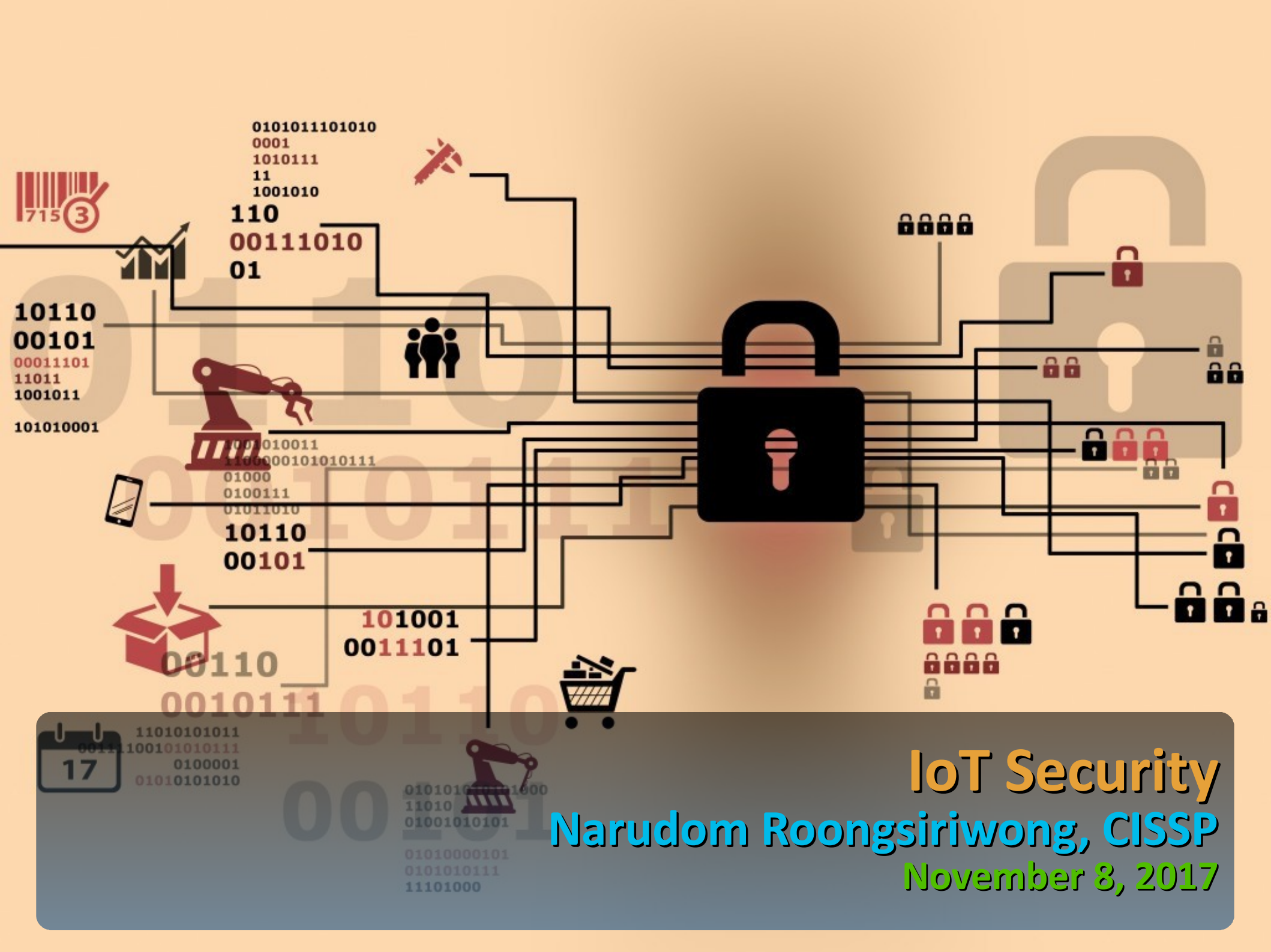


IoT Security

Narudom Roongsiriwong, CISSP

November 8, 2017

WhoAmI

- Lazy Blogger
  - Japan, Security, FOSS, Politics, Christian
  - http://narudomr.blogspot.com
- Information Security since 1995
- Embedded System since 2002
- Head of IT Security and Solution Architecture, Kiatnakin Bank PLC (KKP)
- Consultant for OWASP Thailand Chapter
- Committee Member of Cloud Security Alliance (CSA), Thailand Chapter
- Committee Member of Thailand Banking Sector CERT (TB-CERT)
- Consulting Team Member for National e-Payment project
- Contact: narudom@owasp.org

OWASP

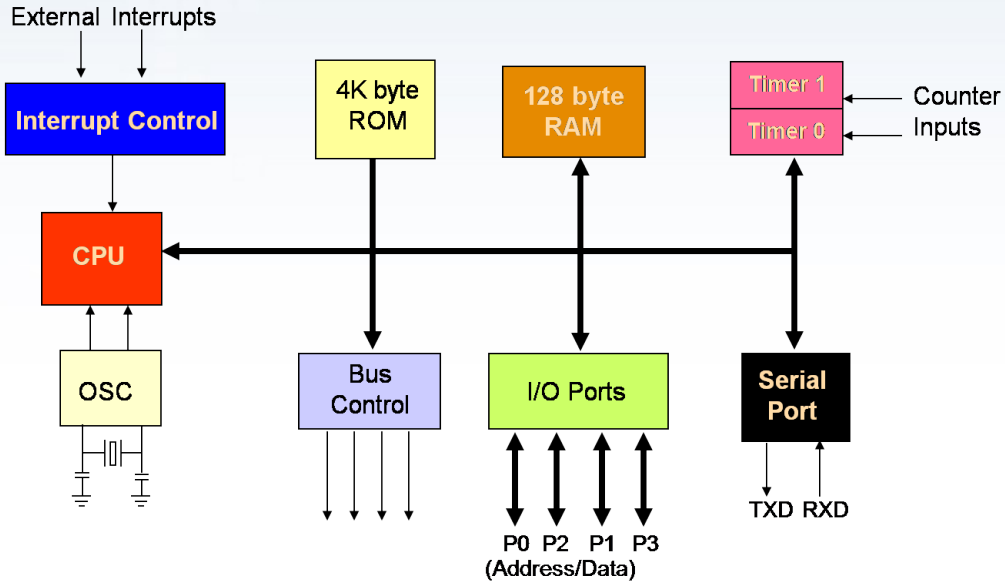
Open Web Application Security Project

My Journey to IoT Security

Microcontroller and Assembly Language

- 1986 Studied Electrical Engineering, Chulalongkorn University
- 1987 Worked Part-Time, Controllers Using Zilog Z80
- 1989 Was Apprenticed at Intronics, Using Intel 8048
- 1989 Designed Heat Exchanger Controller as a Senior Project, Using Intel 8031 (My Favorite 8051)

The 8051 Block Diagram



Network Security

- 1995 Started Working at Information and Telecommunication Services (ITS) as Business Development
- Was Assigned to Market a Firewall, “Eagle Raptor”
- Started My Life in Information Security

Embedded System and C/C++

- 2002 Started a Company, Structure and Composites, Embedded System Design for Bridge and Building Structure Monitoring
- 2004 First WiFi IP Based Bridge Structure Monitoring System
- 2004 Became a Special Instructor in Embedded System Design at Faculty of Engineering, Thammasat University
- 2006 My Company Went Broke
- 2007 Joined Incotec Automation (Thailand)
- 2009 Joined Chanwanich, Project Implementation on Smart Card, PLC and Information Security

OWASP
Open Web Application Security Project

OWASP

Open Web Application Security Project

Information Security Fundamental

What is Security?

- "The quality or state of being secure—to be free from danger"
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology

Security Concepts

Security Concepts			
Core	Confidentiality	Integrity	Availibility
	Authentication	Authorization	Accountability
Design	Need to Know	Least Privilege	Separation of Duties
	Defense in Depth	Fail Safe / Fail Secure	Economy of Mechanisms
	Complete Mediation	Open Design	Least Common Mechanisms
	Psychological Acceptability	Weakest Link	Leveraging Existing Components

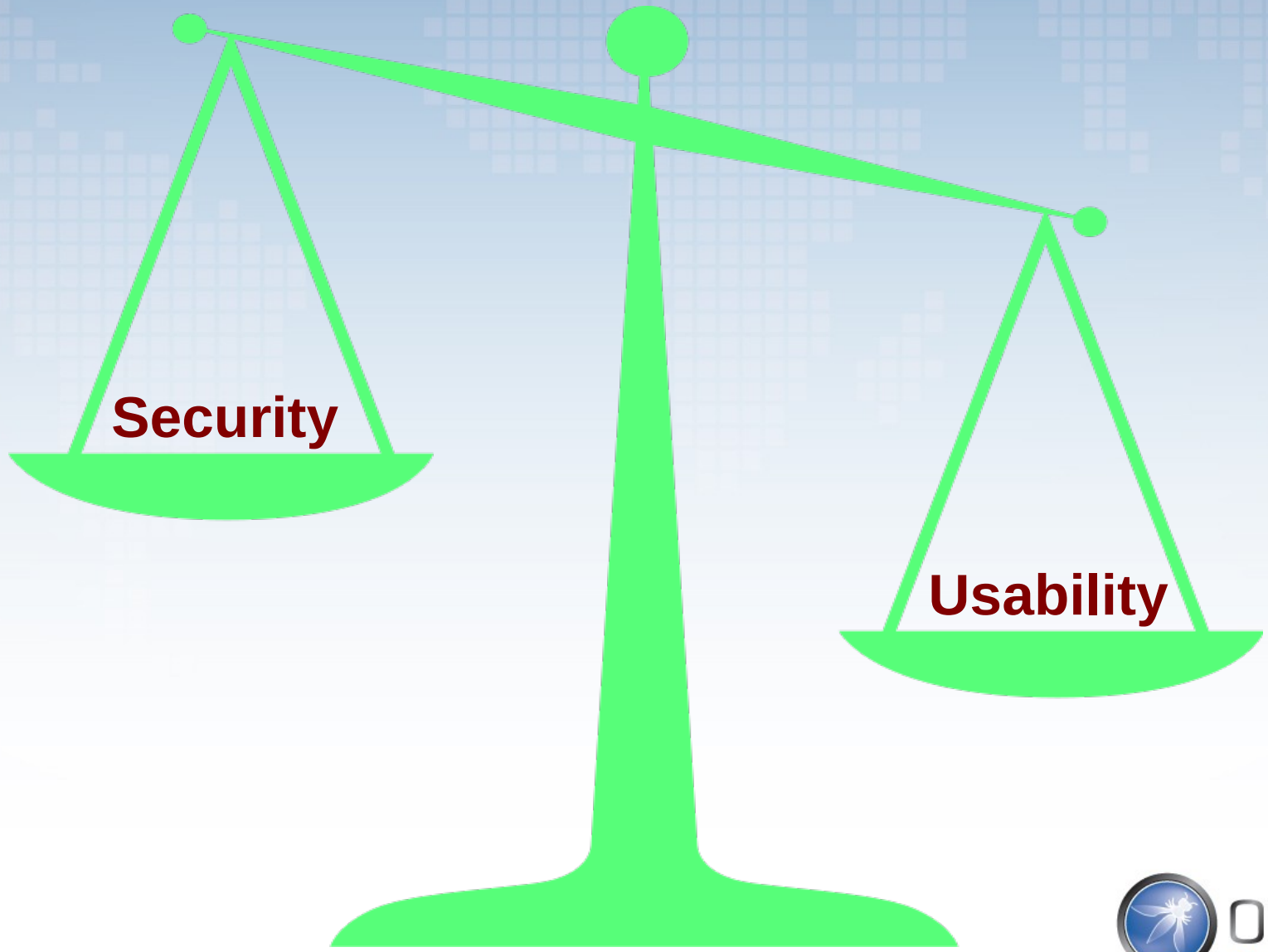
Confidentiality-Integrity-Availability (CIA)

To ensure protection against unauthorized access to or use of confidential information

To ensure that information and vital services are accessible for use when required

To ensure the accuracy and completeness of information to protect business processes

Security vs. Usability



Security vs. Safety (General Usage)

- Security is concerned with malicious humans that actively search for and exploit weaknesses in a system.
- Safety is protection against mishaps that are unintended (such as accidents)

OWASP
Open Web Application Security Project

Why Secure IoT Ecosystems

Problems of IoT Security

- Initial design was for private communication network then moved to IP network and later on the Internet
- Firmware updates are hard or nearly impossible after installations
- Started with basic security then found the security flaws and attached more complex security requirements later
- Low security devices from early design are still out there and used in compatible fall-back mode

Flaw in Design

Home Hacking Tech Deals Cyber Attacks Malware Spying

The Hacker News™
Security in a serious way

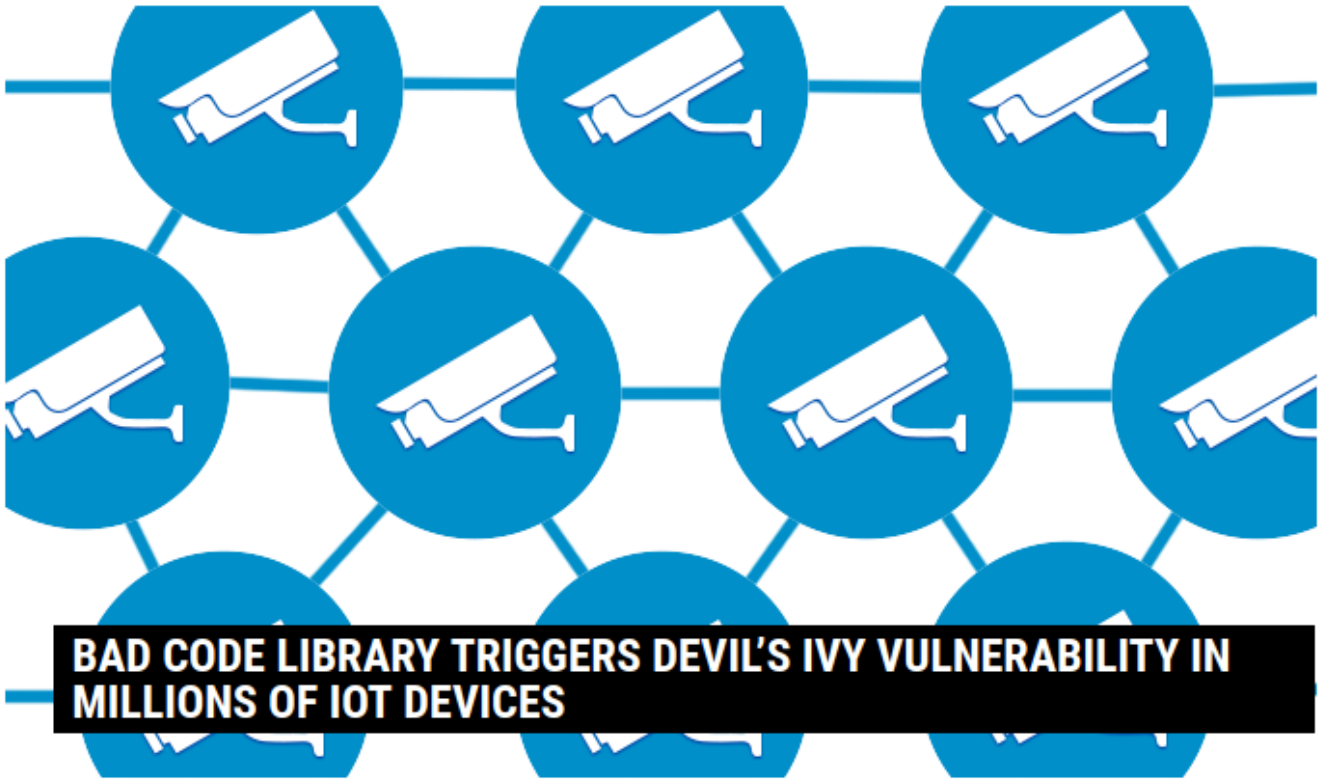
Unpatchable Flaw in Modern Cars Allows Hackers to Disable Safety Features

Thursday, August 17, 2017 Mohit Kumar

Tweet Share Share 48 Share 749 Share 1.34k Share

https://thehackernews.com/2017/08/car-safety-hacking.html

Flaw in Library



by Tom Spring

July 19, 2017 , 6:00 am

Tens of millions of products ranging from airport surveillance cameras, sensors, networking equipment and IoT devices are vulnerable to a flaw that allows attackers to remotely gain control over devices or crash them.

The vulnerability, dubbed Devil's Ivy, was identified by researchers at Senrio, who singled out high-end security cameras manufactured by Axis Communications. Senrio

Top Stories

Silence Gang Borrows From Carbanak To Steal From Banks
November 1, 2017 , 12:24 pm

Flaw in Google Bug Tracker Exposed Reports About Unpatched Vulnerabilities
October 30, 2017 , 4:39 pm

Chain of 11 Bugs Takes Down Galaxy S8 at Mobile Pwn2Own
November 2, 2017 , 1:35 pm

Popular 'Circle with Disney' Parental Control System Riddled With 23 Vulnerabilities
October 31, 2017 , 5:37 pm

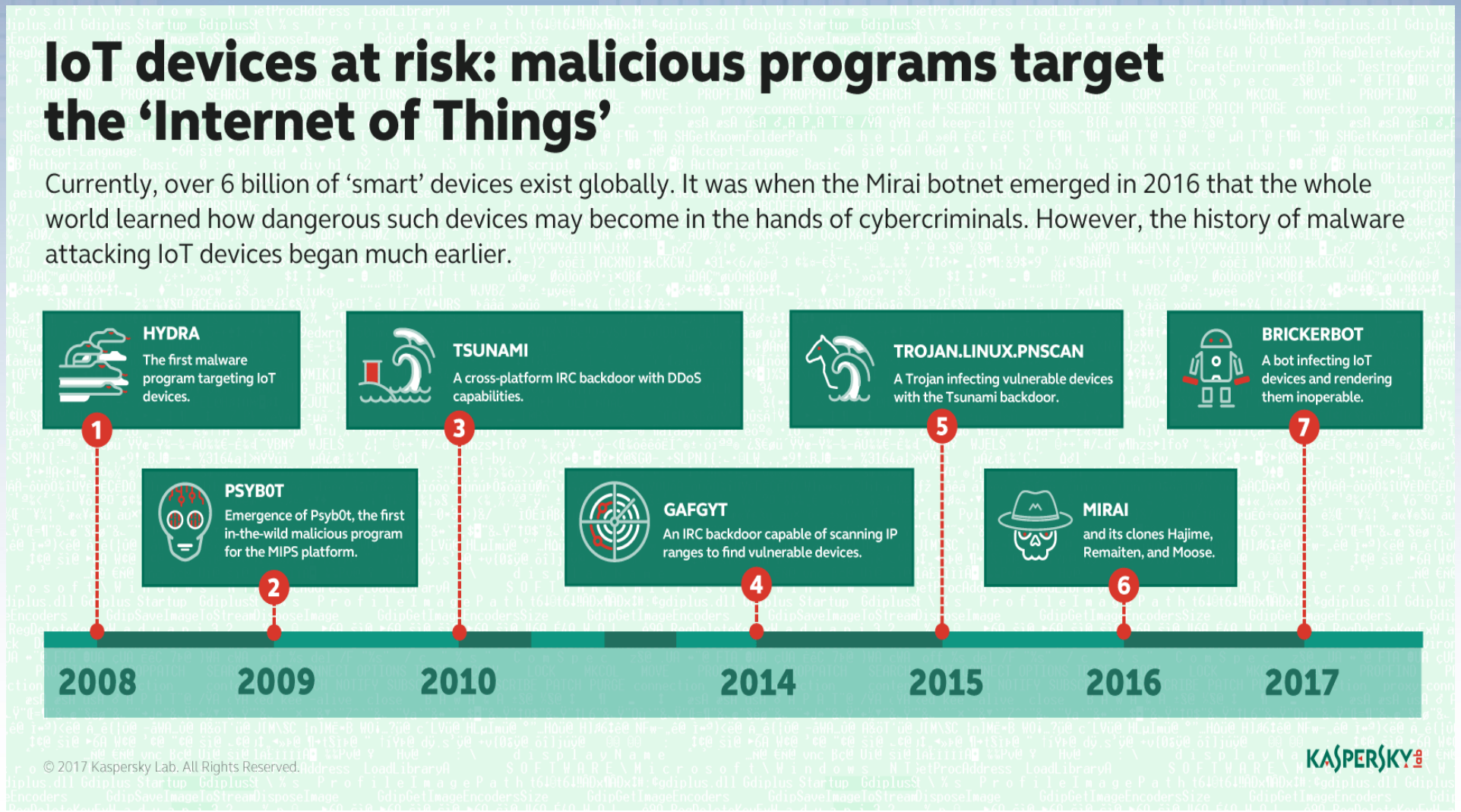
Rockwell Automation Patches Wireless Access Point against Krack
October 27, 2017 , 12:23 pm

Emergency Oracle Patch Closes Bug Rated 10 in Severity
October 31, 2017 , 12:48 pm

Taking HTTPS Denial to an Absurd Level
November 2, 2017 , 2:01 pm

https://threatpost.com/bad-code-library-triggers-devils-ivy-vulnerability-in-millions-of-iot-devices/126913/

Rises of Threats Target IoT Devices



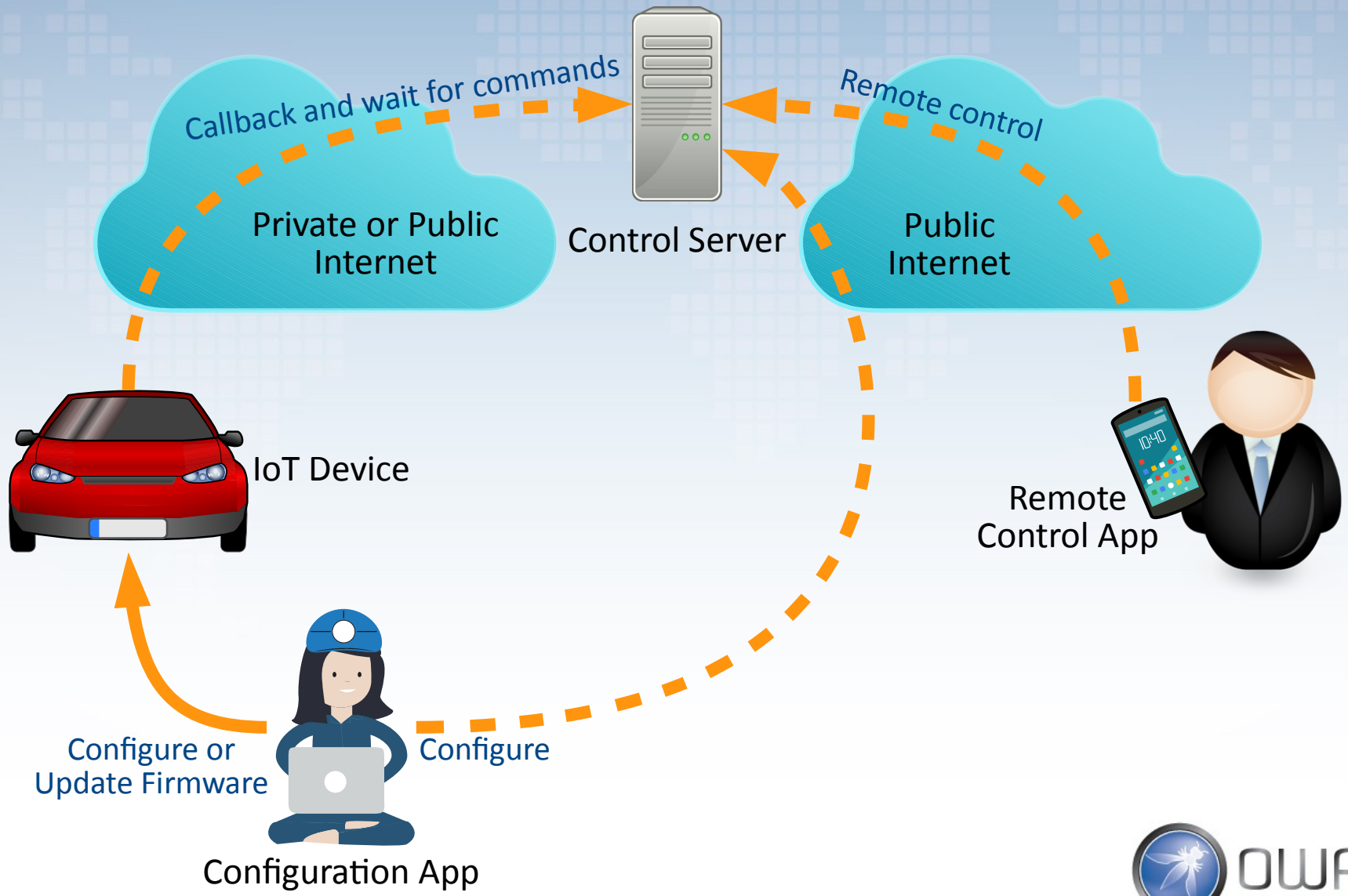
https://securelist.com/honeypots-and-the-internet-of-things/78751/

OWASP
Open Web Application Security Project

Types of IoT Classified by Communication

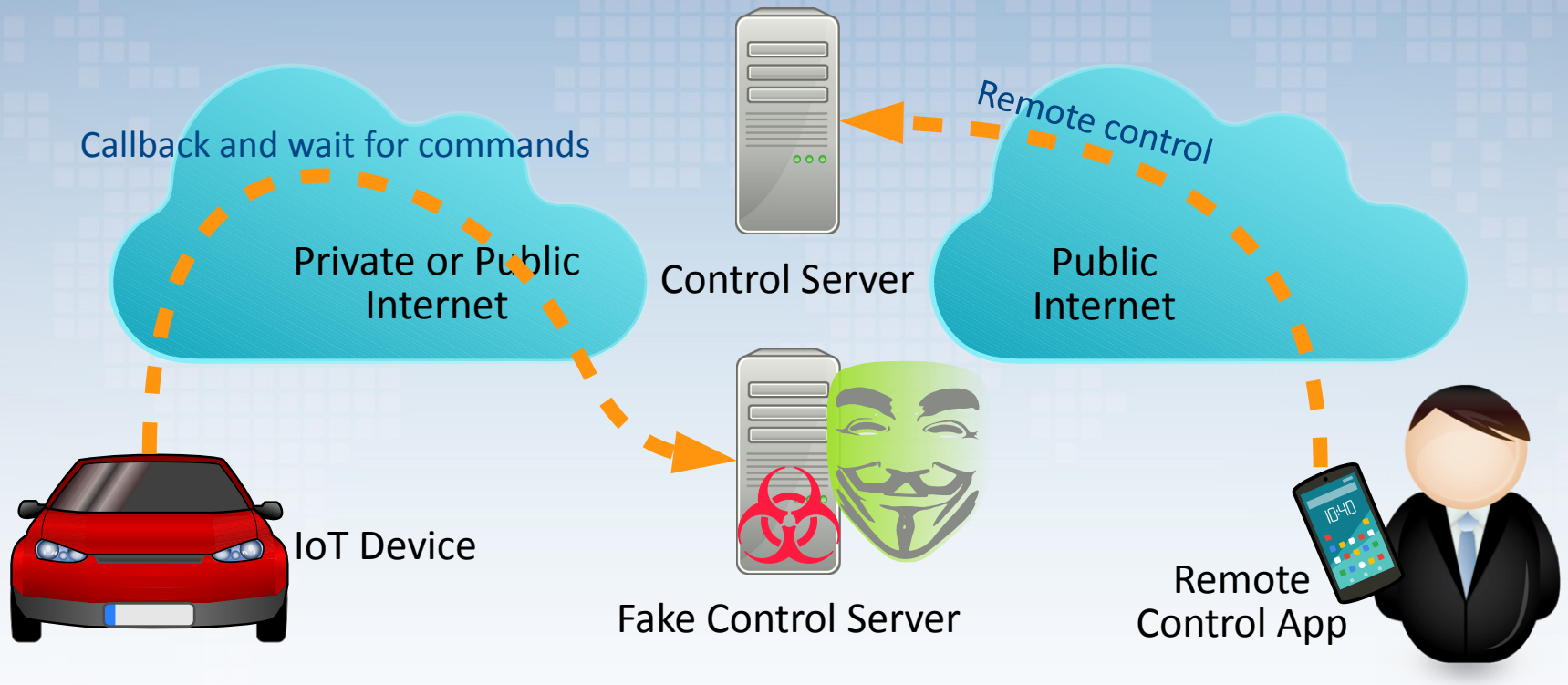
- Client Type
  - Most of implementation
  - e.g. payment terminal, IP Camera (call back to server), Smart Cars
- Server Type
  - e.g. IP Camera (built-in web interface)
- Peer-to-Peer or Mesh

Typical IoT Infrastructure

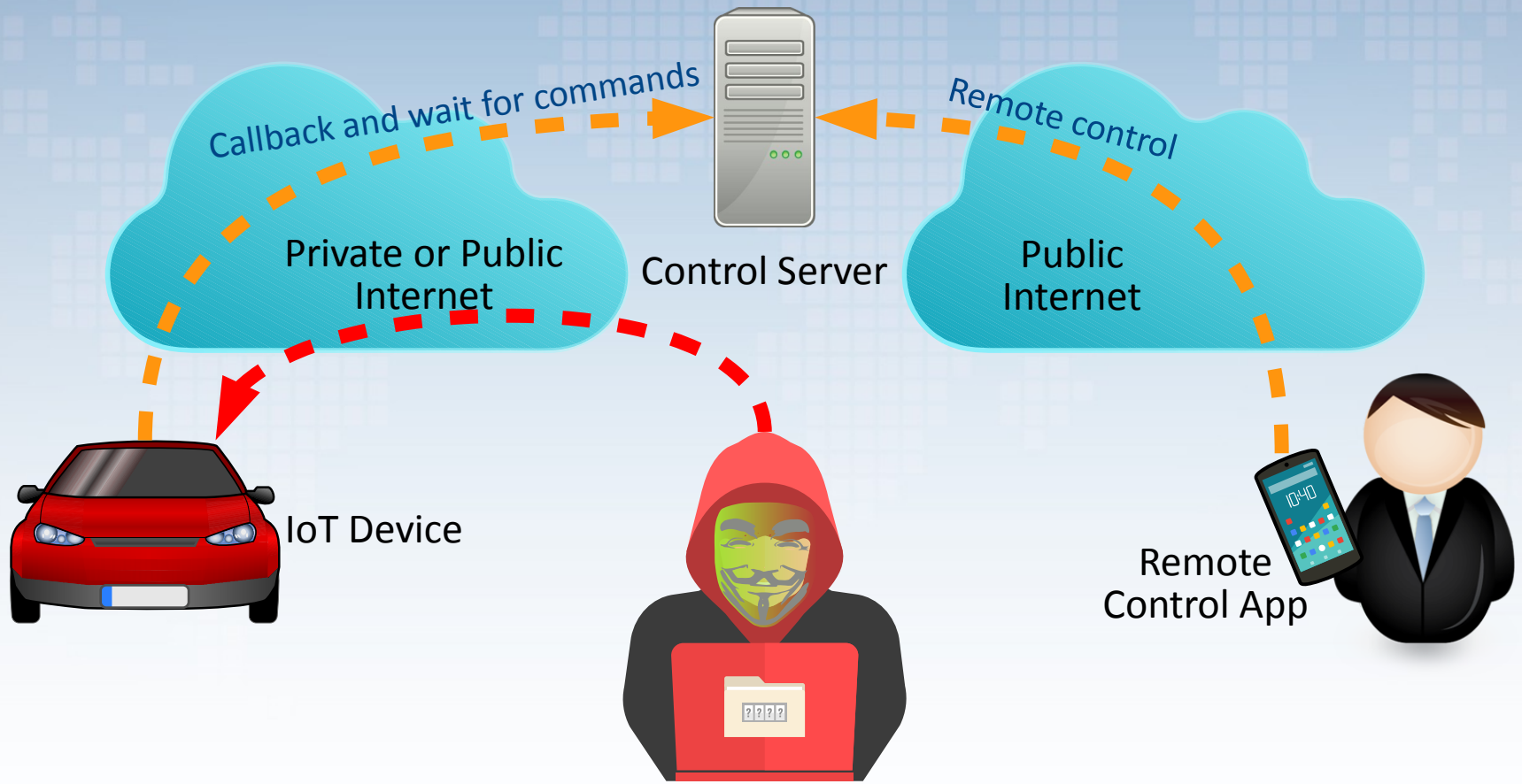


OWASP
Open Web Application Security Project

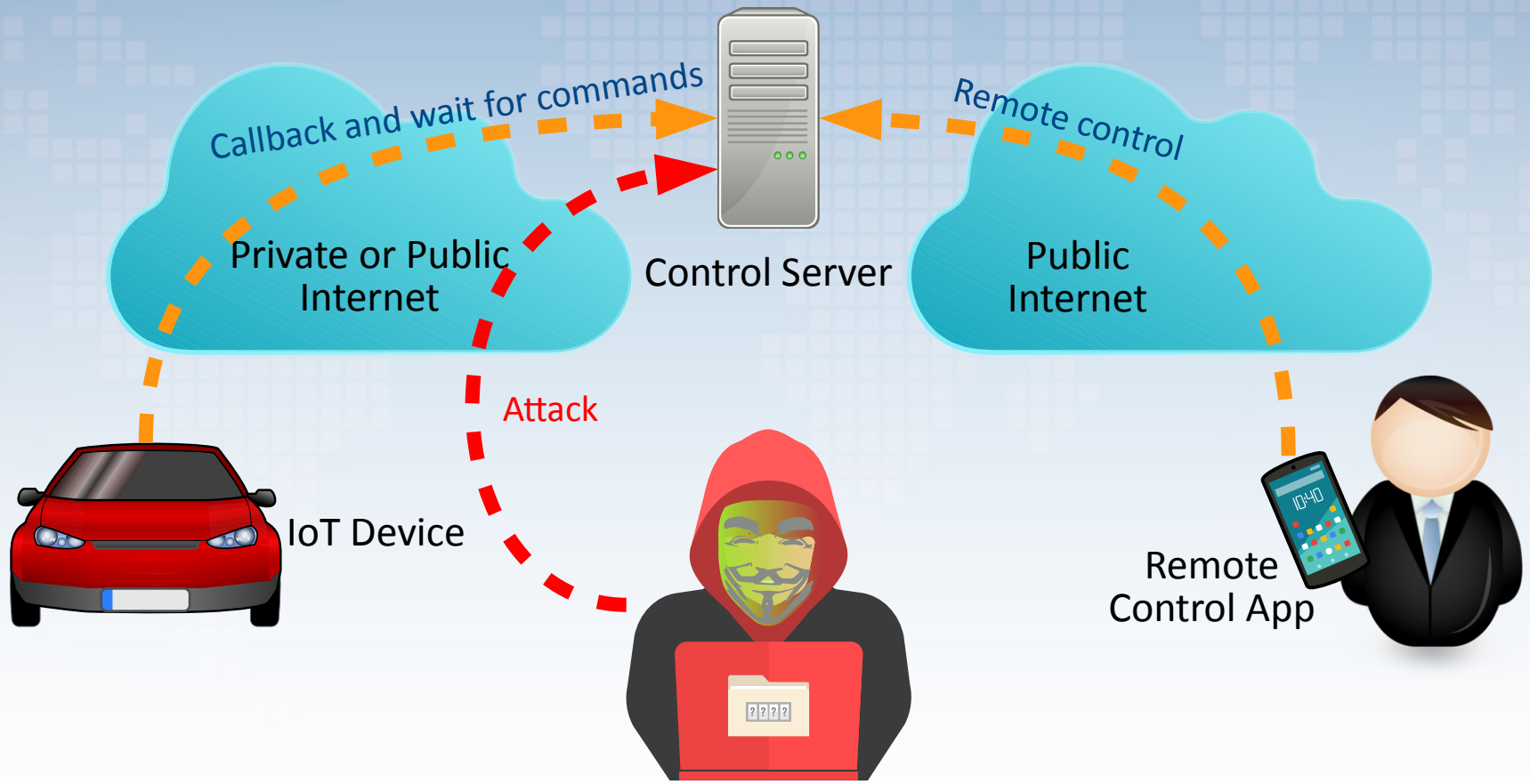
Typical Attack: Fake Control Server



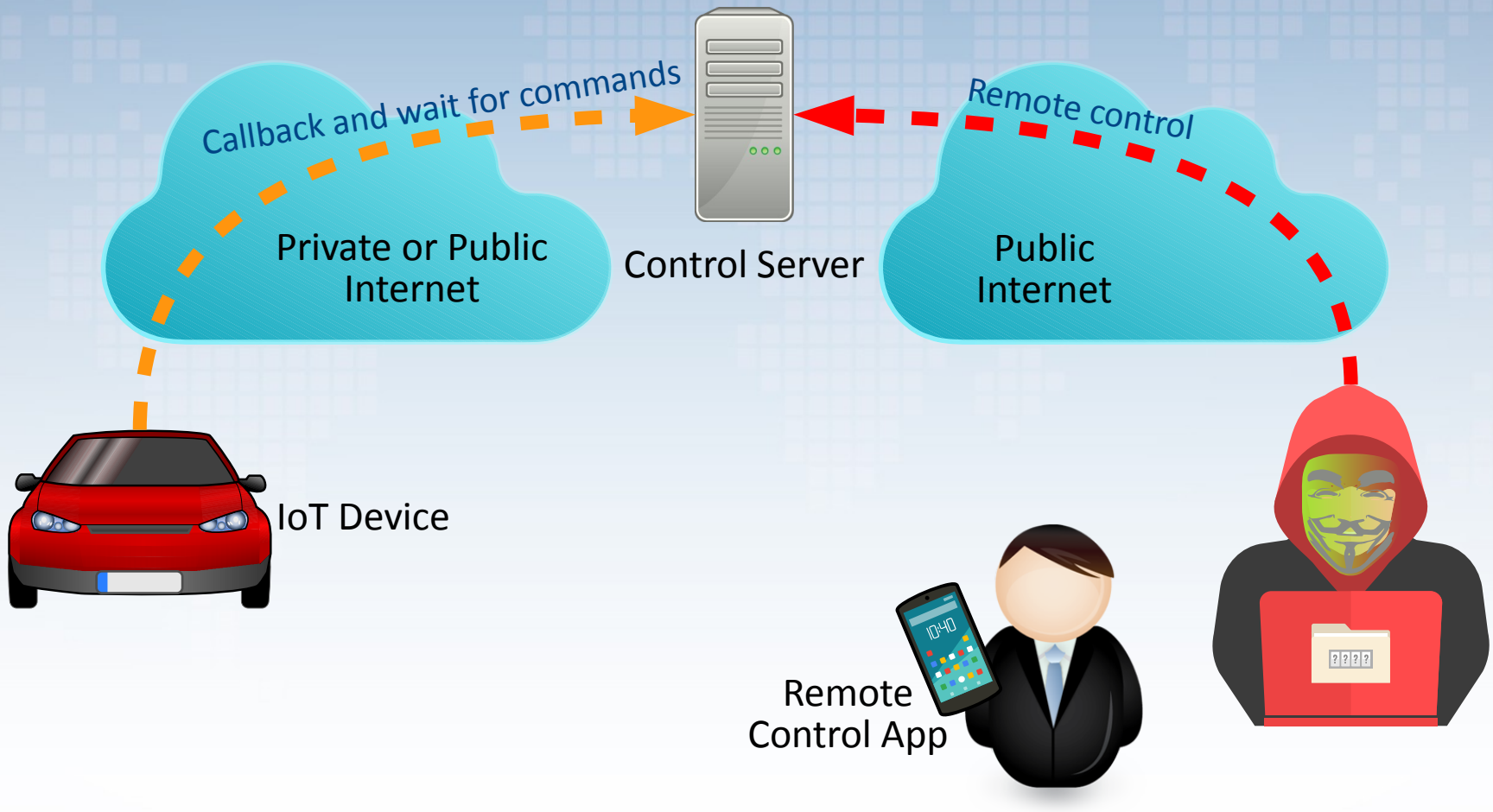
Typical Attack: Attack on Device Open Ports



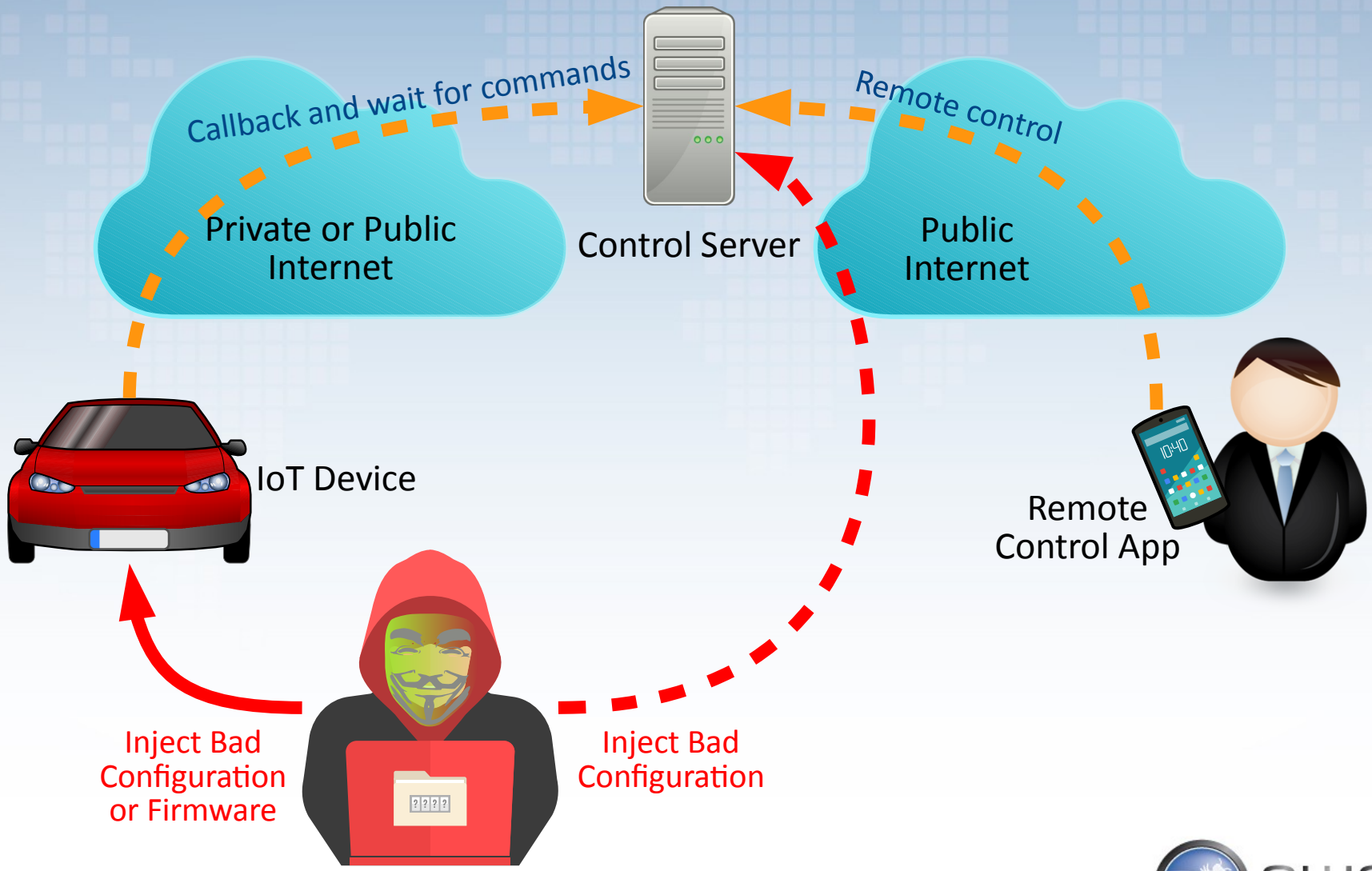
Typical Attack: Attack on Server Open Ports



Typical Attack: Steal Credential

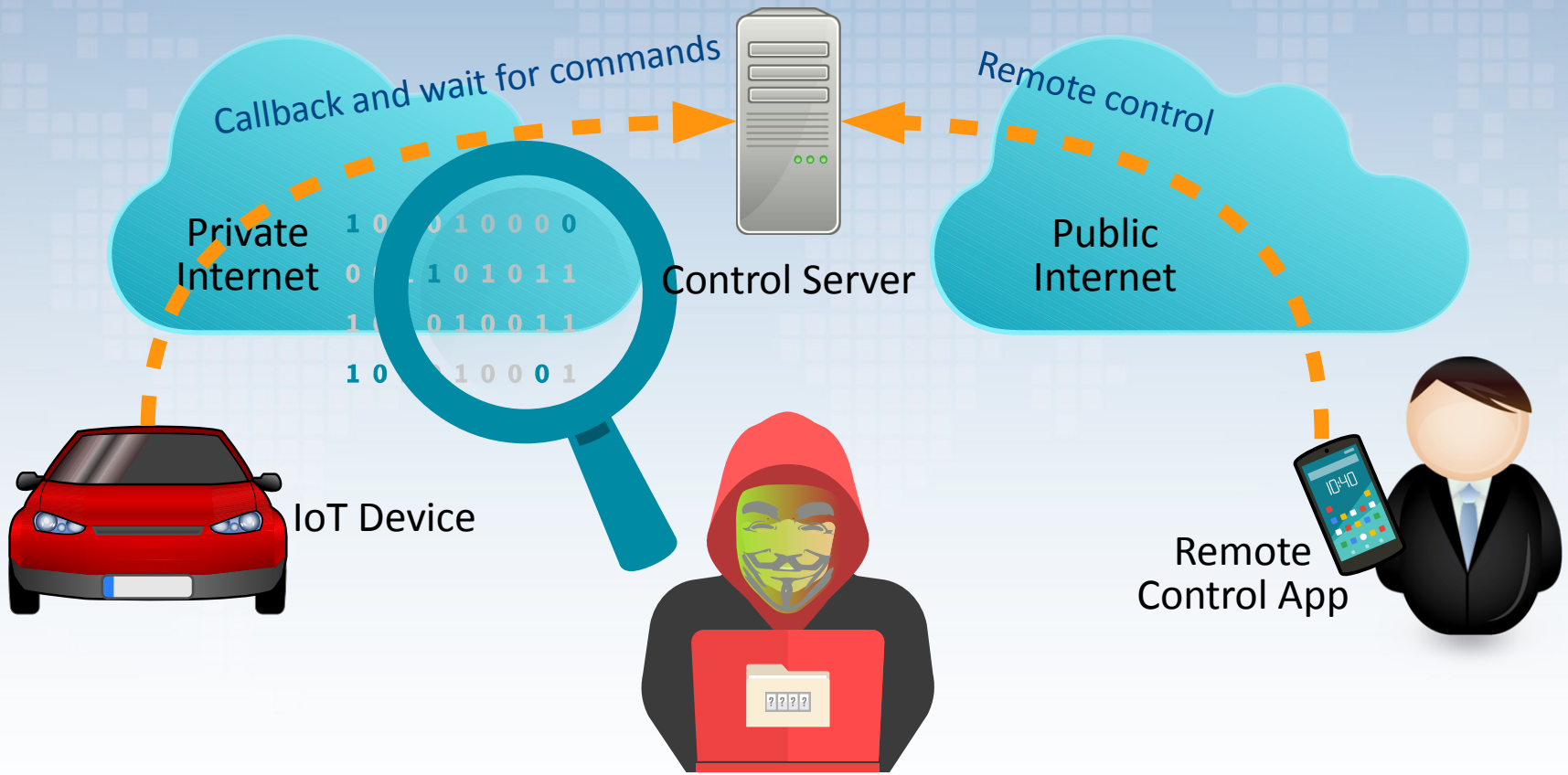


Typical Attack:
Inject Bad Configuration or Firmware



OWASP
Open Web Application Security Project

Typical Attack: Sniff Data on Private Network



Other Attack Surface Areas → See OWASP

- Ecosystem
- Device Memory
- Device Physical Interfaces
- Device Web Interface
- Device Firmware
- Device Network Services
- Administrative Interface
- Local Data Storage
- Cloud Web Interface
- Third-party Backend APIs
- Update Mechanism
- Mobile Application
- Vendor Backend APIs
- Ecosystem Communication
- Network Traffic
- Authentication/Authorization
- Privacy
- Hardware (Sensors)

https://www.owasp.org/index.php/IoT_Attack_Surface_Areas

OWASP Top 10 IoT Vulnerabilities 2014

I1 Insecure Web Interface

I2 Insufficient Authentication/Authorization

I3 Insecure Network Services

I4 Lack of Transport Encryption/Integrity Verification

I5 Privacy Concerns

I6 Insecure Cloud Interface

I7 Insecure Mobile Interface

I8 Insufficient Security Configurability

I9 Insecure Software/Firmware

I10 Poor Physical Security

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

1 Insecure Web Interface

covers IoT device administrative interfaces

Obstacles

Default usernames and passwords

No account lockout

XSS, CSRF, SQLi vulnerabilites

Solutions

Allow default usernames and password to be changed

Enable account lockout

Conduct web application assessments

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

Insufficient Authentication/Authorization 2

covers all device interfaces and services

Obstacles

- Weak passwords
- Password recovery mechanisms are insecure
- No two-factor authentication available

Solutions

- Require strong, complex passwords
- Verify that password recovery mechanisms are secure
- Implement two-factor authentication where possible

OWASP TOP 10 INTERNET OF THINGS VULNERABILITY CATEGORIES

3 Insecure Network Services

covers all network services including device, cloud, web and mobile

Obstacles	Solutions
Unnecessary ports are open	Minimize open network ports
Ports exposed to the internet via UPnP	Do not utilize UPnP
Network services vulnerable to denial of service	Review network services for vulnerabilities

OWASP TOP 10 INTERNET OF THINGS

VULNERABILITY CATEGORIES

Lack of Transport Encryption 4

covers all network services including device, cloud, web and mobile

Obstacles

Sensitive information is passed in clear text

SSL/TLS is not available or not properly configured

Proprietary encryption protocols are used

Solutions

Encrypt communication between system components

Maintain SSL/TLS implementations

Do not use proprietary encryption solutions

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

5 Privacy Concerns

covers all components of IoT solution

Obstacles

- Too much personal information is collected
- Collected information is not properly protected
- End user is not given a choice to allow collection of certain types of data

Solutions

- Minimize data collection
- Anonymize collected data
- Give end users the ability to decide what data is collected

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

Insecure Cloud Interface 6

covers cloud APIs or cloud-based web interfaces

Obstacles

- Interfaces are not reviewed for security vulnerabilities
- Weak passwords are present
- No two-factor authentication is present

Solutions

- Security assessments of all cloud interfaces
- Implement two-factor authentication
- Require strong, complex passwords

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

7 Insecure Mobile Interface

covers mobile application interfaces

Obstacles

- Weak passwords are present
- No two-factor authentication implemented
- No account lockout mechanism

Solutions

- Implement account lockout after failed login attempts
- Implement two-factor authentication
- Require stong, complex passwords

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

Insufficient Security Configurability 8

covers the IoT device

Obstacles

Password security options are not available

Encrytion options are not available

No option to enable security logging

Solutions

- Make security logging available
- Allow the selection of encryption options
- Notify end users in regards to security alerts

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

9 Insecure Software/Firmware

covers the IoT Device

Obstacles

- Update servers are not secured
- Device updates transmitted without encryption
- Device updates not signed

Solutions

- Sign updates
- Verify updates before install
- Secure update servers

OWASP TOP 10

INTERNET OF THINGS

VULNERABILITY CATEGORIES

Poor Physical Security 10

covers the IoT device

Obstacles

- Unnecessary external ports like USB ports
- Access to operating systems through remove media
- Inability to limit administrative capabilities

Solutions

- Minimize external ports like USB ports
- Properly protect operating system
- Include ability to limit administrative capabilities

OWASP

Open Web Application Security Project

Secure IoT Devices That We Use

Mirai Malware

- Malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks
- Primarily targets online consumer devices such as IP cameras and home routers using a table of more than 60 common factory default usernames and passwords, and logs into them to infect them with the Mirai malware
- First found in August 2016
- Use in DDoS attacks
  - 20 September 2016 on the Krebs on Security site which reached 620 Gbit/s and 1 Tbit/s attack on French web host OVH
  - 21 October 2016 multiple major DDoS attacks in DNS services of DNS service provider Dyn
  - November 2016 attacks on Liberia's Internet infrastructure
- The source code for Mirai has been published in hacker forums as open-source

What Can We Learn from Mirai Attacks?

- Do not use default passwords for all default usernames
- If possible, do not allow configuration interface from Internet side
- If the IoT devices are used only in the organization, do not expose to the public Internet
- If there is a need to use from the Internet, open only necessary ports and use non-default ports where possible


Q&A