The IoT as a Growing Threat to Organizations

There is a new cyberthreat that is growing with the potential to have major impact on information security and personal privacy. This threat is associated with the Internet of Things (IoT), and it is growing exponentially. By 2020, there will be 24 billion devices connected to the Internet.[1] Organizations are expected to spend US$6 billion globally by the year 2023 on cybersecurity for IoT devices.[2] The growth in purchasing these IoT products will drive the cost down as they are mass-produced (an example of supply and demand), which encourages sales and increases the reach and presence of the IoT cyberthreat.

> “AS IOT DEVICES BECOME A BIGGER PART OF PERSONAL LIVES, THEY MAY BEGIN TO AFFECT ENTERPRISE SECURITY.”

Home and personal computing (i.e., non-business) devices are expanding the cyberthreat, and the growing IoT infrastructure and network-capable devices can be compromised and used as tools to launch cyber/digital attacks against organizations. The use of compromised non-business Internet-connected devices is a new and growing cyberthreat vector. With the growth of new chips and automation of non-digital devices that can be accessed remotely (via the Internet), hackers have provided a relatively safe place for malware to reside with little concern for removal, mostly because the device owners do not perform digital forensics or malware removal.

The overall market trend is to digitally automate devices that have an on/off button and increase the digital presence so that the makers of the devices can obtain digital statistics to better understand their customers, make better products and reach a bigger market. This is part of the big data analytics movement.

As IoT devices become a bigger part of personal lives, they may begin to affect enterprise security. Understanding the impact that IoT devices used at home and in the office may have on security is crucial to ensure that enterprises remain secure.

IoT Botnet Components

IoT botnets are the source of the threat that forms the basis for distributed denial-of-service (DDoS) attacks, which is currently the predominant malicious use of IoT devices.[3] IoT bots/botnets have the following components:

- Malware planted on the compromised device (also known as the agent)
- Command and control (C&C) servers that control the agents/bots
- Scanners that find vulnerable devices and obtain their addresses and security weaknesses
- Storage server(s) that hold the compromised device addresses, access credentials and vulnerabilities (i.e., device inventory)
- Loaders that download the malware onto the devices
- Distribution servers that contain the malware that is loaded onto the agent device

Larry G. Wlosinski, CISA, CRISC, CISM, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL v3, PMP
Is a senior consultant at Coalfire-Federal with more than 19 years of experience in information security and privacy. He has been a speaker on a variety of IT security and privacy topics at US government and professional conferences and meetings, and he has written numerous articles for the *ISACA® Journal*, magazines and newspapers.

IoT Device Vulnerabilities

With the explosion of IoT, there has been a repetition of past automation information security mistakes, two of the key mistakes being that information security and privacy are not included in the initial design of the device.

New custom communication protocols are being created by manufacturers that differ in communication frequency, range and data rates. If devices are near each other and have the same frequency and data rate, they could possibly interfere with each other, causing a denial of service for both devices. They may also cause unexpected events if the devices were not thoroughly tested to ensure that they could handle variations (intentional or not) to the protocol.

Computer chips are being made with little or no thought for flaw correction. Products are being rushed to market without adequate security safeguards and testing, and device and/or software compromise and misuse is not a concern. Access controls (e.g., passwords, biometric authentication) are not always required or are not required to be changed on first access. Data communication is not encrypted, and data at rest (or in transit) are not encrypted.

IoT Information Security Incidents

Depending on the malware loaded, the compromised devices can perform DDoS attacks, launch emails, spread/replicate to other devices, change the device configuration and privileges, launch other malware, conduct spam campaigns, hide network traffic, generate ad-revenue click fraud, insert backdoors, conduct credential-stuffing attacks (to gain network access), lock the device to prevent other malware from infecting it for other purposes, and steal data, to mention a few malicious purposes.

Attacks against IoT devices were up 600 percent in 2017 compared to 2016. The top IoT honeypot devices attacked were the router (33.6 percent), digital video recorder (23.2 percent) and the network (9.3 percent). The top services attacked are Telnet (50.5 percent; ports 23 and 2323), HTTP (32.4 percent; ports 80 and 8080), and HTTPS (7.7 percent; port 443).[4] IoT devices are now mainstream targets for hackers.

IoT-related cybersecurity vulnerabilities and incidents that have affected enterprises are not new. They have been around for a few years and have become an additional target to exploit for malicious purposes. The Mirai Botnet, for example, which leveraged a Dyn DDoS attack, used known usernames and passwords to log in and infect devices (e.g., digital cameras, DVR players) with malware. This botnet contains 10 predefined attack vectors. Mirai is open-source, meaning hackers can potentially mutate, customize and improve it—resulting in an untold variety of new attack tools that can be detected only through intelligent automation. Mirai caused Twitter, *The Guardian*, Reddit, CNN, Etsy, GitHub, Shopify and SoundCloud to go down. Cybercriminals disrupt services that affect many organizations including Amazon, PayPal, Netflix, Spotify and Twitter.[5, 6]

There have been other incidents as well. The AtomBombing Code Injection Attack performed browser-based attacks, accessed encrypted passwords and took screenshots of a user's system.[7, 8, 9] The Hajime bot booted existing bots, closed ports and hid in devices.[10] The Reaper bot had nine methods of exploiting device vulnerabilities. It affected Linksys, GoAhead and NetGear devices.[11] These are but a few of the instances where IoT devices have been exploited for malicious purposes. It is easy to infect or compromise an IoT device that has an operating system and a digital storage capability if it has no defenses.

Vulnerabilities of IoT Office Devices

Some office devices can be considered within the scope of IoT. Devices that are in the office can be the source of threats that increase risk to the organization.

> “IT IS EASY TO INFECT OR COMPROMISE AN IOT DEVICE THAT HAS AN OPERATING SYSTEM AND A DIGITAL STORAGE CAPABILITY IF IT HAS NO DEFENSES.”

Wireless access points (WAPs) can transmit data in the clear. WAPs are normally only provided by and for the organization, but WAPs from other enterprises (or malicious individuals) can be nearby and can provide a means of entry into the network. If the transmitted business data are sensitive, the risk can be high. To prevent the loss of transmitted data, awareness training programs to instill vigilance against wireless vulnerabilities should be implemented.

Computer tablets can contain all types of office data. Their connection to the organization's network makes them a potential point of entry for cybercriminals. For these devices, the risk is at least moderate because the data could be valuable. Tablets need to be monitored in the same ways as computers and smartphones.

Workstations and laptops with webcams, microphones and/or speakers can capture organizational and personal data. These computing devices can be assessed as a moderate risk because, although the time and effort needed to obtain something valuable is small, the number of devices in the enterprise makes for a large attack surface. To minimize the risk, users should be trained to be vigilant; they should disable any unneeded device features (especially in sensitive work areas); and the organization should establish a policy and provide guidance on device deployment, usage and rules of behavior.

Wireless printers, copiers and scanners can contain many types of data including contracts, organizational and time-sensitive data, and personal information. A wireless printer and/or copier can be used as an unauthorized network bridge allowing access to the network. They contain operating systems and custom software on their internal hard drives. Hackers can siphon off the device's memory to access stored jobs. Additionally, network device passwords can be compromised if the printer utilizes standardized role-based permissions for similar device types. The risk of exploitation or wireless printers is moderate because there is a connection to the organization's network (i.e., intranet). Organizations need to monitor and secure these devices as much as possible to limit access and exposure.

Smart TVs in the office can be connected to the intranet and/or Internet, which leads to the potential of them being a weakness that can be exploited. The likelihood of data loss and associated risk is low for them because smart TVs may not be privy to sensitive data. They can, however, be used as a malware launching point for a data breach. They need to be included in the security inventory and configured securely.

Smartboards that capture white board information can capture business plans, data analyses, metrics and process information. If connected to the enterprise network, smartboards can capture data for future extraction and unauthorized use. The risk to the business is low, however, because the data are usually cryptic, which may make data accessed unusable. They also should be part of the security inventory and configured accordingly.

Security cameras that are in and around the building may be IP-based and connected to the network. If this is the configuration and the system is Internet-access capable, they could allow for remote spying. The supporting servers (or appliances) can be hacked and infected with malware. The cameras are considered to be a low-risk threat because the information is localized and video exposure of sensitive or proprietary information would be very small. These network endpoints need to be secured or purchased with data security features.

> “THE THREAT IS GROWING BECAUSE HACKERS ARE SWITCHING FROM USING SERVERS AND LAPTOPS (WHICH ARE MORE SECURE NOW) TO THE UNPROTECTED IOT DEVICES TO INFECT AND BE A MALWARE LAUNCHING POINT.”

Smart devices (e.g., smartphones, disguised recording devices) in executive office(s) can possibly capture audio and video conversations. Aside from the devices mentioned previously, executives sometimes obtain new technology for personal reasons. These devices may be able to see, listen and capture conversations including sensitive and proprietary information. These devices can normally be considered low risk because the threat is localized, but can be high if pursued by competitors or people with malicious intent. As a countermeasure, executives can be trained on the security and privacy risk associated with new technology.

Vulnerabilities of Home and Personal IoT Devices

Some home and personal IoT devices can be compromised and used as indirect launching points for a device or network infection or compromise at an organization. The more devices that exist, the bigger the threat, because it increases the methods of attack (i.e., threat vectors). Users must be vigilant to the methods of the hackers and the weakness of new technology, otherwise the past will be repeated and the ability to combat hackers will get worse. The more footholds the hackers have, the worse it gets.

Smart/cell phones and tablets (with vulnerable applications) contain personal email addresses, schedules, conversations and preferences. Malicious wireless access can affect privacy, and devices could be infected to be launch points for an attack. There is a high risk to organizations if these devices also connect to an enterprise network. As a result, organizations must keep all software (e.g., security, applications) and patches up-to-date, establish a bring your own device (BYOD) policy, and not allow connections to the organization's network. **Figure 1** shows the risk associated if certain home IoT devices are allowed to connect to the enterprise network.

Many of these devices do not hold information that could be of financial value, but can, in some cases, be of value for malicious use. The threat is growing because hackers are switching from using servers and laptops (which are more secure now) to unprotected IoT devices to infect and be a malware launching point. The growing cyberthreat of personal IoT devices is a result of the growing number of devices that can be utilized for malicious purposes (i.e., gain access, spread the malware, conduct DDoS attacks, obtain sensitive and/or personal data).

General IoT Concerns

Sometimes securing IoT devices in the working environment cannot be done. These problems may not be fixable, but the device capability can be remedied by obtaining newer, and possibly more secure, models. Awareness and research are important because organizations and individuals may not have the funds to replace devices with more secure versions.

Software patching is the first problem area. Sometimes products are sold with old and unpatched embedded operating systems and software. Some devices are designed to minimize manufacturing costs by incorporating chips with limited storage with the result that they cannot be updated or patched. Additionally, device purchasers often fail to change passwords on the devices. All these oversights provide an opportunity for device exploitation.

New and unique communication standards are being created by vendors with no consideration for

Figure 1—Risk of Connecting Personal IoT Devices to the Organization's Network

Device	Associated Risk	Security Tips
Smart assistants, e.g., Amazon's Alexa, Apple's Siri	• Collect highly sensitive data, and what is said could be recorded and retrievable • May become entry point for attack	• Avoid bringing these devices into offices.
DVRs	• May be compromised and used to launch DDoS attack • Could exploit data for malicious purposes such as blackmail for business secrets, e.g., marketing plans, new products in development, mergers	• Monitor for suspicious activity and reboot (i.e., turning off and on) if unusual activity is observed to clear device memory.
Home automation, e.g., baby monitors, appliances, cybertoys, alarm systems for windows and doors	• Many lack ability to be patched, so they are often targeted by hackers	• Replace insecure or old devices with more secure models.
Routers and firewalls	• Could be configured to prevent updates needed to secure devices • Susceptible to man-in-the-middle (MITM) attacks)	• Ensure that they are securely configured or replaced with routers and firewalls that have better security.
Wearable devices, e.g., connected medical devices, augmented reality devices	• May be used as launching point into network if device is not secured	• Develop policy regarding wearable devices in the workplace.

security. Device manufacturers create unique communication protocols[12, 13, 14] that can inhibit interoperability with other/management systems. The interference with established communication protocols and defined actions could be disrupted. The fact that wireless capabilities are growing and evolving could evolve into interruptions that affect mobile computing devices and mobile wireless devices such as programmable cars and drones. Hackers are exploiting communication standards that do not have security considerations.[15]

The IoT infrastructure is another problem area because there is no single required standard for device-to-device authentication. There is no standard on linking devices securely to cloud services, and there is little or no protection at the software and infrastructure levels.

The control of devices lost, stolen or discarded is another problem area. If there is no consideration for privacy in the design because devices may carry personal and/or sensitive information, then how can they be cleaned once they are out of the original owner's possession? The risk is that the IoT device (e.g., Alexa, Siri) has recorded sensitive information, e.g., credit card numbers, that can be used for personal gain. The ability to remotely wipe and disable services and connectivity may not exist, which provides malicious individuals an opportunity to exploit the information.

Securing IoT Devices in the Enterprise Context

The first thing an organization should do when confronted with the possibility of an IoT-related vulnerability is to develop a bring your own device (BYOD) policy. The policy needs to address/include the following:

- Who is eligible to have a personal device for business use? Without it, there is no justification for enforcement.
- Which IoT devices are allowed (and not allowed)? Enterprise-owned IoT devices should have solid security, especially if they are connected to the network. Should approved devices be segmented on the network and have limited access or be prohibited entirely? Are exceptions/waivers allowed? What are the device registration procedures (if any)?

- Which websites or cloud services can employees access for business purposes? To manage this potential opening for malware, the enterprise should implement white and black lists at the network perimeter (i.e., firewall).
- Identify and inform employees of malicious applications that should not be installed on their devices. The more awareness, the more likely it is that the enterprise could prevent an intrusion and possible foothold for malicious activity.
- Outline the consequences of not following the organization's policy. What measures should be taken to prevent unauthorized and unexpected intrusion attempts from compromised IoT devices? Should they include device confiscation or destruction, personnel reprimand, or even personnel termination?

> “SEGMENTING (I.E., ISOLATING) IOT DEVICES INTO A SEPARATE NETWORK IS ANOTHER BEST PRACTICE, ESPECIALLY IF IT IS KNOWN THAT THEY DO NOT ADHERE TO OR HAVE SECURE AND APPROVED DATA COMMUNICATION PROTOCOLS.”

An operational business recommendation is to use a cloud service to simplify the update and management of remote devices. Centralized and standardized configuration and management of remote devices is a best practice that should be considered. Organizations should have an adequate incident response plan (IRP) and train staff on how to respond to various scenarios involving IoT devices. For example, should a device be saved and isolated in the hope of applying forensics to better understand the malware and determine ways to prevent future malicious intrusion attempts?

For overall information security and data loss prevention, data at rest and in transit should always be protected via encryption. This best practice is becoming more and more important with the increasing threat of privacy concerns and data breaches.

Finally, it is crucial to educate employees on the risk of bringing personal mobile devices to work and using them to access enterprise-owned information.

Network/Infrastructure Recommendations

Enterprises should implement network access restrictions for all IoT devices to ensure control of the devices. Segmenting (i.e., isolating) IoT devices into a separate network is another best practice, especially if it is known that they do not adhere to or have secure and approved data communication protocols. A risk evaluation should be performed for all wireless devices to ensure that they do not impact the enterprise's network computing environment. If they do, they may need to be prohibited or reconfigured. Enterprises should also create a security framework that uses public-key cryptography to authenticate communication between remote devices and gateways. This prevents the possibility of hackers gaining access to data on IoT devices and makes it difficult to send unauthorized control signals or launch DDoS attacks.

Another recommendation is to continuously monitor the network for anomalous activity and to take action to rectify any unusual activity found. Using network behavioral analysis software can detect anomalies in traffic and, when combined with automatic signature generation for mitigation, makes for an effective and quick control response.

A recommendation for network solution providers is to establish and follow a common architectural framework and a common set of communication protocols to ensure interoperability between devices. The IoT appears to be repeating history by going to market first and not considering security ramifications. Protocols for IoT devices vary by infrastructure, identification, data communications and transport, device discovery, data protocols, device management, semantic, and frameworks.[16]

Standards organizations need to get more involved. There is, however, a glimmer of hope from the IEEE Computer Society[17] and their involvement with deep learning, but it is limited to mobile devices.

Recommendations for IoT Devices

There are many best security practices for mobile devices, and they apply to IoT devices as well. They include not obtaining/purchasing IoT devices that cannot have their software, passwords or firmware updated. IoT devices should be configurable so they boot up securely. Users must be able to change the account name and password from the standard factory default credentials that hackers can obtain. Device owners should not share serial numbers, IP addresses and other sensitive information regarding IoT devices on social networks. Organizations should only install approved software on devices that can access the network.

Software best practices also apply. If possible, enterprises should make sure any security software that is installed is up-to-date and active on any devices that are connected to the enterprise's network (or being used to access enterprise data). IoT devices should always be patched with the latest software and firmware updates to mitigate vulnerabilities. Devices that are accessible over the Internet should be used to allow updates and patches. Security teams should be aware and always checking the latest information on discovered vulnerabilities for all IoT devices and they should check and upgrade firmware as soon as notified.

Additionally, vendors should produce products that permit the disabling of features (e.g., Plug and Play, Telnet) so that those features require activation by users only if needed.

Conclusion

IoT devices have vulnerabilities, they are being used as launching points for malware attacks and system compromises, and they exist in the home and in the office, and infections and device compromises are spreading to any device that can store data and execute software.

The other bad news is that these IoT devices are in their infancy when it comes to information security and privacy. However, there are steps that can be taken to make the work environment more secure and capable in protecting data and personal information. Awareness, vigilance and removal of nonsecure devices are at the top of the list. Implementing these steps will help secure the organization and the home.

Endnotes

1 Business Insider Intelligence, "Here's How the Internet of Things Will Explode by 2020," 28 April 2016, *https://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-4-28*

2 Business Wire, "Juniper Research: IoT Security Spend to Reach $6 Billion by 2023, Growing 300% from 2018," 11 July 2018, *https://www.businesswire.com/news/home/20180711005040/en/Juniper-Research-IoT-Security-Spend-Reach-6*

3 Bitdefender, "78% of Malware Activity in 2018 Driven by IoT Botnets, NOKIA Finds," *https://www.bitdefender.com/box/blog/iot-news/78-malware-activity-2018-driven-iot-botnets-nokia-finds/*

4 Symantec, *Internet Security Report (ISTR)*, vol. 23, March 2018, *http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf*

5 Woolf, N.; "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say," *The Guardian*, October 2016, *https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet*

6 Greene, T.; "How the Dyn DDoS Attack Unfolded," *NetworkWorld*, 21 October 2016, *https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html*

7 Liberman, T.; "Atombombing: Brand New Code Injection for Windows," Ensilo, 27 October 2016, *https://blog.ensilo.com/atombombing-brand-new-code-injection-for-windows*

8 Liberman, T.; "Atombombing: A Code Injection That Bypasses Current Security Solutions," Ensilo, 27 October 2016, *https://blog.ensilo.com/atombombing-a-code-injection-that-bypasses-current-security-solutions*

9 Khandelwal, S.; “Dridex Banking Trojan Gains ‘AtomBombing’ Code Injection Ability to Evade Detection,” *The Hacker News*, 1 March 2017, *https://thehackernews.com/2017/03/dridex-atombombing-malware.html*

10 Leyden, J.; “Mysterious Hajime Botnet Has Pwned 300,000 IoT Devices,” *The Register*, 27 April 2017, *https://www.theregister.co.uk/2017/04/27/hajime_iot_botnet/*

11 Greenberg, A.; “The Reaper IoT Botnet Has Already Infected a Million Networks,” *Wired*, 20 October 2017, *https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/*

12 RS Components, “11 Internet of Things (IoT) Protocols You Need to Know About,” 20 April 2015, *https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about*

13 Kisi, “6 Communication Protocols Used by IoT,” Kisi Blog, 30 May 2018, *https://www.getkisi.com/blog/internet-of-things-communication-protocols*

14 Al-Sarawi, S.; M. Anbar; K. Alieyan; M. Alzubaidi; “Internet of Things (IoT) Communication Protocols: Review,” 2017 8th International Conference on Information Technology (ICIT), July 2017, *https://www.researchgate.net/publication/320614944_Internet_of_Things_IoT_Communication_Protocols_Review*

15 Wlosinski, L.; “Mobile Computing Device Threats, Vulnerabilities and Risk Factors are Ubiquitous,” *ISACA® Journal,* vol. 4, 2016, *https://www.isaca.org/archives*

16 Postscapes, “IoT Standards and Protocols,” 1 January 2019, *https://www.postscapes.com/internet-of-things-protocols/*

17 Cameron, L.; “Deep Learning Meets the Internet of Things: How New Frameworks Will Drive the Next Generation of Mobile Apps,” IEEE Computer Society, *https://www.computer.org/publications/tech-news/research/deep-learning-iot-frameworks-next-generation-mobile-apps*