelessly hack the drone's operations by leveraging software vulnerabilities in the device. Using a hobbyist drone as test subject, the team was able to find three different techniques to send rogue commands from a laptop, disrupt the drone's normal operations while mid-flight, and even cause it to crash.

The implications of the security flaws are much bigger for enterprises and organizations, considering that drones are already being used in law enforcement, education, healthcare, and commercial industries such as agriculture, construction, logistics and gas and oil rig as well as aircraft inspection.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

B. Surveillance Cameras Found Embedded with Malware
According to security researcher Mike Olsen, he discovered that the outdoor surveillance cameras he had purchased contained malware. In his blog post, Olsen described how the software interface showed the camera feed, but the admin page did not offer normal control settings.

Home surveillance and security cameras are a great way to provide security to homes and the workplace. Because of smartifying things, people can access recorded security activities online—making it accessible to anyone with an internet connection, including unauthorized users with the tools and the knowledge.

C. Iranian Hackers Indicted over Alleged Cyber Attacks Targeting US Banks and NY Dam
The US Department of Justice (DoJ) recently indicted 7 Iranians over a slew of high-profile distributed-denial-of-service (DDoS) attacks on major banks, as well as an attempt to shut down a New York dam. The attackers, engaged in a systematic campaign of distributed denial-of-service (DDoS) attacks. The attacks involved the use of botnets and other malicious computer code, and targeted nearly 50 institutions in the US financial sector—including Bank of America, the New York Stock Exchange, and Capital One—with floods of traffic of up to 140Gbps between late 2011 and mid-2013.

Level-3 Heading: A level-3 heading must be indented, in Italic and numbered with an Arabic numeral followed by a right parenthesis. The level-3 heading must end with a colon.

D. Nissan Leaf can be hacked via Mobile App and Web Browser
The talk around car hacks seems to be gaining momentum. Just recently, computer security researchers Troy Hunt and Scott Helme discovered that Nissan's Leaf car app can potentially be used to remotely hack any Nissan Leaf's in-car systems. According to Hunt's findings, he was able to connect to a Leaf model remotely using Nissan's mobile app and control car features remotely without passwords, also found that features such as the car's current battery life, travel times and distances, and climate control can be hacked into as well.

It's certainly not the first time a car hack has been discovered. Last year, a notable car-jackingstunt demonstrated how a hacker with a 3G connection can connect to a Jeep Cherokee's infotainment system. Once connected, the vehicle's engine and brakes could be controlled remotely, and resulted in a recall of 1.4 million units. The increasing number of connected devices being used is expected to result in at least one smart device failure that could result in physical harm in 2016.

E. Researchers Discover a Not-So-Smart Flaw In Smart Toy Bear
The Smart Toy Bear, made by Fisher-Price for children ages 3 to 8, is "an interactive learning friend that talks, listens, and 'remembers' what your child says and even responds when spoken to". This is done by connecting to the Internet through a WiFi connection. The security hole was found in its app, by Boston-based researchers, which serves as a link that allows parents to communicate with system servers. The flaw, according to researchers, fails to secure data stored in a remote server, thus allowing any hacker or bogus customer to gain easy, unauthorized access. Further, cybercriminals could potentially use the flaw to their advantage to mine information from a target family and lure them into giving more with a phishing attack.

IV. IOT THREAT INVESTIGATION

While there are fewer IoT security incidents reported due to the lack of public reporting, we can see patterns in these incidents in terms of the potential impacts. In fact, according to SANS 2014 survey, "Breaches on the Rise in Control Systems," it indicates that IoT intrusions are increasing. This year almost 27 percent of the respondents indicated a breach or infection in their control system environments, up from 20 percent the previous year. Another 13 percent had suspected breaches.

A. Common Attacks
IoT is all about connecting and networking devices that up until now have not necessarily been connected. This means that all of those devices, whether it is a brand new connected refrigerator or a connected vehicle, are creating new access point to the network and therefore posing an increase in security and privacy risk. While the type of attacks often follow the same procedure as before, depending on the ecosystem, the device and environment, the available protection level and many more,impact of each attack can vary dramatically.
Following are some of the most common cyber-attacks, and a description of to an unprecedented rise in the level of risk with the possibilities of the IoT.

I. Botnets:
A botnet is a network of systems clubbed together for remotely taking control and distributing malware. Which is controlled by botnet operators via Command-and-Control-Servers (C&C Server), they are used by criminals on a large scale for many things: stealing private information, exploiting online-banking data, DDoS-attacks or for spam and phishing emails.
With the advance in IoT, many objects and devices are atrisk, or are already being part of'thingbots' – a botnet that assimilate independent connected objects. Botnets as well as thingbots consist of many different devices, all

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

connected to each other via computers, laptops, smartphones and tablets to now also those "smart" devices. These things have two key characteristics in common: they are internet enabled and they are able to transfer data automatically via a network. Anti-spam technology can spot accurately if one machine sends thousands of similar emails, but it's a lot harder to find if those emails are being sent from different devices that are part of a botnet. They all have one aim: that the platform crashes while struggling to handle huge amount of requests.

IoT devices can prove Shangri-Lafor DDoS bots for various factors,beginning with that they commonly run embedded versions of the Linux operating system, which also means that they lack in security. These devices usually have full access to Internet, with no limitations or filtering on bandwidth, and can be easily jeopardized because manufacturers often re-use parts of software and hardware in different domains of devices.

Arbor Networks researchers revealed LizardStresser, (DDoS) botnet was recently used in attacks as large as 400 gigabits per second (Gbps) that leverage the power of IoT devices.

II. Man-in-the-Middle Concept:

The man-in-the-middle concept is where an attacker or hacker is looking to interrupt and breach communications between two separate systems. It can be a dangerous attack because it is one where the attacker secretly intercepts and transmits messages between two parties when they are under the belief that they are communicating directly with each other. As the attacker has the original communication, they can trick the recipient into thinking they are still getting a legitimate message. Many cases have already been reported within this threat area, cases of hacked vehicles and hacked "smart refrigerators".

These attacks can be extremely dangerous in the IoT, because of the nature of the "things" being hacked. For example, these devices can be anything from industrial tools, machinery, or vehicles to innocuous connected "things" such as smart TV's or garage door openers.

III. Data & Identity Theft:

The main blueprint of identity theft is to amass data. General data available on the internet, in combinationwith social media information, and the add-on data from smart watches, fitness trackers and smart meters, smart fridges and many more give a great all-round idea of personal identity. The more details can be found about a user, the easier and the more sophisticated a targeted attack aimed at identity theft can be.

IV. Social Engineering:

Social engineering is to manipulate people so they give up confidential information. The types of information that criminals seek can vary, but while targeting individuals, the criminals are usually trying to trick the user into giving them passwords or bank information. Or they could be trying to find an entry point of a computer in order to secretly install malicious software that will then give them access to personal information, as well as giving them control over the computer. Typically, social engineering hacks are done in the form of phishing emails, which seek to have user give away information, or redirects to websites like banking or shopping sites that look legitimate, alluring user to enter their details.

V. Denial of Service (DoS):

DoS attack happens when a service is unavailable, that would usually work. There can be various reasons for the unavailability, but it usually associatedwith infrastructure that cannot endure due to capacity overload. In a Distributed Denial of Service (DDoS) attack, a large number of systems malignantly attack single target. This is often done by a botnet, where various devices are programmed (often unknown to the owner) to request a service at the same time.

In contrast to hacking attacks like phishing or brute-force attacks, DoS doesn't normally try to steal information or leads to security loss, but the loss of reputation for the affected company can still worth a lot of time and money. Often a DoS attack lends itself to activists and blackmailers.

B. Threat Categorization and Their Best Practice.

Potential attacks against the Internet of Things can be sorted into three primary categories based on the target of the attack—attacks against devices, attacks against the communication between devices and masters, and attacks against the masters.

I. Attacks against IoT Devices:

To a potential attacker, a device presents an interesting target for several reasons. Firstly, many of the devices will have an inherent value by the simple nature of their function. For example connected security camera could provide valuable information about the security posture of a given location when compromised.

Best Practice: Securing the Internet of Things requires device ID certificates to be issued to each device at the point of manufacturing to establish identity and facilitate authentication to service and other devices.

II. Attacks against Communications:

Common method of attack involves monitoring and modifying messages as they are communicated. The volume and sensitivity of data traveling the IoT environment makes these types of attacks especially dangerous, as messages and data could be intercepted, captured, or manipulated while in transit. All of these threats jeopardize the trust in the information and data

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

being transmitted, and the ultimate confidence in the overall infrastructure.
Best Practice: As sensitive data travels through the cloud and IoT environment, it should be encrypted to prevent interception. Likewise, stored data should be transparently and impeccably encrypted to prevent theft

III. Attacks against the Masters of Device:
For every device or service in the Internet of Things, there must be a master. The master's role is to issue and manage devices, as well as expedite data analysis. Attacks against the masters (including manufacturers, cloud service providers, and IoT solution providers) have the potential to inflict the most amount of harm. These parties will be entrusted with large amounts of data, some of it highly sensitive in nature. This data also has value to the IoT providers because of the analytics, which represent a core, strategic business asset—and a significant competitive vulnerability if exposed.
Best Practice: Code signing of firmware/software updates using code signed with digital certificates. Additionally, all communication with devices in the field should use SSL (Secured Socket Layer) certificates.

C. Attack Patterns
A number of patterns emerge from observing the IoT security threats.

I. Targeted Attacks
In IoT, many of the attacks are dogged and targeted, where attackers use multiple vectors of attack to gain a stronghold within the network from which to move laterally. In this environment network managers can't depend on the security strategy in which they merely get rid of the easy rewards of security susceptibilities hoping that attackers would quickly move on to the next easy target.

II. Collateral Damage Risk
The growth of IoT specific malware, even when designed for a targeted attack, often employs self-propagating infection techniques, even unintended targets are often compromised. Significant exposure of new susceptibilities (and old but unpatched/unaddressed vulnerabilities), and even zero-day exploits mean that these concerns will only increase.

III. Social Engineering and Phishing
Many of the targeted attack campaigns use employees to gain an initial foothold on a network. This is also a common initial vector for malware.

IV. Remote Access
The distributed nature of IoT controllers, as well as the common outline where a vendor is used to manage a system, combined with components that often don't support modern security controls or protocols, means that remote access is a common vector of attack. Many of the documented incidents use this as a primary attack method.

D. Patterns in IoT Network Vulnerabilities
According to ICS-CERT, based on the security assessments it conducted in FY14, a significant number of vulnerabilities it found (28 percent) on critical infrastructure networks was clustered in six areas (in terms of NIST 800-53 control families):

I. Boundary Protection:
Lack of firewall control in IoT networks, include lack of sufficient logical separation from enterprise IT/OT networks or Internet.

II. Information flow enforcement:
Lack of technical access control mechanisms, such as firewalls, routers, proxies, gateways, and tunnels to control the flow of information in an IoT network and ingress/egress between networks in accordance with policy.

III. Remote Access:
Weak security controls for remote access including internet facing systems, vendors and contractors, VPN configurations, the use of personal devices and vulnerable OSs.

IV. Least privilege:
Provisioning users with elevated privileges beyond the minimum required, such as the use of administrator accounts for routing functions, creates a risk for both unintentional and malicious incidents.

V. Physical Access Control:
Not securing physical access to IoT equipment.

VI. Security function isolation:
Implementation of flat network topologies without multiple layers of security controls simplify exploitation while making monitoring connectivity between systems of different trust levels more difficult.

V. CHALLENGES

Following are the challenges for implementing security in IoT embedded devices, based on their specialized nature.

Critical functionality: In addition to devices, systems and appliances in a home, embedded devices also are found controlling the world's transportation infrastructure, the utility grids, communication systems and many other capabilities relied upon by modern society. Interruption of these capabilities by a cyber-attack could have catastrophic consequences.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

Replication: Once designed and built, embedded devices are mass produced. There may be thousands to millions of identical devices. If a hacker is able to build a successful attack against one of these devices, the attack can be replicated across all devices.

Security assumptions: Many embedded engineers have long assumed that embedded devices are not targets for hackers. These assumptions are based on outdated assumptions including the belief in security by obscurity. As a result, security is often not considered a critical priority for embedded designs. Today's embedded design projects are often including security for the first time and do not have experience and previous security projects to build upon.

Not easily patched: Most embedded devices are not easily upgraded. Once they are deployed, they will run the software that was installed at the factory. Any remote software update capability needs to be designed into the device to allow security updates. The specialized operating systems used to build embedded devices may not have automated capabilities that allow easy updates of the device firmware to ensure security capabilities are frequently updated. The device itself may not have the IO or required storage that allows for updating to fight off security attacks.

Long life cycle: The life cycle for embedded devices is typically much longer than for PCs or consumer devices. Devices may be in the field for 15 or even 20 years. Building a device today that will stand up to the ever evolving security requirements of the next two decades is a tremendous challenge.

Proprietary/industry specific protocols: Embedded devices often use specialized protocols that are not recognized and protected by enterprise security tools. Enterprise firewalls and intrusion detection system are designed to protect against enterprise specific threats, not attacks against industrial protocols.

Deployed outside of enterprise security perimeter: Many embedded devices are mobile or are deployed in the field. As a result, these devices may be directly connected to the Internet with none of the protections found in a corporate environment.

VI. CONCLUSION

At its core, IoT is all about connecting and networking devices that up until now have not necessarily been connected. This means that all of those devices, whether it is your brand new connected refrigerator or your connected vehicle, are creating a new entry point to the network and therefore posing an increasing security and privacy risk.Hackers could reduce the temperature on smart thermostats to freeze water pipes, crash airplanes and cars, and even attack connected medical devices that are required to keep people alive.

The researchers have a rich record of already exposed susceptibilities in the web interfaces of IoT devices, and to no one's surprise, the record contains over 9000 vulnerabilities. Since many of the discovered vulnerabilities have already been disclosed, the impact on end user security is potentially much higher because some users ignore firmware updates available for their devices. So there is an urgent need to change our mindset towards this storm of IoT. Security steps should become easily accessible, awareness should be raised not only among the users but also among the companies manufacturing these products. And during the design and implementation phases, individuals and companies should make use of proven, reliable tools and libraries. Amateur security solutions should be avoided and experts' consideration should be involved primarily. IoT networks need to be worried about both sophisticated targeted attacks from competitors and nation-states, as well as accidental misuse from employees, contractors, and vendors.

REFERENCES

[1] http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[2] http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#653621b6828
[3] https://safenet.gemalto.com/data-protection/securing-internet-of-things-iot/
[4] http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/internet-of-things/attack-scenarios
[5] https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot/
[6] http://www.darkreading.com/endpoint/another-iot-dominated-botnet-rises-with-almost-1m-infected-devices/d/d-id/1326776
[7] http://www.forbes.com/sites/forbestechcouncil/2016/09/01/what-everyone-should-know-about-the-internet-of-things/#521876184faa
[8] http://www.prnewswire.com/news-releases/cyberx-reveals-the-first-iot-worm-aimed-at-cctvs-589852131.html
[9] http://www.informationsecuritybuzz.com/hacker-news/ripper-malware-attacks-thai-atms/
[10] https://techcrunch.com/2016/08/16/how-to-prevent-your-iot-devices-from-being-forced-into-botnet-slavery/
[11] http://www.google.co.in/