How not to become another security headline…

Craig Heath, Jeff Day, Richard Marshall

IoT Security Foundation

Headlines and the Compliance Framework

Richard Marshall

IoTSF Plenary Chair and CEO Xitex Ltd

We can't carry on like this

IoT Security Foundation

Researchers Discover 500,000+ IoT Devices Vulnerable to Mirai Botnet

MARITZA SANTILLAN
OCT 10, 2016 | LATEST SECURITY NEWS

How A Researcher Hacked iKettles to Steal WiFi Passwords All Across London

October 21st, 2015

WEIRD NEWS

Talking Doll Cayla Hacked To Spew Filthy Things

02/09/2015 04:10 pm ET | Updated Feb 10, 2015

21 OCT 16 **Hacked Cameras, DVRs Powered Today's Massive Internet Outage**

Krebs on Security

Researchers hack Philips Hue lights via a drone; IoT worm could cause city blackout

Researchers hijack Philips Hue lights with a drone to show how IoT worm could take over smart lights in a city.

Darlene Storm in Computer World

Modified Mirai botnet could infect five million routers

by Michael Heller
Senior Reporter
Published: 30 Nov 2016

Researchers said a modified version of the Mirai botnet code has been attacking routers by exploiting a specific vulnerability and may leave millions at risk.

Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking

Latest recall designed to protect connected vehicles from remote manipulation, says automobile company

Hacking traffic lights with a laptop is easy

TECHNOLOGY NEWS | Tue Oct 4, 2016 | 8:58pm BST

J&J warns diabetic patients: Insulin pump vulnerable to hacking

Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON

The results from this year's IoT hacking contest are in and it's not a pretty picture

CSO Online: Lucian Constantin

Compliance Framework Goals

1. Clear and auditable requirements
2. Classifications of requirements:
   - Integrity
   - Availability
   - Confidentiality
3. Applicability of requirements
   1. Initially Consumer focussed
4. Certification Questionnaire

How would this have impacted some of the hacks to date…?

“Researchers Discover 500,000 IoT Devices Vulnerable to Mirai Botnet”

Mirai self propagates itself creating botnets through insecure IoT devices such as routers, IP Cameras, Printers and DVRs:

1. Spreads by scanning the Internet for IoT devices which use factory default or hardcoded login names and passwords
2. Logs into the device and downloads malicious software which connects to a central command and control server.

Mitigation of Mirai on IoT Devices

The Framework covers exploits such as these:

2.3.5.5 - If a connection requires a password or passcode or passkey for connection authentication, the default password or factory reset password is unique to each device.

2.3.6.12 - The product allows the factory default or OEM login accounts to be disabled or erased or renamed.

2.3.6.13 - The product supports having any or all of the factory default user login passwords, altered prior to installation.

2.3.3.1 - The product has measures to prevent unauthenticated software and files being loaded onto it.

“How A Researcher Hacked iKettles to Steal WiFi Passwords All Across London”

The iKettle is relatively insecure through:

1. The kettle does not authenticate the WiFI AP it is connected to by anything other than it’s SSID thus allowing it to be connected to a fake AP
2. The Telnet service on the kettle has a default PIN of ‘000000’ allowing a remote Telnet session.
3. This allows the attacker to get the kettle to dump out the WPA PSK using the AT-KEY command for the WiFi network

Mitigation of attack the iKettles

The Framework covers exploits such as these:

2.3.4.3 - All interactive operating system accounts or logins have been disabled or eliminated from the software.

2.3.5.5 - If a connection requires a password or passcode or passkey for connection authentication, the default password or factory reset password is unique to each device. Examples are WiFi access passwords and Bluetooth PINS.

2.3.5.6 - Where a wireless interface has an initial pairing process, the passkeys are changed from the default prior to providing normal service.

2.3.5.9 - All network communications keys are stored securely.

“Talking Doll Cayla Hacked To Spew Filthy Things”

Attack of Carly doll by Ken Munro & Tim Medin revealed:

1. The phrase database can be modified despite the app SQL database being encrypted – the password –is stored in plaintext in the phone app
2. Any Bluetooth system can connect to Carly and use it as a speaker or as a remote device, albeit only one device can be connected to a Carly doll at any one time…

Mitigation on Carly vulnerabilities

The Framework covers exploits such as these:

2.3.6.8 - The product securely stores any passwords using an industry standard cryptographic algorithm.

2.3.5.1 - The product prevents unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.

2.3.5.5 - If a connection requires a password or passcode or passkey for connection authentication, the default password or factory reset password is unique to each device. Examples are WiFi access passwords and Bluetooth PINS.

“New wave of ‘Mirai’ attacking home routers”

Attack of DSL Routers through open port 7547 normally used for TR-069 remote management.

1. Through port 7547 use TR-064 SOAP "NewNTPServer” command to download a file name ‘1’ through ‘7’ into local temp directory and then executes the ‘1’ file…
2. Deletes itself from filesystem so that it only resides in memory
3. Close vulnerable port using iptables to prevent further attacks
4. Using DNS 8.8.8.8 resolve command and control servers
5. Using the WAN port scan internet for open TCP 7547 ports

Mitigation of Port 7547 attack on home routers

The Framework covers exploits such as these:

2.3.3.1 - The product has measures to prevent unauthenticated software and files being loaded onto it

2.3.3.3 - Where remote software upgrade can be supported by the device, the software images are digitally signed by an authorised trust entity.

2.3.5.1 - The product prevents unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.

Headlines and Best Practice Case Studies

Jeff Day

WG2 Chair and Senior Security Consultant BT plc

Contents

The following lists the security topic areas in the IoTSF Secure Design Best Practice Guidelines.

Each topic area has an assigned letter for easy reference. It also indicates they collectively form a set of Guidelines that should be acted on as a whole. However no specific order of reading or action is intended.

Each topic area must be studied, understood and every security item implemented where possible. These security items should be documented to form part of the overall security design of the product. Any item that cannot be implemented for good technical or business reasons must also be documented in the design.

More details about every security topic area can be found on the IoTSF website.

EXECUTIVE SUMMARY....5
A - CLASSIFICATION OF DATA....6
B - PHYSICAL SECURITY....7
C - DEVICE SECURE BOOT....8
D - SECURE OPERATING SYSTEM....9
E - APPLICATION SECURITY....10
F - CREDENTIAL MANAGEMENT....11
G - ENCRYPTION....12
H - NETWORK CONNECTIONS....13
J - SOFTWARE UPDATES....14
K - LOGGING....15

B: PHYSICAL SECURITY

IoT devices are often deployed in locations that can be accessed easily for extended periods of time. This makes them liable to physical damage, tampering with switches and making connections to management, debugging and test ports. Side-channel attacks may allow the extraction of encryption keys or other data by monitoring power consumption, temperature fluctuations or electromagnetic emissions etc. Devices in the supply chain are also at risk.

Production devices can be protected against physical access to data and intellectual property by physically barring access and removing all means of unwanted connection.

1. Any interface used for administration or test purposes during development should be removed from a production device, disabled or made physically inaccessible.
2. All test access points on production units must be disabled or locked, for example by blowing on-chip fuses to disable JTAG.
3. If a production device must have an administration port, ensure it has effective access controls, e.g. strong credential management, restricted ports, secure protocols etc.
4. Make the device circuitry physically inaccessible to tampering, e.g. epoxy chips to circuit board, resin encapsulation, hiding data and address lines under these components etc.
5. Provide secure protective casing and mounting options for deployment of devices in exposed locations
6. To identify and deter access within the supply chain, consider making the device and packaging "tamper evident".
7. For high-security deployments, consider design measures such as active masking or shielding to protect against side-channel attacks.

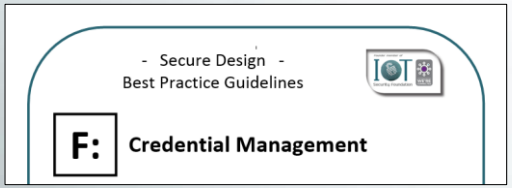
Further discussion on physical protection can be found at: <insert url here>.

Resources on how to apply physical security are listed below:

- Hardware-Oriented Security
- Securing Hardware for Embedded Systems (1)
- Securing Hardware for Embedded Systems (2)

"Entering the network via the dongle was extremely easy, as the device runs its own Wi-Fi network. This network is secured only by an 8 (numeric) digit password […] (and is easily cracked). A successful brute-force attack […] allows unauthorized […] access to the network."

"Would you sell a root shell in your network for $25 dollars?"



Use good password management techniques, for example no blank or simple passwords allowed, permit non-alphanumerics (e.g. + or *) as well as letters and digits. (See additional material on IoTSF web site)

"Vendors themselves should be aware of the information security aspect at the time when new IoT devices are still at the product design stage. This is crucial to avoid introducing security flaws such as the ones we detailed in this blog."

www.checkpoint.com

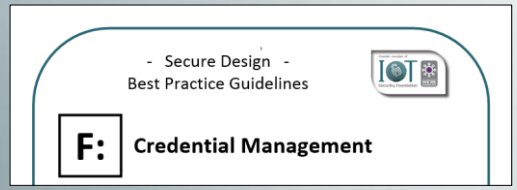
Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide

A certificate issued to a "Daniel“ […] is used in firmware from [*add several well known hardware vendor names here*]. This certificate is found in a [*popular*] SDK. The affected vendors used it as a basis to develop their own firmware. More than 480,000 devices on the web are using this single certificate.

A certificate issued […] in Bangalore, India is used in firmware from [*add several well known hardware vendor names here*]. This certificate can be attributed to a [*popular*] SDK for ADSL2+ routers. Over 300.000 devices on the web are using this certificate. A SSH host key can be attributed to this SDK as well.

A certificate issued to "MatrixSSL Sample Server Cert" is used in WiMAX gateways from [*add several well known hardware vendor names here*]. All affected devices use the same code base […]. At least 80.000 devices on the web are using this certificate.

www.sec-consult.com



Every certificate must be unique and therefore only exist on one device. Do not copy digital certificates across multiple devices.

(See additional material on IoTSF web site)

Headlines and Vulnerability Disclosure

Craig Heath

WG4 Chair and Director, Franklin Heath Ltd

How Not To Manage It…

“ "We are aware of the report on Twitter…" an Owlet spokeswoman told us. ”

Making The Best Of It…

"…triggered Philips to release a firmware patch for owners of its "Hue" connected bulbs. "

IoT Security Foundation WG4 Vulnerability Disclosure Guidelines

1. Introduction
2. Vulnerability Disclosure Process Guidelines
3. Internal Organisation and Processes
4. References and Abbreviations

- Web Site
- Sample Web Page Text
- Means of Contact
- Communicating with the Researcher
- Resolving Conflict
- Timing of Response
- Security Advisory
- Credit where Credit is Due
- Money
- Discouraging Damaging Actions

Practising What We Preach

Security Vulnerability Contact Information

Acceptable Research

Whilst we encourage investigation of potential security vulnerabilities, we cannot condone any activities which might interfere with legitimate users or which might contravene applicable computer misuse and data protection legislation. For that reason, the following activities are prohibited:

- Modification or destruction of data
- Interruption or degradation of services, for example Denial of Service attacks
- Disclosure of personal, proprietary or financial information

disclosure with us will appear here with consent.

Questions…

More information on:

- Best Practice Guides
- Compliance Framework
- Vulnerability Disclosure Guidelines

- Can be found at can be found at:

https://iotsecurityfoundation.org

Thank You!