



Internet of Things Security White Paper 2018

Media Analysis
Social Media
Statistics



TABLE OF CONTENT

White Paper to address areas of concern for IoT security. Each section addresses a different area of the IoT ecosystem, and where potential security risks could come from.

01 SECURITY: WHAT'S ALL THIS HYPE?	2
02 A SUPERHERO WITH A VULNERABILITY	2
03 IOT ARCHITECTURE: WHERE TO GET STARTED	3
04 COMMUNICATION PROTOCOLS: THE WEALTH AND WOES	4
05 IOT HARDWARE: HACKERS' FASCINATION WITH YOUR DEVICE	5
06 THE INTERNET CAN BE A SCARY PLACE	6
07 HARDWARE STRENGTH IS RISKY BUSINESS	7
08 WRAPPING UP SECURITY FOR THE INTERNET OF THINGS	8
09 GLOSSARY	9
10 SOURCES	10

SECURITY What's all this hype?

In 2014, the Internet of Things (IoT) had a global market of \$2.99T (trillion); by 2020, that number will reach \$8.9T, "...attaining a 19.92% Compound Annual Growth Rate."¹ Likewise, the number of deployed devices will increase from 6.6 billion in 2016 to 22.5 billion in 2021.² As the IoT market grows with device deployments, the concern over security will grow with it; in fact, worldwide spending on IoT security will be \$547.2 million in 2018 alone, an increase from \$433.95 in 2017.³

A SUPERHERO WITH A VULNERABILITY

The Internet of Things is the interconnectedness of devices via the Internet. Watches, coffee machines, refrigerators, thermostats, and cars, these once offline items are quickly speaking to the Internet, driving technological innovation. Composed of Internet-enabled hardware, these Things perform commonplace computing tasks, although these devices can now speak to, and receive instructions from, the Internet.

As Things (smart devices, or Internet-enabled embedded devices) repurpose technology available in PC's and servers, emblematic tech threats are presented as IoT security considerations. Such threats include:

Communication protocols security

Data sniffing and spoofing

Denial-of-Service

Man-in-the-Middle attacks

Brute forcing

Weakened hardware

Weak encryption implementation

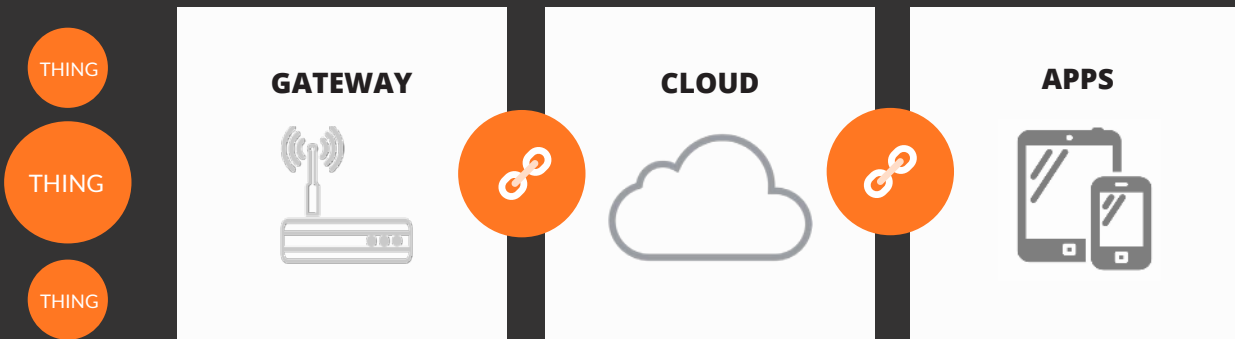
As the number of devices grows, so should our vigilance in understanding IoT security.

IOT MAKES A
CONNECTED
WORLD POSSIBLE.
THAT'S WHAT
ALL THE HYPE'S
ABOUT. SO LET'S
DIVE INTO THE
REASONS WHY
YOU NEED TO
SECURE YOUR
COMPONENTS
BEFORE YOUR
NEXT PROJECT



Where to get started

NO MATTER HOW YOU IMPLEMENT, IT 'S IMPORTANT TO NOTE THAT EACH LEVEL OF THE ARCHITECTURE HOLDS ITS UNIQUE VULNERABILITY CONCERNS.



To understand IoT security, we must understand IoT architecture. Although its implementation can vary, the general schema can be described from the human perspective: a user uses a control device to communicate with a cloud service, which broadcasts through the Internet to reach a local network, which in turn communicates with a Thing.⁴

In short, a Thing utilizes a gateway in order to reach the Internet, where such gateways can exist as general-purpose network routers, smart phones, and Bluetooth routers. In each case, the gateway is the communication link between a smart device and any endpoint elsewhere on the Internet, out of the local network (the realm between the Thing and the gateway). Here is where we run into one of our most prolific security concerns.

FIGURE 1
COMMUNICATION FROM THING TO INTERNET AND VICE VERSA.

Communication Protocols

the wealth and woes

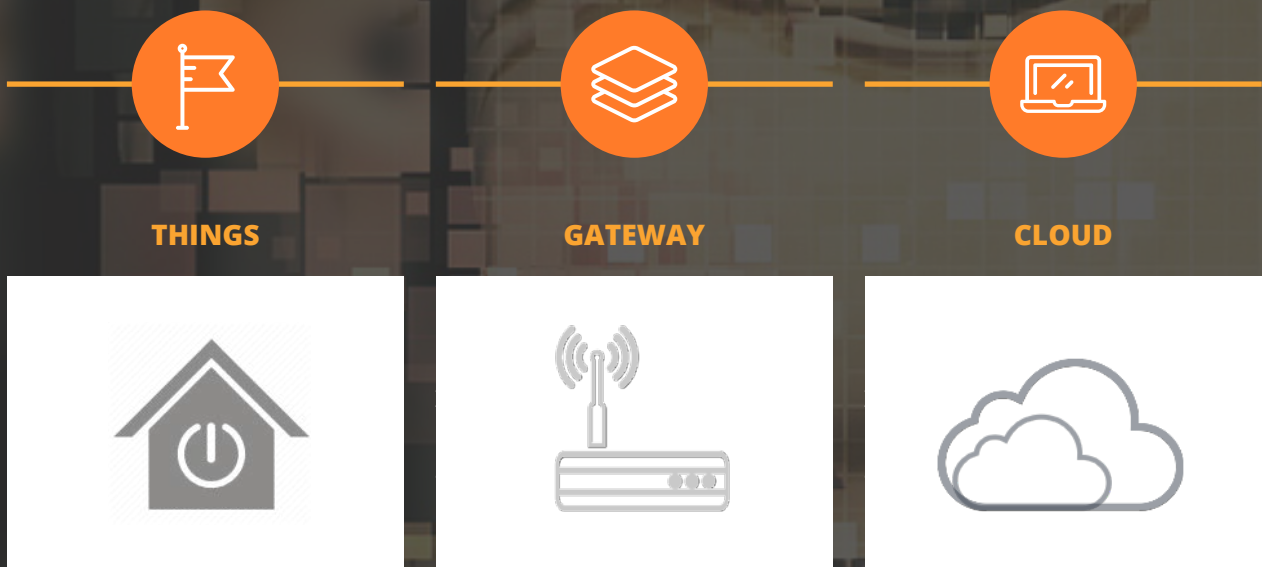
THE INTERNET OF THINGS EXPOSES ITSELF TO A WEALTH OF COMMUNICATION PROTOCOLS.

This is both a benefit and a concern.⁵ Due to the profusion of protocols, we have a wealth of technology to utilize, affording developers flexibility. Each protocol requires an intimate knowledge of security in order to implement. Fortunately, it's easy to get that knowledge through some research.

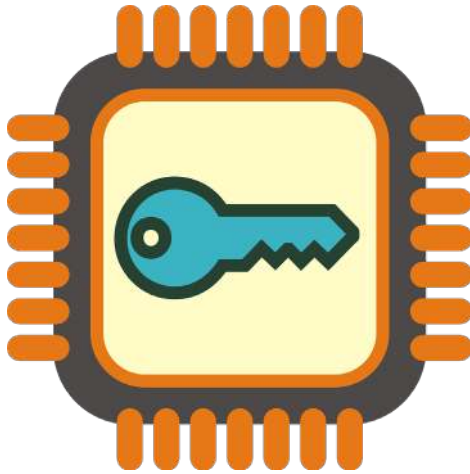
As such, by using any number of protocols, security architects and developers must understand the security pitfalls associated with each protocol.

FIGURE 2

POINTS OF RISK EXIST BETWEEN THE TRANSFER OF DATA BETWEEN A THING TO THE GATEWAY, AND FROM THE INTERNET TO THE GATEWAY. COMMUNICATION TAKES PLACE VIA COMMUNICATION PROTOCOLS.



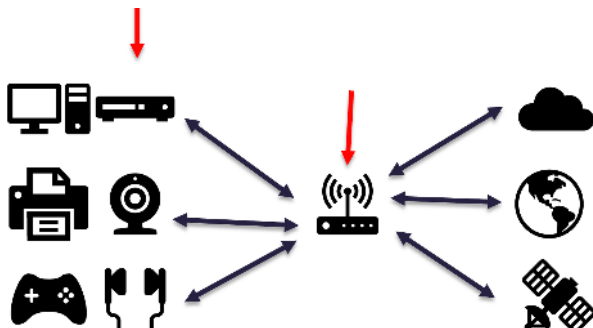
Hacker's Fascination With Your Device



To employ these protocols, we defer this task to hardware: either from our smart device or from our gateway. Smart devices are made of single-board microcontrollers, such as Arduino, Intel Galileo, and Beagle. Each single-board microcontroller is manufactured with similar components found in personal computers, such as processors, RAM, and WiFi-enabled network interface controllers.

Gateways, such as general-purpose network routers, smart phones, and Bluetooth routers, ship with their own hardware components that uniquely facilitate data transmittance. The security risks associated with each component pose separate security considerations.

TO HELP VISUALIZE THESE CONCEPTS, LET US EXPLORE AN EXAMPLE. A COMMON IOT SCENARIO IS FOR OUR SMART DEVICE TO MAKE WEB REQUESTS USING HTTP. SOME OF THE QUESTIONS WE MAY ASK ARE:



What security concerns exist with HTTP?

What are known HTTP security pitfalls, and how are they mitigated?

What hardware does our smart device use to make HTTP requests?

Which hardware options are available for facilitating these requests and how is a solution made?

How do we further secure our environment based on these choices?



The Internet can be a scary place

Smart devices communicate to, and receive instructions from, the Internet; if our device can speak outwardly, then both intended and unintended commands can communicate to our device. Aiding to this concern, where communication occurs is a chance for malicious interception and manipulation of data delivery; IoT is no different.

PROTECTING SMART DEVICES
FROM COMMUNICATION VIA
THE INTERNET IS IMPORTANT



SUBJECT TO SUSPICION: INPUT FROM THE INTERNET

Not all input from the Internet comes from our intended targets; it is important to create security measures that handle data input securely.



SECURITY: HANDLE INPUT SAFELY & STOP MALICIOUS ACTIVITY

Malicious activity include as Denial-of-Service, data sniffing and spoofing, brute forcing, Man-in-the-Middle, and SSL and DNS-based attacks.

Man-in-the-Middle Attack

an example

Let's take a look at one of the specters haunting IoT; Man-in-the-Middle, or MITM, attacks. These attacks occur when someone "[intercepts] a communication between two nodes" and usurps it maliciously.⁷

According to McAfee, browser-based MITM attacks (called Man-in-the-Browser, or MITB) comprised 25% of the top network attacks in 2016⁷, 8; IoT infrastructure incorporating web applications are therefore targets for these attacks.

Likewise, Denial-of-Service (DoS) and Secure Sockets Layer (SSL) attacks, components of MITM, constituted 33% and 6% of 2016 network attacks respectively; this amounts to 64% of network attacks in 2016 being Man-in-the-Middle.

All is not lost: common methods of protecting IoT infrastructure from MITM attacks include proper firewall configuration, regular updating of device software, and using SSL certificates and adept encryption across the system.



HARDWARE SECURITY

The internet of Things uses the same hardware as devices we know & love.

Hardware Strength is risky business

To conclude on hardware-based security, we should understand the security concerns associated with the limitation of hardware resources. Smart devices are small computers; small being the key word, this alludes to the limited power capabilities of our Things. With such limited resources are security measures capable of such resource power.⁶

The main concern here is that encryption will be hesitant to withstand high-volume brute-force attacks, as our Things will most-likely rely on swift, lightweight encryption algorithms. To prevail, these device limitations can be aided by separating devices onto various networks and by utilizing firewalls.

Wrapping Up

summary of iot security

IOT MAKES A CONNECTED WORLD POSSIBLE. THAT'S WHAT ALL THE HYPE'S ABOUT

The Internet of Things is transforming the world. Fighting malaria and growing food more efficiently,⁹ makes 22.5 billion IoT devices sound like a welcome number. As the Internet continues its distributed growth, IoT will further revolutionize the human experience; in turn, vigilant IoT security must be maintained. If secure, the IoT revolution will surely prosper.



THE HYPE

As the IoT market grows with device deployments, the concern over security will grow with it.



WHERE TO START

It's important to note that each level of the IoT architecture holds its own unique vulnerability.



COMMUNICATION PROTOCOLS

IoT exposes itself to a wealth of communication protocols.



MALICIOUS INTERNET

Protecting smart devices from communication via the internet is important.



MAN IN THE MIDDLE ATTACK EXAMPLE

MIM attacks are when someone intercepts and maliciously usurps data.



HARDWARE RISKS

The concern is when encryption is too light to repel high-volume brute force attacks.

Glossary

terms and definitions

IOT (INTERNET OF THINGS). THE DISTRIBUTED, INTERCONNECTEDNESS OF DEVICES (OR THINGS) AND THE INTERNET

THING. A device that receives and produces data in Internet of Things.

Architecture: Design and implementation of infrastructure

Brute forcing: A method of bypassing security by flooding password unlocking attempts at password-protected content

Cloud: Internet-based services

Denial of Service: An attack where the amount of information received on a device exceeds the capable amount

Gateway: Device or computer between devices and the Internet

Man-in-the-Middle (MITM): Attack where data is intercepted between the endpoint and starting point of communication

Man-in-the-Browser(MITB): A form of MITM attack that targets web browsers integrity of your devices and computers

Network: A particular grouping of computers communicating with each other on the Internet

Protocol: A specific method of communicating data across Internet-enabled computers

Secure Sockets Layer Attack: An attack that targets the SSL protocol, allowing the attack to analyze transmitted data

Service: A consumable function on the Internet that accomplishes a business task

Sniffing: Analyzing the transmittance of data across the Internet

Spoofing: Imitating a someone or something on the Internet, such as a website or device

Threat: A malicious risk that can impact the integrity of your devices and computers

Sources

1. **Louis Columbus**, 2017 Roundup Of Internet Of Things Forecasts, Forbes Media LLC, December 10, 2017 <https://www.forbes.com/sites/louiscolumnbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#48ac19b71480>

2. **Peter Newman**, The Internet of Things 2018 Report: How the IoT is evolving to reach mainstream with business and consumers, Business Insider Inc, January 12, 2017 <http://www.businessinsider.com/the-internet-of-things-2017-report-2017-1>

3. **Internet of Things** security spending worldwide from 2014 to 2018 (in million U.S. dollars), Statista Inc., 2018 <https://www.statista.com/statistics/543089/iot-security-spending-worldwide/>

4. **Anna Gerber**, Simplify the development of your IoT solutions with IoT architectures, IBM Corp., August 07 2017 <https://www.ibm.com/developerworks/library/iot-lp201-iot-architectures/>

CHECK OUT SOME OF THESE SOURCES IF YOU'RE CRAVING MORE DETAILS ON IOT SECURITY.

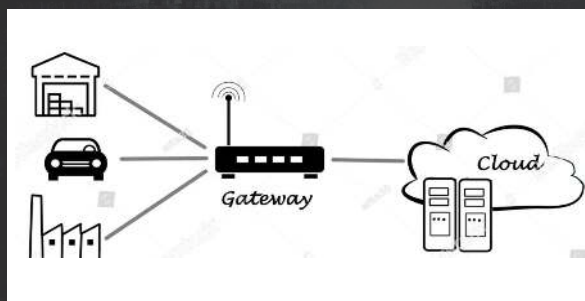
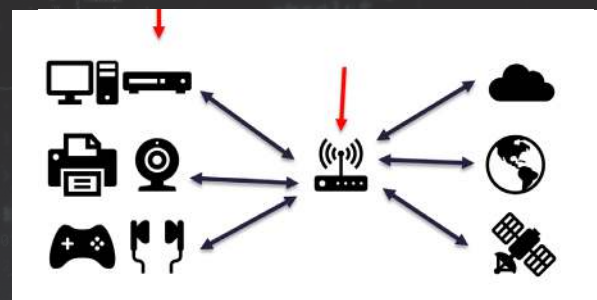
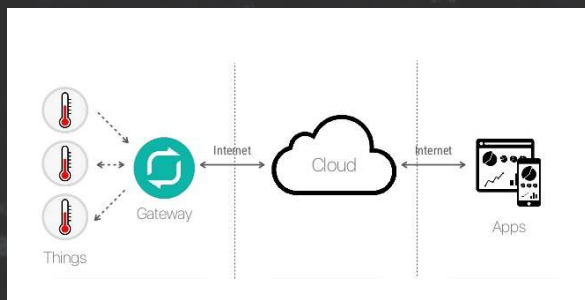
5. **Gunnar Peterson and Mark O'Neill**, Top Ten Security Considerations for the Internet of Things, Axway, 2015 https://www.axway.com/sites/default/files/resources/whitepapers/axway_whitepaper_top10_security_internet_of_things_en.pdf

6. **Anna Gerber**, Top IoT security challenges, IBM Corp., November 17, 2017 <https://developer.ibm.com/dwblog/2017/iot-security-challenges/?lnk=hm>

7. **Zoran Cekerevac, Zdenek Dvorak, Ludmila Prigoda, & Petar Cekerevac**, Internet of Things and ManInTheMiddle Attacks - Security and Economic Risks, MEST Journal, July 15, 2017 http://mest.meste.org/MEST_2_2017/10_03.pdf

8. **Christiaan Beek et al.**, McAfee Labs Threats Report September 2016, McAfee, LLC, September 2016 <https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf>

9. **Tom Kaneshige**, The Awesome Power of IoT, Informa USA, Inc., November 07 2016 <http://www.ioti.com/iot-trends-and-analysis/awesome-power-iot>



1. Communication from Thing to Internet, and vice versa.
2. Points of risk exist between the transfer of data between a Thing to the gateway, and from the Internet to the gateway. Communication takes place via communication protocols.
3. Each hardware brings its own set of security risks and concerns based on the components within.

COPYRIGHT INFORMATION

All figures, charts, and images used in this white paper are licensed for use by CirrusLabs, either through a purchased license for commercial use or a free public license for commercial use. All research sources used to produce this whitepaper belong to the companies and authors who produced this research, and CirrusLabs has credited all of these sources to their original owners.