Engaging with IoT Security Best Practices

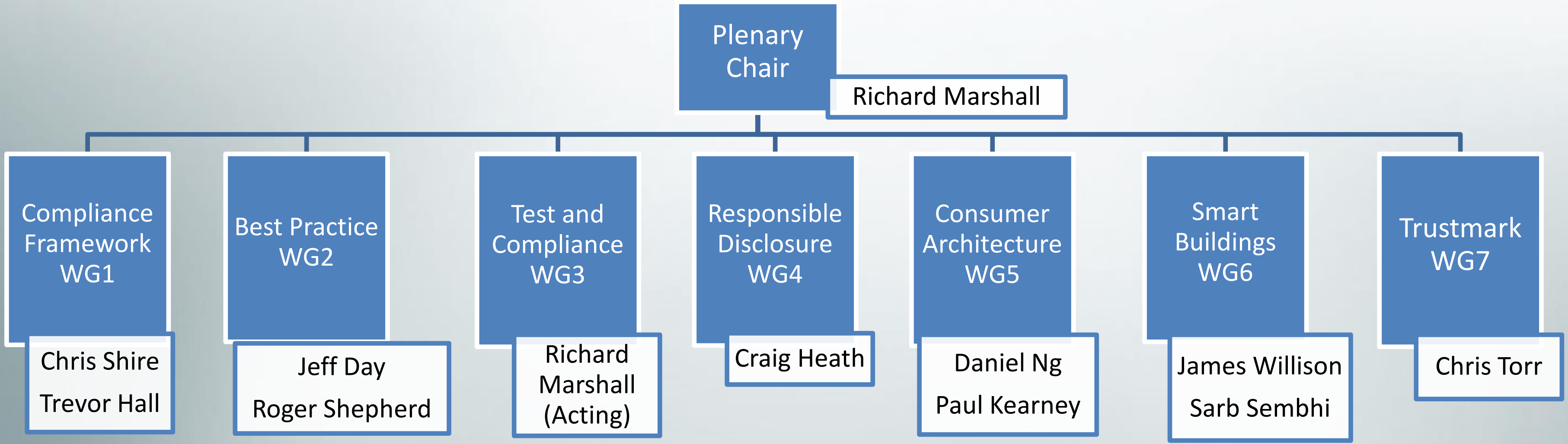
IoTSF Conference 2018

4th December 2018

Richard Marshall

IoTSF Plenary Chair

Working Groups



Plenary Chair

Richard Marshall

Compliance Framework WG1

Chris Shire

Trevor Hall

Best Practice WG2

Jeff Day

Roger Shepherd

Test and Compliance WG3

Richard Marshall (Acting)

Responsible Disclosure WG4

Craig Heath

Consumer Architecture WG5

Daniel Ng

Paul Kearney

Smart Buildings WG6

James Willison

Sarb Sembhi

Trustmark WG7

Chris Torr

Release 1.0

IoT Security Compliance Framework

Release 1.0

© 2016 IoT Security Foundation

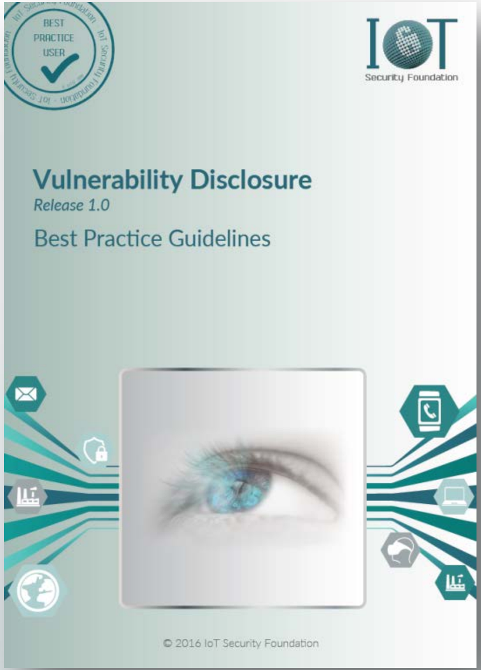
RELEASE 1.0

Connected Consumer Products

Release 1.0

Best Practice Guidelines

© 2016 IoT Security Foundation



Vulnerability Disclosure

Release 1.0

Best Practice Guidelines

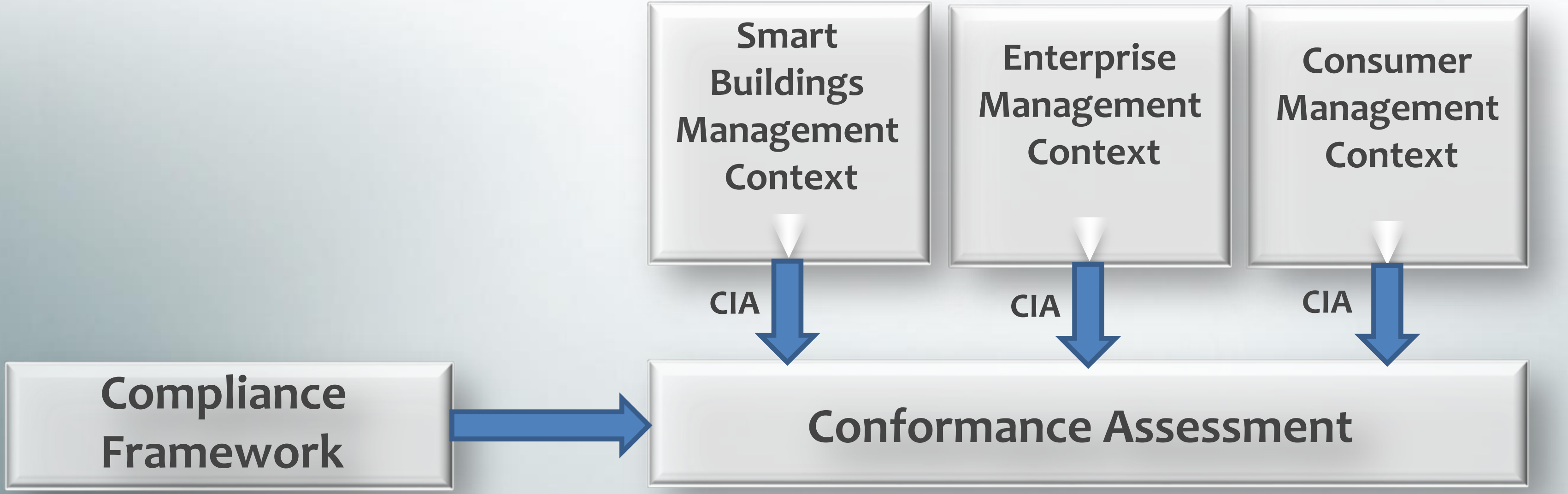
© 2016 IoT Security Foundation

Release 2.0

Change of Scope from Consumer to generic

- Compliance Framework 2.0
  - Expanded compliance requirements
  - Improved compliance checklist
- Best Practice Guides
  - Architectures

WG Document Context



Smart Buildings Management Context

Enterprise Management Context

Consumer Management Context

CIA

CIA

CIA

Compliance Framework

Conformance Assessment

What's new in the Compliance Framework 2.0?

Engaging with IoT Security Best Practices

Chris Shire

Infineon

Audience

Who is the Compliance Framework for:

- For **Managers** in organisations that provide IoT products, technology and or services

- For **Developers and Engineers, Logistics and Manufacturing Staff**, it provides a detailed checklist to use in their daily work and in project reviews to validate the use of best practice by different functions

- For **Supply Chain Managers**, the structure can be used to guide the auditing of security practices.

Release 2.0 to be published today

BEST PRACTICE USER

IoT Security Foundation

IoT Security Compliance Framework

Release 2 December 2018

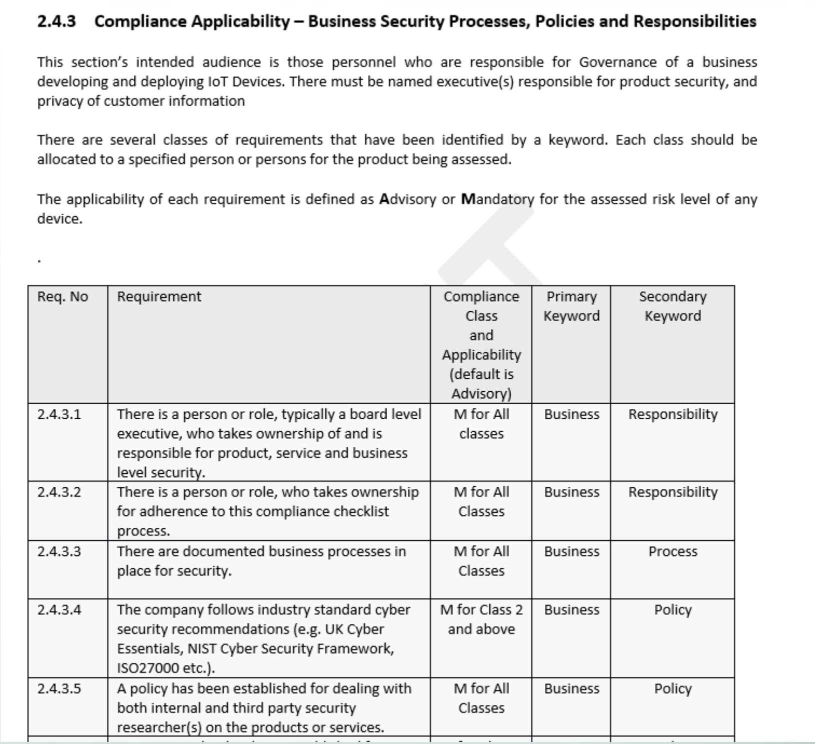
© 2018 IoT Security Foundation

What's New with Version 2?
Introduces Key Requirements for IoT Security

- ➢ Management Governance
- ➢ Engineered for Security
- ➢ Fit for Purpose Cryptography
- ➢ Secure Network Framework and Applications
- ➢ Secure Production Processes and Supply Chain
- ➢ Safe and Secure for the Customer

New Framework 2.0 - outcome

- ➢ Look and Feel :
- ➢ Simpler
- ➢ Clearer
- ➢ Easily Organised
- ➢ Faster to Adopt



2.4.3 Compliance Applicability – Business Security Processes, Policies and Responsibilities

This section's intended audience is those personnel who are responsible for Governance of a business developing and deploying IoT Devices. There must be named executive(s) responsible for product security, and privacy of customer information

There are several classes of requirements that have been identified by a keyword. Each class should be allocated to a specified person or persons for the product being assessed.

The applicability of each requirement is defined as **A**dvisory or **M**andatory for the assessed risk level of any device.

.

Req. No	Requirement	Compliance Class and Applicability (default is Advisory)	Primary Keyword	Secondary Keyword
2.4.3.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	M for All classes	Business	Responsibility
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance checklist process.	M for All Classes	Business	Responsibility
2.4.3.3	There are documented business processes in place for security.	M for All Classes	Business	Process
2.4.3.4	The company follows industry standard cyber security recommendations (e.g. UK Cyber Essentials, NIST Cyber Security Framework, ISO27000 etc.).	M for Class 2 and above	Business	Policy
2.4.3.5	A policy has been established for dealing with both internal and third party security researcher(s) on the products or services.	M for All Classes	Business	Policy

How to use them…

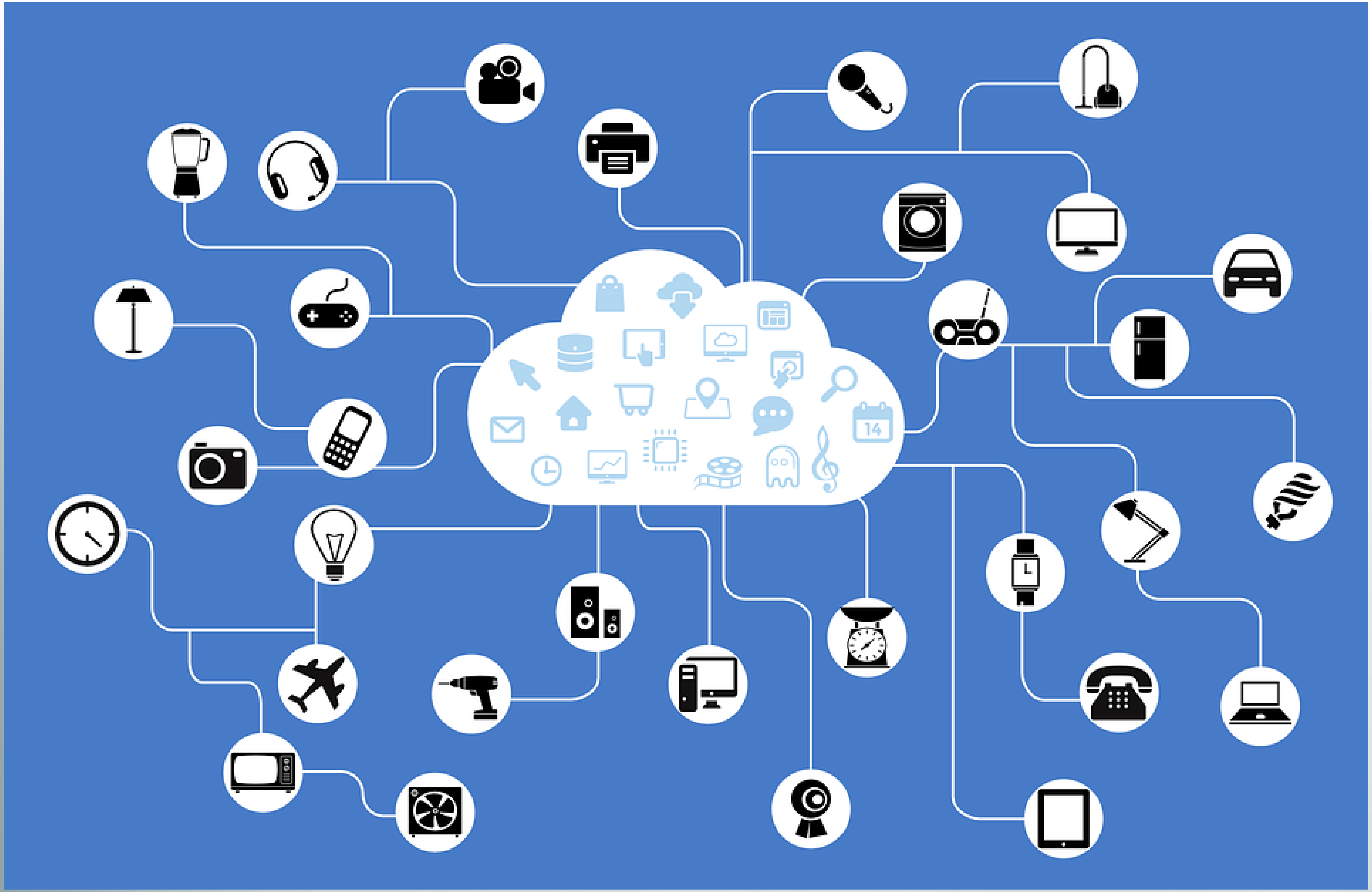
- Cover how to use:
- The Compliance Framework 2.0
- Checklist
- Best Practice Guides

Introducing the Best Practice Guides

Engaging with IoT Security Best Practices

Jeff Day

BT



"There are known knowns.

There are things we know we know.

We also know there are known unknowns.

That is to say, ***we know there are some things we do not know****.*

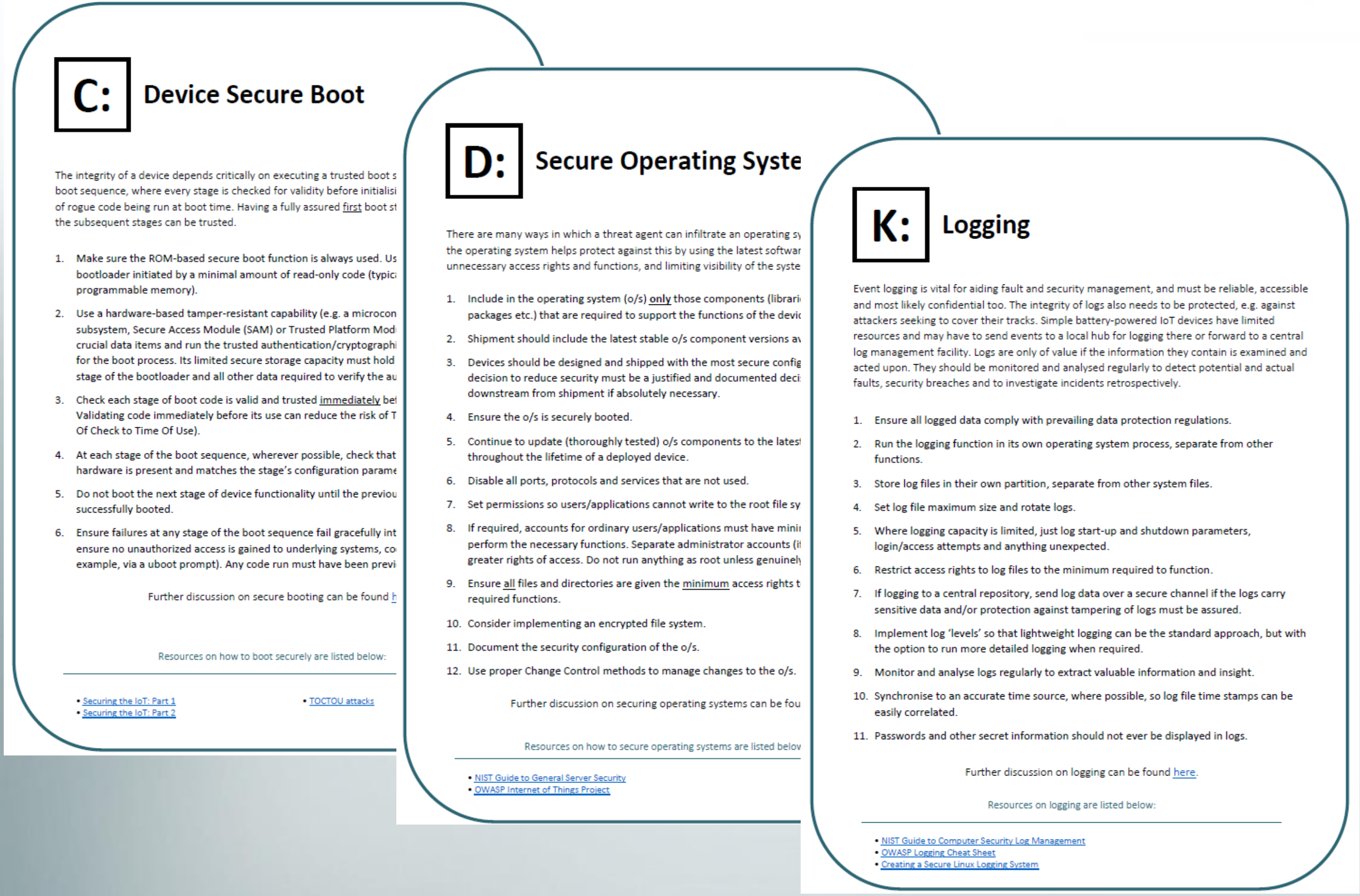
But ***there are also unknown unknowns, the ones we don't know we don't know****."*

Donald Rumsfeld (former U.S. Secretary of Defense) response to a question at a U.S. Department of Defense news briefing on February 12, 2002 about the lack of evidence linking the government of Iraq with the supply of weapons of mass destruction to terrorist groups.

Our Mission: *Make it Safe to Connect*

Our mission is to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this we will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems.

Build Secure, Buy Secure, Be Secure



C: Device Secure Boot

The integrity of a device depends critically on executing a trusted boot s
boot sequence, where every stage is checked for validity before initialisi
of rogue code being run at boot time. Having a fully assured first boot st
the subsequent stages can be trusted.

1. Make sure the ROM-based secure boot function is always used. Us
   bootloader initiated by a minimal amount of read-only code (typic
   programmable memory).
2. Use a hardware-based tamper-resistant capability (e.g. a microcon
   subsystem, Secure Access Module (SAM) or Trusted Platform Mod
   crucial data items and run the trusted authentication/cryptographi
   for the boot process. Its limited secure storage capacity must hold
   stage of the bootloader and all other data required to verify the au
3. Check each stage of boot code is valid and trusted immediately bef
   Validating code immediately before its use can reduce the risk of T
   Of Check to Time Of Use).
4. At each stage of the boot sequence, wherever possible, check that
   hardware is present and matches the stage's configuration parame
5. Do not boot the next stage of device functionality until the previou
   successfully booted.
6. Ensure failures at any stage of the boot sequence fail gracefully int
   ensure no unauthorized access is gained to underlying systems, co
   example, via a uboot prompt). Any code run must have been previ

Further discussion on secure booting can be found h

Resources on how to boot securely are listed below:

- Securing the IoT: Part 1
- Securing the IoT: Part 2
- TOCTOU attacks

D: Secure Operating Syste

There are many ways in which a threat agent can infiltrate an operating sy
the operating system helps protect against this by using the latest softwar
unnecessary access rights and functions, and limiting visibility of the syste

1. Include in the operating system (o/s) only those components (librari
   packages etc.) that are required to support the functions of the devic
2. Shipment should include the latest stable o/s component versions av
3. Devices should be designed and shipped with the most secure config
   decision to reduce security must be a justified and documented deci
   downstream from shipment if absolutely necessary.
4. Ensure the o/s is securely booted.
5. Continue to update (thoroughly tested) o/s components to the latest
   throughout the lifetime of a deployed device.
6. Disable all ports, protocols and services that are not used.
7. Set permissions so users/applications cannot write to the root file sy
8. If required, accounts for ordinary users/applications must have mini
   perform the necessary functions. Separate administrator accounts (i
   greater rights of access. Do not run anything as root unless genuinel
9. Ensure all files and directories are given the minimum access rights t
   required functions.
10. Consider implementing an encrypted file system.
11. Document the security configuration of the o/s.
12. Use proper Change Control methods to manage changes to the o/s.

Further discussion on securing operating systems can be fou

Resources on how to secure operating systems are listed belov

- NIST Guide to General Server Security
- OWASP Internet of Things Project

K: Logging

Event logging is vital for aiding fault and security management, and must be reliable, accessible and most likely confidential too. The integrity of logs also needs to be protected, e.g. against attackers seeking to cover their tracks. Simple battery-powered IoT devices have limited resources and may have to send events to a local hub for logging there or forward to a central log management facility. Logs are only of value if the information they contain is examined and acted upon. They should be monitored and analysed regularly to detect potential and actual faults, security breaches and to investigate incidents retrospectively.

1. Ensure all logged data comply with prevailing data protection regulations.
2. Run the logging function in its own operating system process, separate from other functions.
3. Store log files in their own partition, separate from other system files.
4. Set log file maximum size and rotate logs.
5. Where logging capacity is limited, just log start-up and shutdown parameters, login/access attempts and anything unexpected.
6. Restrict access rights to log files to the minimum required to function.
7. If logging to a central repository, send log data over a secure channel if the logs carry sensitive data and/or protection against tampering of logs must be assured.
8. Implement log 'levels' so that lightweight logging can be the standard approach, but with the option to run more detailed logging when required.
9. Monitor and analyse logs regularly to extract valuable information and insight.
10. Synchronise to an accurate time source, where possible, so log file time stamps can be easily correlated.
11. Passwords and other secret information should not ever be displayed in logs.

Further discussion on logging can be found here.

Resources on logging are listed below:

- NIST Guide to Computer Security Log Management
- OWASP Logging Cheat Sheet
- Creating a Secure Linux Logging System

A - Classification of Data
B - Physical Security
C - Device Secure Boot
D - Secure Operating System
E - Application Security
F - Credential Management
G - Encryption
H - Network Connections
J - Securing Software Updates
K - Logging
L - Software Update Policy

How to use the Compliance Framework Release 2.0

Engaging with IoT Security Best Practices

Chris Shire

Infineon

IoTSF Compliance Framework V2.0 Overview Agenda

- Introduction
- What's New
- How to use the Framework
- Next Steps

IoTSF Compliance Framework Introduction

- Allows an IoT product to be assessed for security
  - Can be self-assessed or used by a 3rd party
- The collective output of 30+ IoTSF members and 2+ years of work.
- Requires expertise, time and effort

IoTSF Compliance Framework Introduction

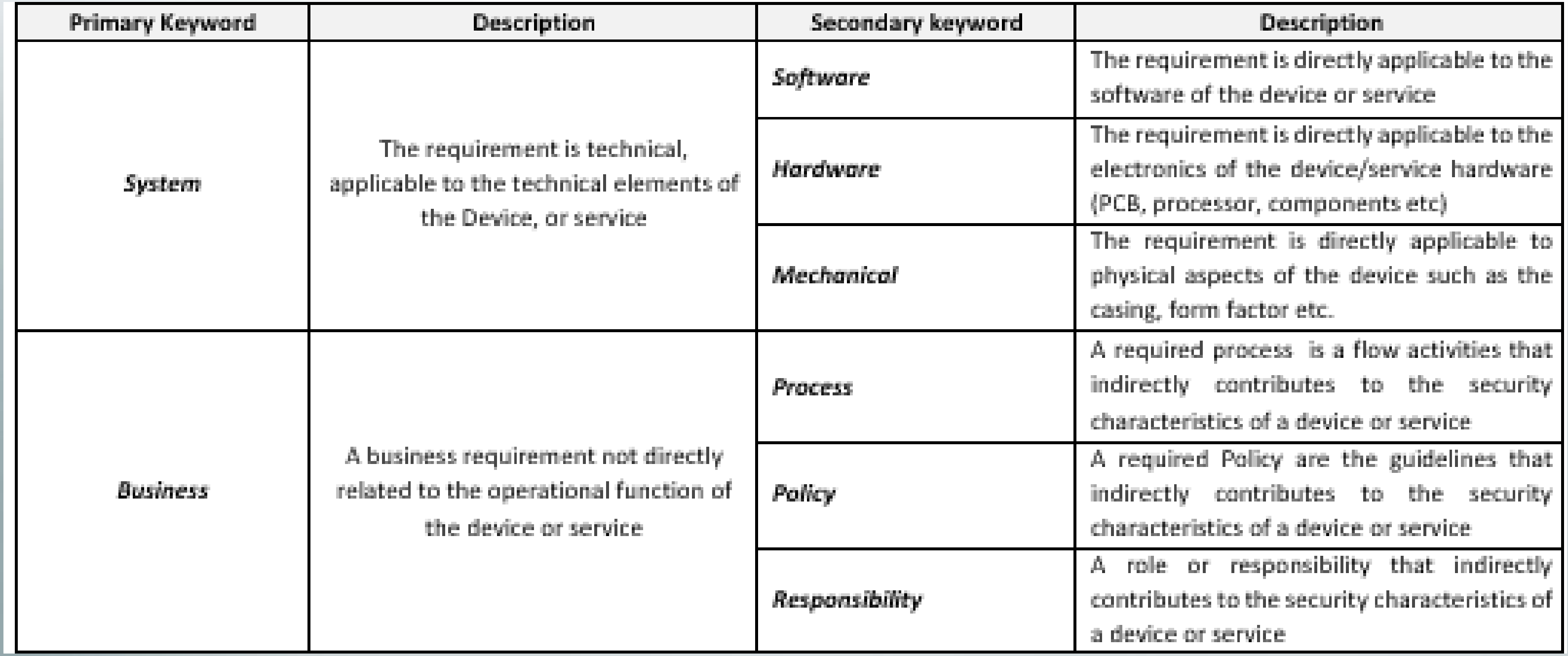
- Why use it?
- What is inside?
- Who should use it?
- How to use it?
- When to use it?

- If an IoT product has risks
- 200+ checks and hints
- Anyone involved with IoT
- Employ security experts
- From product conception

Framework Outline

Key Requirements	Objective
Management governance	There must be a named executive responsible for product security, and privacy of customer information.
Engineered for security	The hardware and software must be designed with attention to security threats.
Fit for purpose cryptography	These functions should be from the best practice industry standards.
Secure network framework and applications	Precautions have been taken to secure Apps, web interfaces and server software
Secure production processes and supply chain	Making sure the security of the product is not compromised in the manufacturing process or in the end customer delivery and installation.
Safe and secure for the customer	The product is safe and secure "out of the box" and in its day to day use.

What's New with Version 2: Keywords

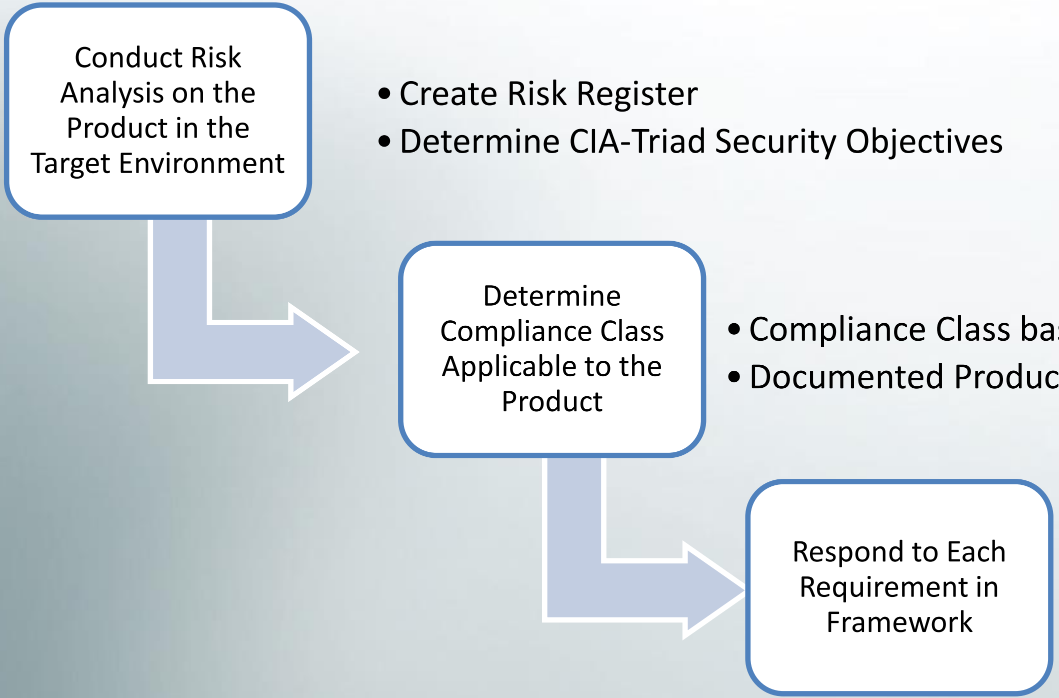


Primary Keyword	Description	Secondary keyword	Description
System	The requirement is technical, applicable to the technical elements of the Device, or service	*Software*	The requirement is directly applicable to the software of the device or service
		Hardware	The requirement is directly applicable to the electronics of the device/service hardware (PCB, processor, components etc)
		Mechanical	The requirement is directly applicable to physical aspects of the device such as the casing, form factor etc.
Business	A business requirement not directly related to the operational function of the device or service	*Process*	A required process is a flow activities that indirectly contributes to the security characteristics of a device or service
		Policy	A required Policy are the guidelines that indirectly contributes to the security characteristics of a device or service
		Responsibility	A role or responsibility that indirectly contributes to the security characteristics of a device or service

What Else? Deletions & Additions

- One schema for all applications
  - Compliance Class varies by risk appetite
- Deleted:
  - Product Categories
- Additions:
  - Keywords for each requirement to ease assessment
  - User Guidance
  - Enhanced introduction with Benefits and Key Requirements.

IoTSF Compliance Framework
Step by Step...



Conduct Risk Analysis on the Product in the Target Environment

- Create Risk Register
- Determine CIA-Triad Security Objectives

Determine Compliance Class Applicable to the Product

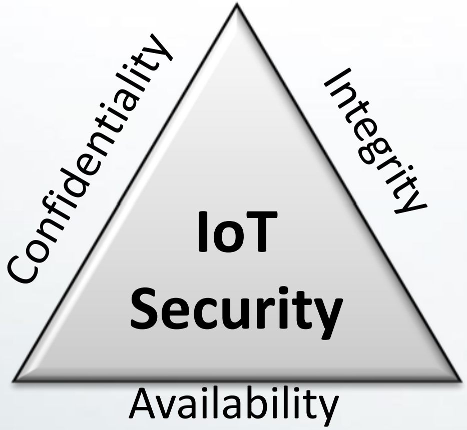
- Compliance Class based on Security Objectives
- Documented Product Environment

Respond to Each Requirement in Framework

- Complete Compliance Checklist(Excel)
- Reference Evidence Documents

Security Objectives

- The CIA Triad



  - Confidentiality : control of data
  - Integrity : assure the data can be trusted
  - Availability : ensure reliable , authorised access

Security Objectives - Confidentiality

- **Basic** – devices processing public information
- **Medium** – devices processing sensitive information, including Personally Identifiable Information, whose compromise would have limited impact on an individual or organisation
- **High** - devices processing very sensitive information, including sensitive personal data whose compromise would have significant impact on an individual or organisation

Security Objectives - Integrity

- Basic - resists low level threat sources that have very little capability and priority
- Medium - threat sources that have from very little, focussed capability, through to researchers with significant capability
- High - devices resist substantial level threat sources

Security Objectives - Availability

- Basic - devices whose lack of availability would cause minor disruption
- Medium – devices whose lack of availability would have limited impact on an individual or organisation
- High – devices whose lack of availability would have significant impact to an individual or organisation, or impacts many individuals

Compliance Class

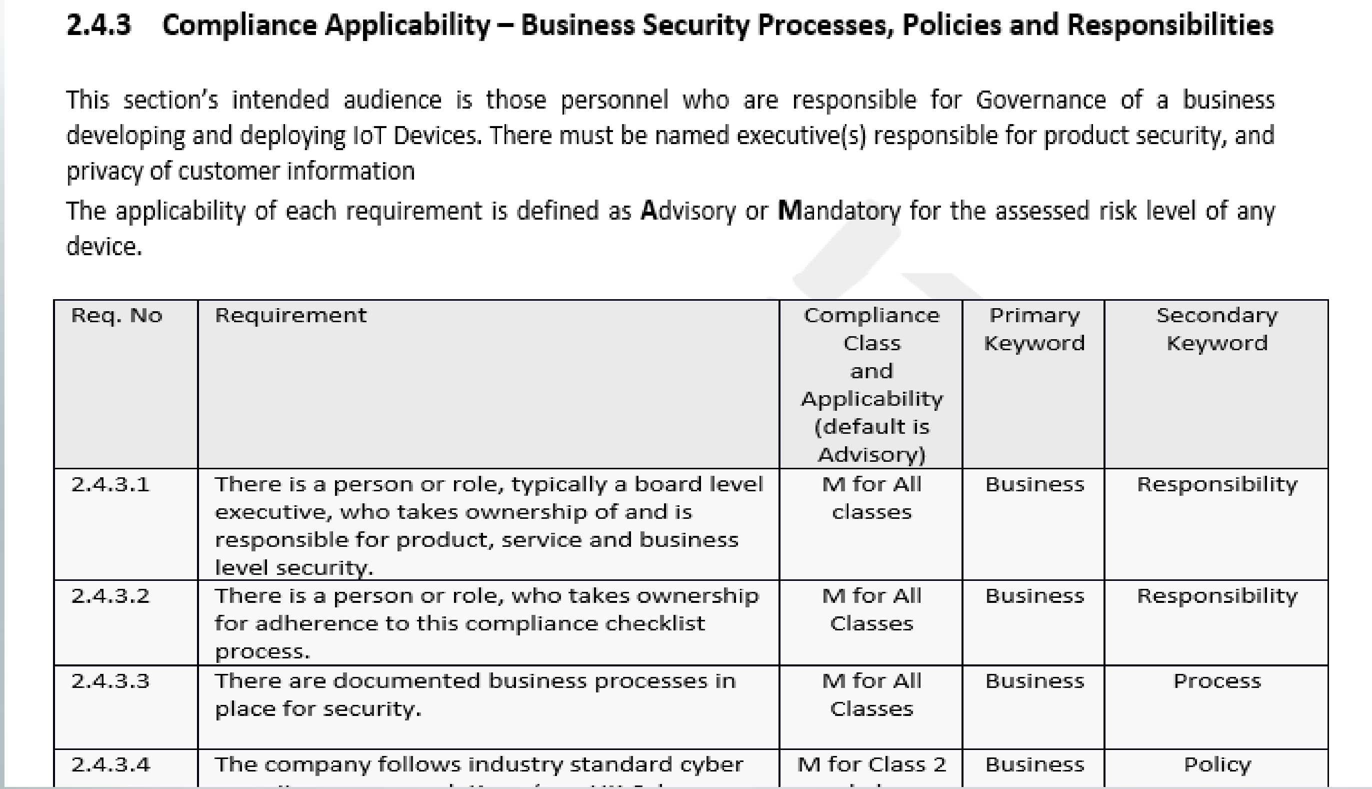
The requirements in the Framework are classified as follows:

- ***Class 0:*** *where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or* organisation.
- ***Class 1:*** *where compromise to the data generated or loss of control is likely to result in no more than limited impact on an individual or organisation.*
- ***Class 2:*** *in addition to class 1, the device is designed to resist attacks on availability that would have significant* impact *on an individual or organisation, or impact many individuals. For example by limiting operations of an infrastructure to which it is connected.*
- ***Class 3:*** *in addition to class 2, the device is designed to protect sensitive data including sensitive personal data.*
- ***Class 4:*** *in addition to class 3, where compromise to the data generated or loss of control have the potential to affect critical infrastructure or cause personal injury.*

Compliance Class : Security Objectives

Compliance Class	Security Objective		
	Confidentiality	**Integrity**	**Availability**
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

IoTSF Compliance Framework – Assessment



2.4.3 Compliance Applicability – Business Security Processes, Policies and Responsibilities

This section's intended audience is those personnel who are responsible for Governance of a business developing and deploying IoT Devices. There must be named executive(s) responsible for product security, and privacy of customer information

The applicability of each requirement is defined as **A**dvisory or **M**andatory for the assessed risk level of any device.

Req. No	Requirement	Compliance Class and Applicability (default is Advisory)	Primary Keyword	Secondary Keyword
2.4.3.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security.	M for All classes	Business	Responsibility
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance checklist process.	M for All Classes	Business	Responsibility
2.4.3.3	There are documented business processes in place for security.	M for All Classes	Business	Process
2.4.3.4	The company follows industry standard cyber	M for Class 2	Business	Policy

IoTSF Compliance Framework – Next Steps

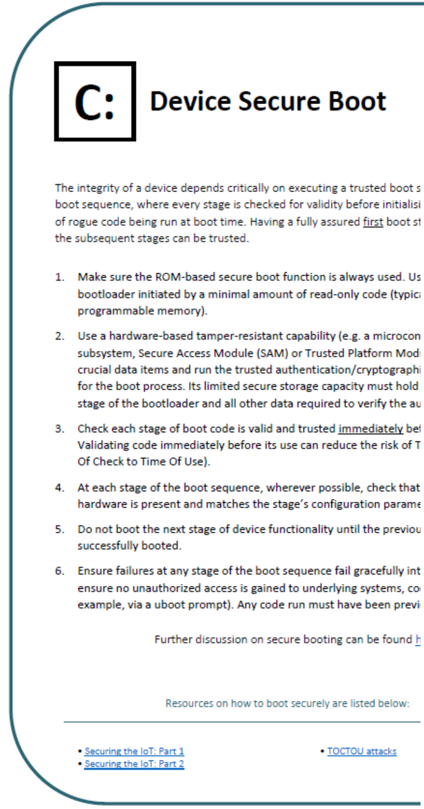
1. When a new IoT product is conceived, as part of the business planning, conduct a top level risk assessment to scope the threats, impacts, and mitigations.
2. Ask the IoTSF for advice.

How to use the Best Practice Guides

Engaging with IoT Security Best Practices

Jeff Day

BT



C: Device Secure Boot

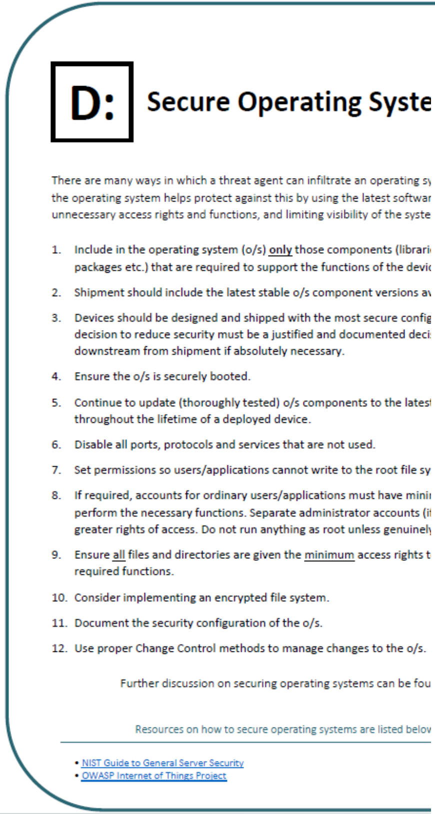
The integrity of a device depends critically on executing a trusted boot s
boot sequence, where every stage is checked for validity before initialisi
of rogue code being run at boot time. Having a fully assured first boot st
the subsequent stages can be trusted.

1. Make sure the ROM-based secure boot function is always used. Us
bootloader initiated by a minimal amount of read-only code (typic
programmable memory).
2. Use a hardware-based tamper-resistant capability (e.g. a microcon
subsystem, Secure Access Module (SAM) or Trusted Platform Mod
crucial data items and run the trusted authentication/cryptographi
for the boot process. Its limited secure storage capacity must hold
stage of the bootloader and all other data required to verify the au
3. Check each stage of boot code is valid and trusted immediately bel
Validating code immediately before its use can reduce the risk of T
Of Check to Time Of Use).
4. At each stage of the boot sequence, wherever possible, check that
hardware is present and matches the stage's configuration parame
5. Do not boot the next stage of device functionality until the previou
successfully booted.
6. Ensure failures at any stage of the boot sequence fail gracefully int
ensure no unauthorized access is gained to underlying systems, co
example, via a uboot prompt). Any code run must have been previ

Further discussion on secure booting can be found h

Resources on how to boot securely are listed below:

- Securing the IoT: Part 1
- Securing the IoT: Part 2
- TOCTOU attacks



D: Secure Operating Syste

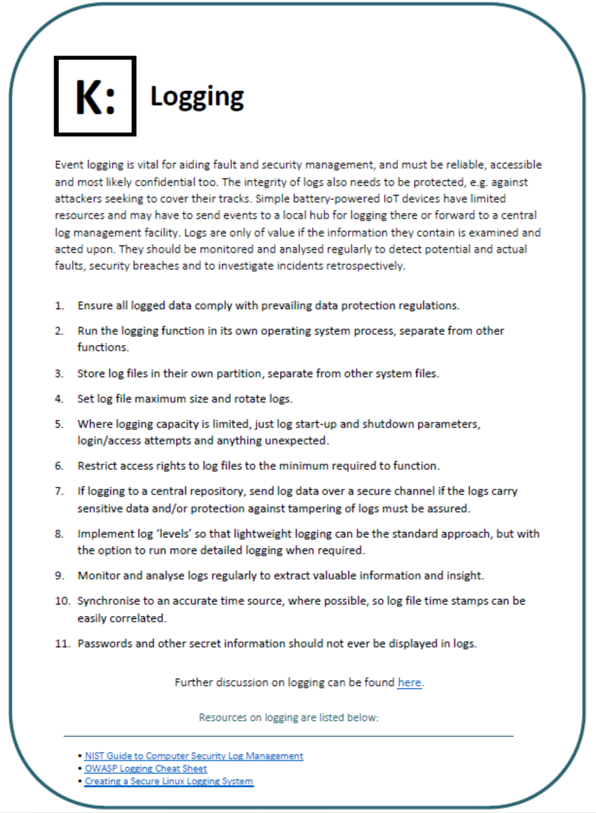
There are many ways in which a threat agent can infiltrate an operating sy
the operating system helps protect against this by using the latest softwar
unnecessary access rights and functions, and limiting visibility of the syste

1. Include in the operating system (o/s) only those components (librari
packages etc.) that are required to support the functions of the devic
2. Shipment should include the latest stable o/s component versions av
3. Devices should be designed and shipped with the most secure config
decision to reduce security must be a justified and documented deci
downstream from shipment if absolutely necessary.
4. Ensure the o/s is securely booted.
5. Continue to update (thoroughly tested) o/s components to the latest
throughout the lifetime of a deployed device.
6. Disable all ports, protocols and services that are not used.
7. Set permissions so users/applications cannot write to the root file sy
8. If required, accounts for ordinary users/applications must have minii
perform the necessary functions. Separate administrator accounts (i
greater rights of access. Do not run anything as root unless genuinel
9. Ensure all files and directories are given the minimum access rights t
required functions.
10. Consider implementing an encrypted file system.
11. Document the security configuration of the o/s.
12. Use proper Change Control methods to manage changes to the o/s.

Further discussion on securing operating systems can be fou

Resources on how to secure operating systems are listed belov

- NIST Guide to General Server Security
- OWASP Internet of Things Project



K: Logging

Event logging is vital for aiding fault and security management, and must be reliable, accessible and most likely confidential too. The integrity of logs also needs to be protected, e.g. against attackers seeking to cover their tracks. Simple battery-powered IoT devices have limited resources and may have to send events to a local hub for logging there or forward to a central log management facility. Logs are only of value if the information they contain is examined and acted upon. They should be monitored and analysed regularly to detect potential and actual faults, security breaches and to investigate incidents retrospectively.

1. Ensure all logged data comply with prevailing data protection regulations.
2. Run the logging function in its own operating system process, separate from other functions.
3. Store log files in their own partition, separate from other system files.
4. Set log file maximum size and rotate logs.
5. Where logging capacity is limited, just log start-up and shutdown parameters, login/access attempts and anything unexpected.
6. Restrict access rights to log files to the minimum required to function.
7. If logging to a central repository, send log data over a secure channel if the logs carry sensitive data and/or protection against tampering of logs must be assured.
8. Implement log 'levels' so that lightweight logging can be the standard approach, but with the option to run more detailed logging when required.
9. Monitor and analyse logs regularly to extract valuable information and insight.
10. Synchronise to an accurate time source, where possible, so log file time stamps can be easily correlated.
11. Passwords and other secret information should not ever be displayed in logs.

Further discussion on logging can be found here.

Resources on logging are listed below:

- NIST Guide to Computer Security Log Management
- OWASP Logging Cheat Sheet
- Creating a Secure Linux Logging System

Key Areas to Secure

- Understand the Data
- Physically secure the installation
- Secure all the software
- Manage who gets on the system
- Connect to the network securely
- Implement & manage s/w updates
- Keep track of what’s happening on the system

Key Areas to Secure <-> BPGs

Key Areas to Secure	Best Practice Guide
Understand the Data	A: Classification of Data
Physically secure the installation	B: Physical Security
Secure all the software	C: Device Secure Boot
	D: Secure Operating System
	E: Application Security
Manage who gets on the system	F: Credential Management
	G: Encryption
Connect to the network securely	H: Network Connections
Implement & manage s/w updates	J: Securing Software Updates
	L: Software Update Policy
Keep track of what's happening on the system	K: Logging

A - Classification of Data

B - Physical Security

C - Device Secure Boot

D - Secure Operating System

E - Application Security

F - Credential Management

G - Encryption

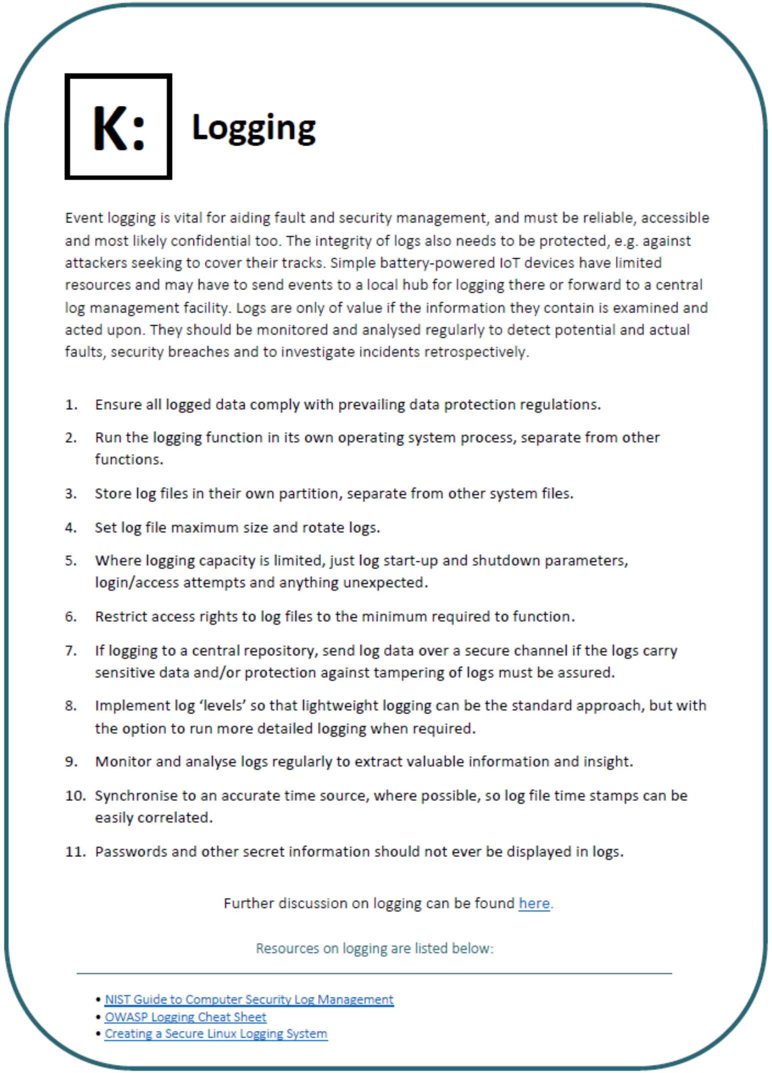
H - Network Connections

J - Securing Software Updates

K - Logging

L - Software Update Policy

Example BPG



K: Logging

Event logging is vital for aiding fault and security management, and must be reliable, accessible and most likely confidential too. The integrity of logs also needs to be protected, e.g. against attackers seeking to cover their tracks. Simple battery-powered IoT devices have limited resources and may have to send events to a local hub for logging there or forward to a central log management facility. Logs are only of value if the information they contain is examined and acted upon. They should be monitored and analysed regularly to detect potential and actual faults, security breaches and to investigate incidents retrospectively.

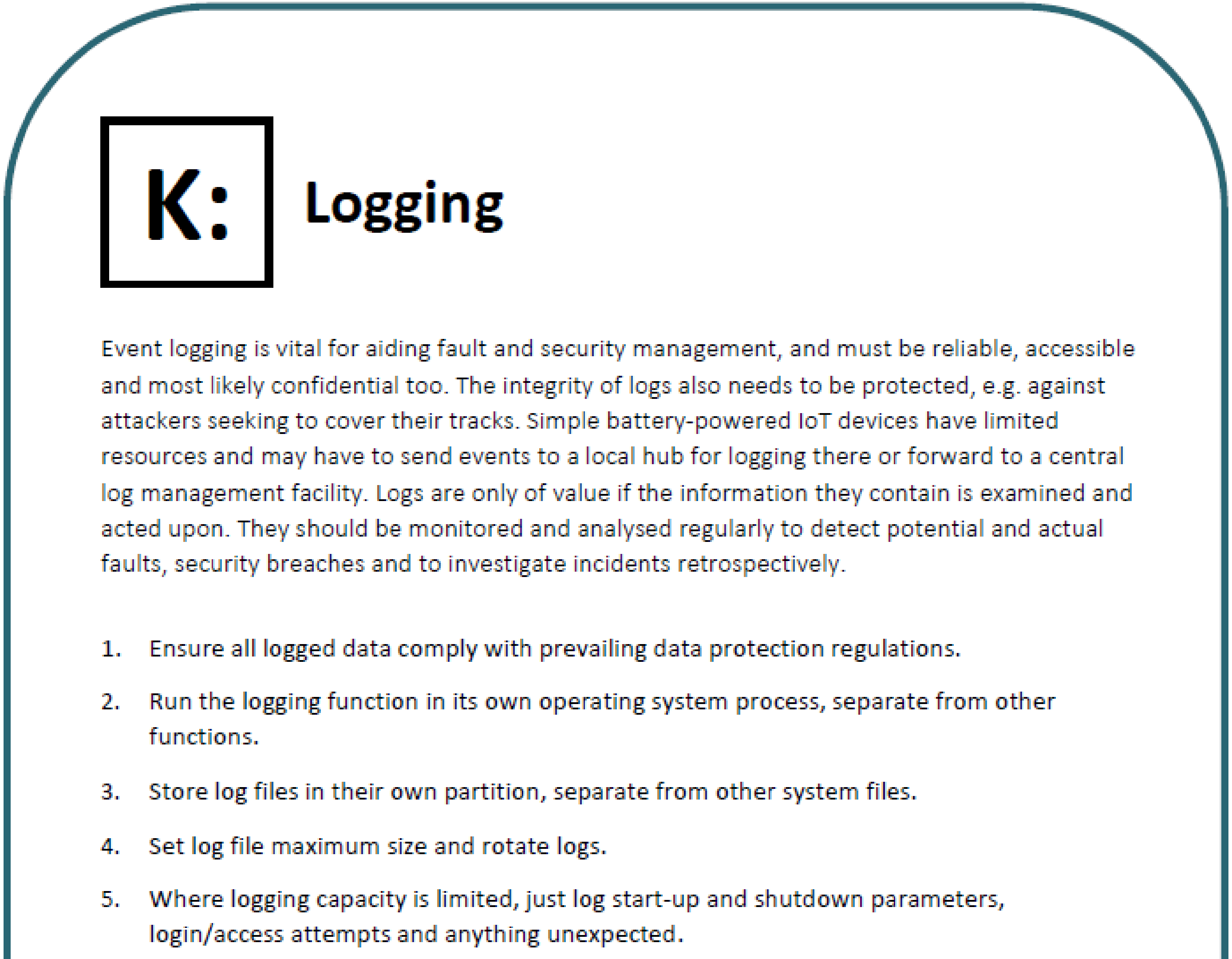
1. Ensure all logged data comply with prevailing data protection regulations.
2. Run the logging function in its own operating system process, separate from other functions.
3. Store log files in their own partition, separate from other system files.
4. Set log file maximum size and rotate logs.
5. Where logging capacity is limited, just log start-up and shutdown parameters, login/access attempts and anything unexpected.
6. Restrict access rights to log files to the minimum required to function.
7. If logging to a central repository, send log data over a secure channel if the logs carry sensitive data and/or protection against tampering of logs must be assured.
8. Implement log 'levels' so that lightweight logging can be the standard approach, but with the option to run more detailed logging when required.
9. Monitor and analyse logs regularly to extract valuable information and insight.
10. Synchronise to an accurate time source, where possible, so log file time stamps can be easily correlated.
11. Passwords and other secret information should not ever be displayed in logs.

Further discussion on logging can be found here.

Resources on logging are listed below:

- NIST Guide to Computer Security Log Management
- OWASP Logging Cheat Sheet
- Creating a Secure Linux Logging System

Example BPG: Logging (Upper half)

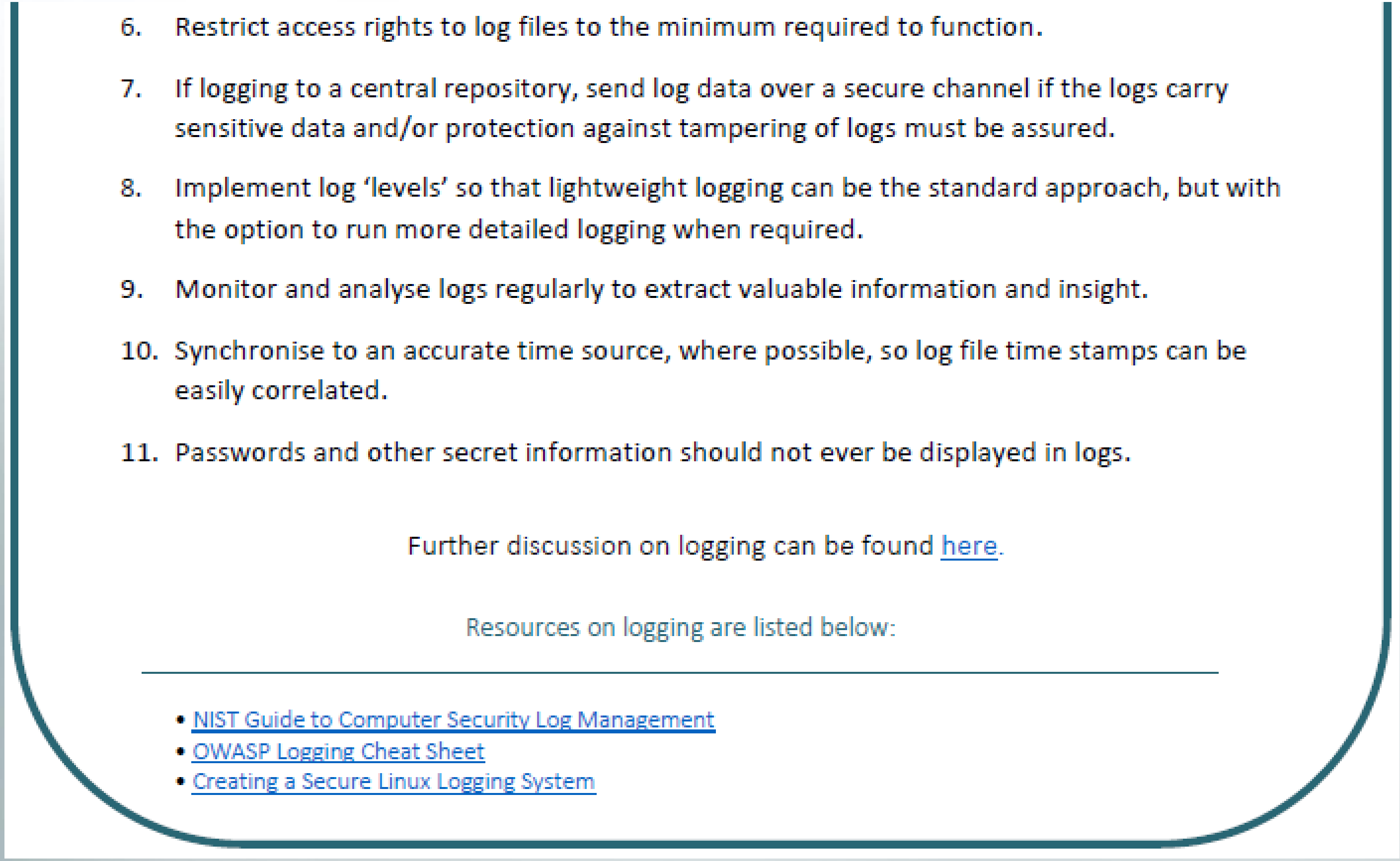


K: Logging

Event logging is vital for aiding fault and security management, and must be reliable, accessible and most likely confidential too. The integrity of logs also needs to be protected, e.g. against attackers seeking to cover their tracks. Simple battery-powered IoT devices have limited resources and may have to send events to a local hub for logging there or forward to a central log management facility. Logs are only of value if the information they contain is examined and acted upon. They should be monitored and analysed regularly to detect potential and actual faults, security breaches and to investigate incidents retrospectively.

1. Ensure all logged data comply with prevailing data protection regulations.
2. Run the logging function in its own operating system process, separate from other functions.
3. Store log files in their own partition, separate from other system files.
4. Set log file maximum size and rotate logs.
5. Where logging capacity is limited, just log start-up and shutdown parameters, login/access attempts and anything unexpected.

Example BPG: Logging (Lower half)



6. Restrict access rights to log files to the minimum required to function.
7. If logging to a central repository, send log data over a secure channel if the logs carry sensitive data and/or protection against tampering of logs must be assured.
8. Implement log 'levels' so that lightweight logging can be the standard approach, but with the option to run more detailed logging when required.
9. Monitor and analyse logs regularly to extract valuable information and insight.
10. Synchronise to an accurate time source, where possible, so log file time stamps can be easily correlated.
11. Passwords and other secret information should not ever be displayed in logs.

Further discussion on logging can be found here.

Resources on logging are listed below:

- NIST Guide to Computer Security Log Management
- OWASP Logging Cheat Sheet
- Creating a Secure Linux Logging System

References from the Compliance Framework

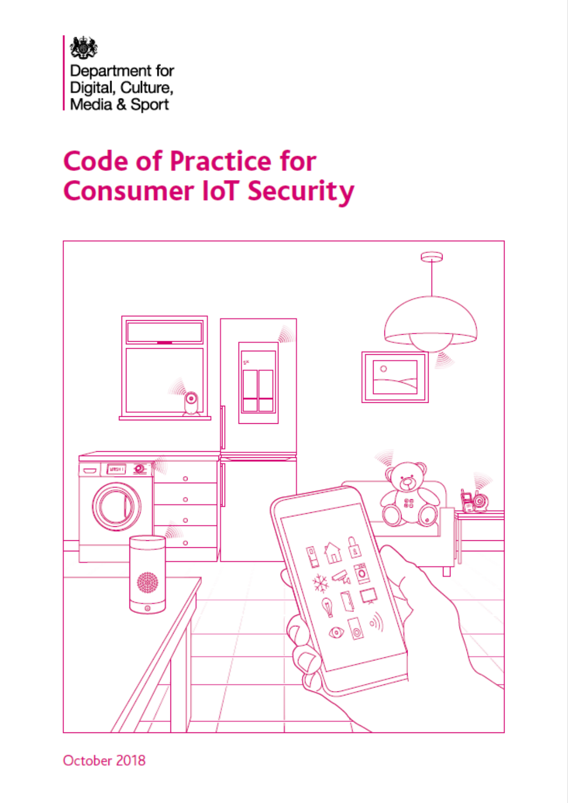
Examples:

> *“This section’s intended audience is those personnel who are responsible for hardware and mechanical quality. Guidance is available from the IoTSF [Ref 44] regarding Physical Security (part B) Secure Boot (part C), Secure Operating Systems (part D).”*

> “This section’s intended audience is for those personnel who are responsible for device application quality e.g. Software Architects, Product Owners, and Release Managers. Guidance is available from the IoTSF [Ref44] regarding Secure Operating Systems (part D), Credential Management (Part F), and Software Updates (part J).”

> “This section’s intended audience is for those personnel who are responsible for device security. Guidance is available from the IoTSF [Ref44] regarding Credential Management (Part F), and Network Connections (part H).”

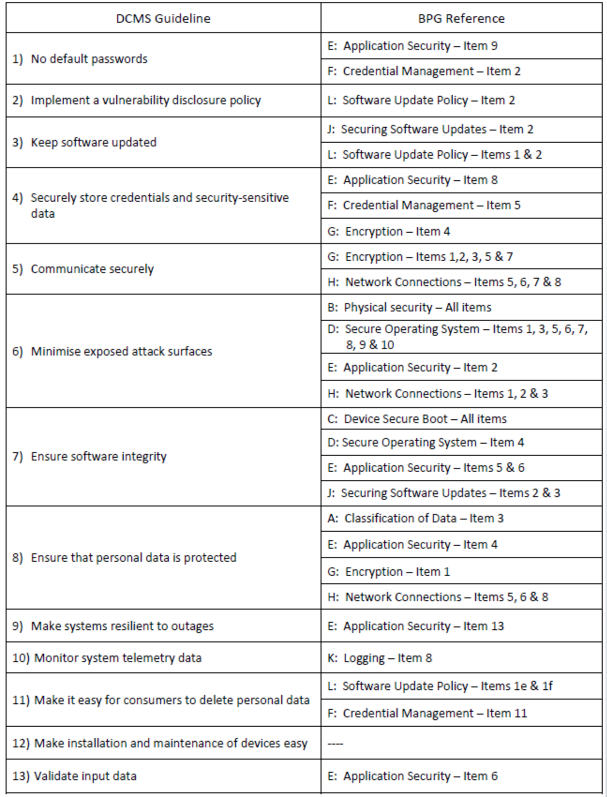
DCMS Code of Practice <-> BPG Mapping



Department for Digital, Culture, Media & Sport

Code of Practice for Consumer IoT Security

October 2018



DCMS Guideline	BPG Reference
1) No default passwords	E: Application Security – Item 9
	F: Credential Management – Item 2
2) Implement a vulnerability disclosure policy	L: Software Update Policy – Item 2
3) Keep software updated	J: Securing Software Updates – Item 2
	L: Software Update Policy – Items 1 & 2
4) Securely store credentials and security-sensitive data	E: Application Security – Item 8
	F: Credential Management – Item 5
	G: Encryption – Item 4
5) Communicate securely	G: Encryption – Items 1,2, 3, 5 & 7
	H: Network Connections – Items 5, 6, 7 & 8
6) Minimise exposed attack surfaces	B: Physical security – All items
	D: Secure Operating System – Items 1, 3, 5, 6, 7, 8, 9 & 10
	E: Application Security – Item 2
	H: Network Connections – Items 1, 2 & 3
7) Ensure software integrity	C: Device Secure Boot – All items
	D: Secure Operating System – Item 4
	E: Application Security – Items 5 & 6
	J: Securing Software Updates – Items 2 & 3
8) Ensure that personal data is protected	A: Classification of Data – Item 3
	E: Application Security – Item 4
	G: Encryption – Item 1
	H: Network Connections – Items 5, 6 & 8
9) Make systems resilient to outages	E: Application Security – Item 13
10) Monitor system telemetry data	K: Logging – Item 8
11) Make it easy for consumers to delete personal data	L: Software Update Policy – Items 1e & 1f
	F: Credential Management – Item 11
12) Make installation and maintenance of devices easy	----
13) Validate input data	E: Application Security – Item 6

Contents

DCMS <-> BPG Mapping

Executive Summary

A - Classification of Data

B - Physical Security

C - Device Secure Boot

D - Secure Operating System

E - Application Security

F - Credential Management

G - Encryption

H - Network Connections

J - Securing Software Updates

K - Logging

L - Software Update Policy

Best Practice Guides

Available on IoT Security Foundation web site

https://iotsecurityfoundation.org

More Guides and Articles coming in 2019!

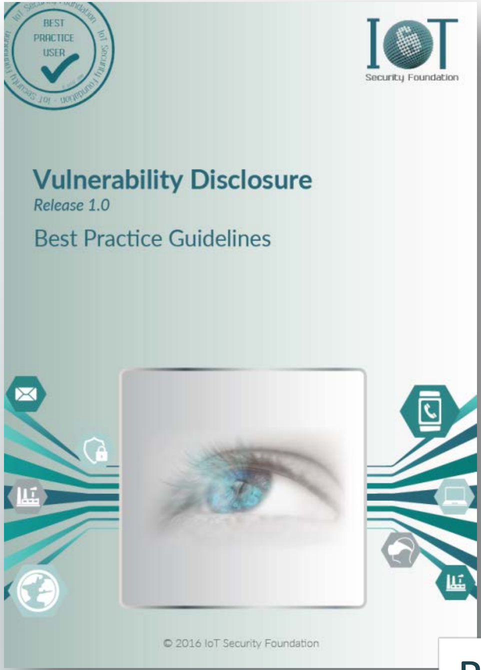
How to use the Vulnerability Disclosure Guide

Engaging with IoT Security Best Practices

Richard Marshall

IoTSF Plenary Chair

Vulnerability Disclosure



Vulnerability Disclosure

Release 1.0

Best Practice Guidelines

© 2016 IoT Security Foundation

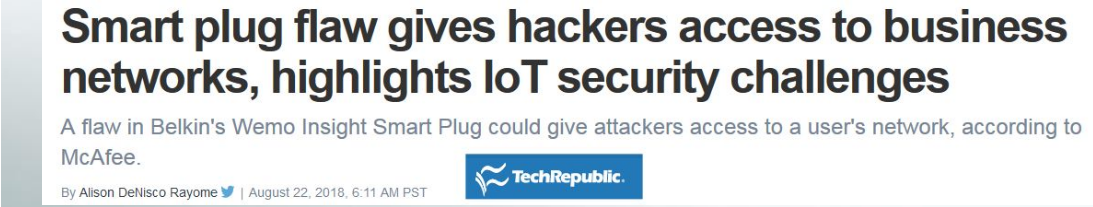
RELEASE 1.0

Post Product Launch

Is a Vulnerability Disclosure policy and process in place?

- Can you respond before your Company makes the…

Headlines…

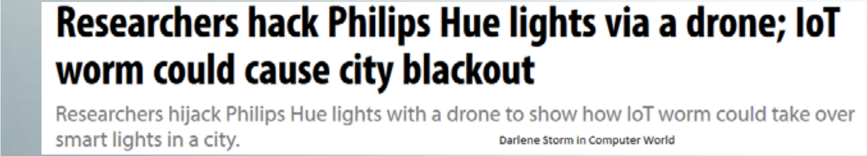


Smart plug flaw gives hackers access to business networks, highlights IoT security challenges

A flaw in Belkin's Wemo Insight Smart Plug could give attackers access to a user's network, according to McAfee.

By Alison DeNisco Rayome | August 22, 2018, 6:11 AM PST

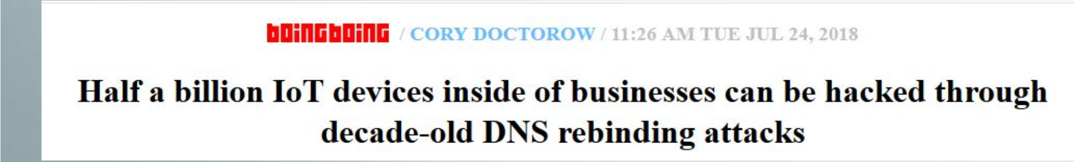
TechRepublic.



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

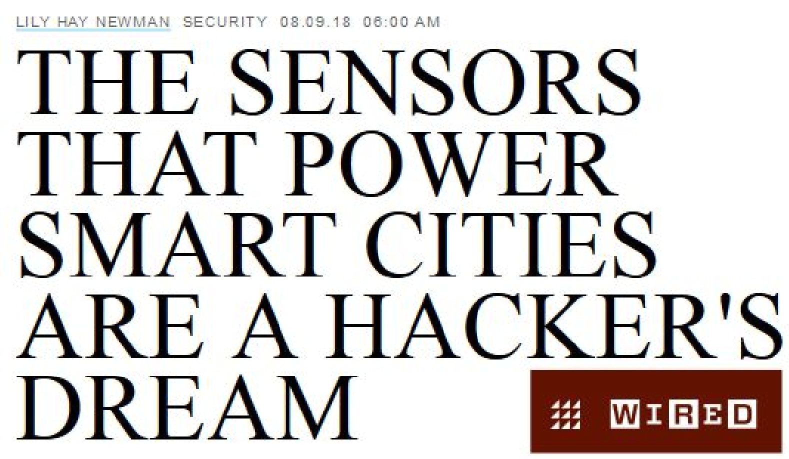
Researchers hijack Philips Hue lights with a drone to show how IoT worm could take over smart lights in a city.

Darlene Storm in Computer World



bOiNGbOiNG / CORY DOCTOROW / 11:26 AM TUE JUL 24, 2018

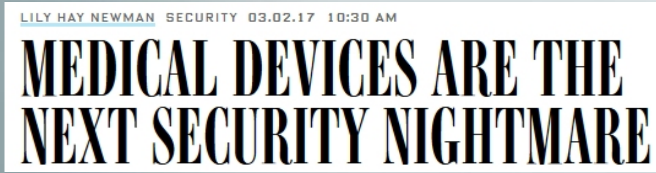
Half a billion IoT devices inside of businesses can be hacked through decade-old DNS rebinding attacks



LILY HAY NEWMAN SECURITY 08.09.18 06:00 AM

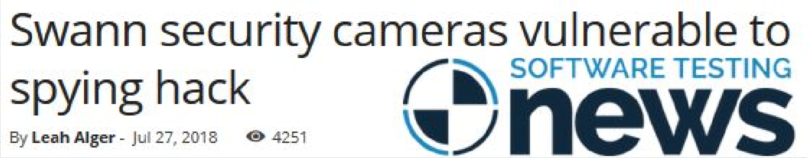
THE SENSORS THAT POWER SMART CITIES ARE A HACKER'S DREAM

WIRED



LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE



Swann security cameras vulnerable to spying hack

By Leah Alger - Jul 27, 2018 4251

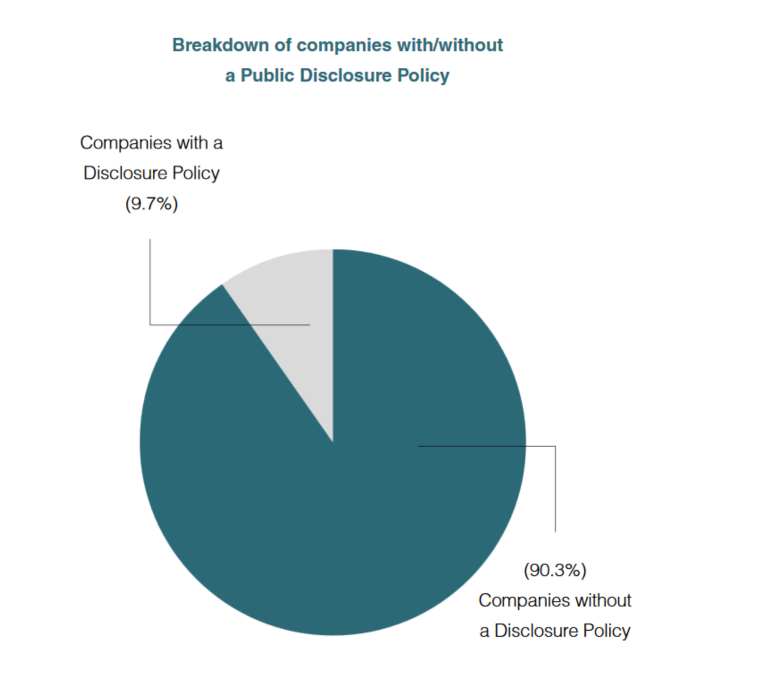
SOFTWARE TESTING news

How common?

331 Consumer Product Companies reviewed for a Vulnerability Disclosure policy…

- 90.3% did not have a publically declared policy
- Only 9.7% had a policy available for research contact

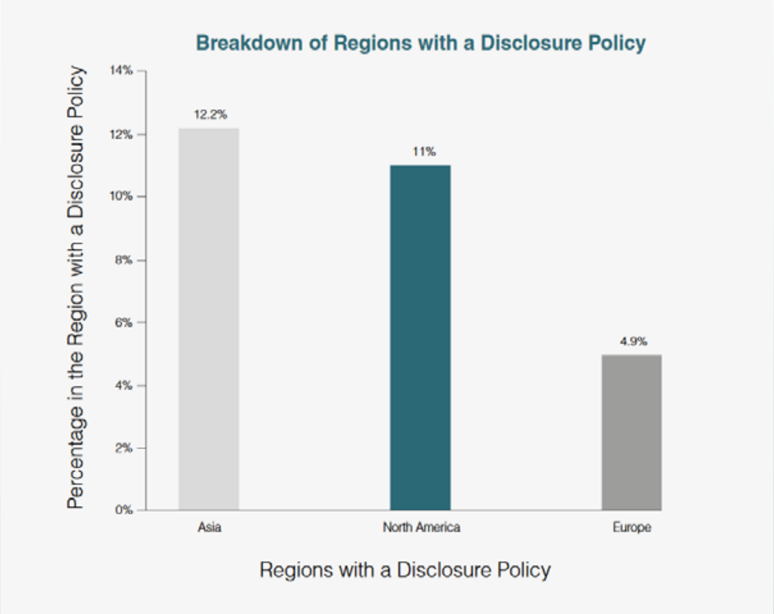
https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability-Disclosure-Design-v4.pdf



Regional Differences

Regional breakdown:

- Asia 12.2%
- North America 12.2%
- Europe 4.9%



https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability-Disclosure-Design-v4.pdf

Post Product Launch

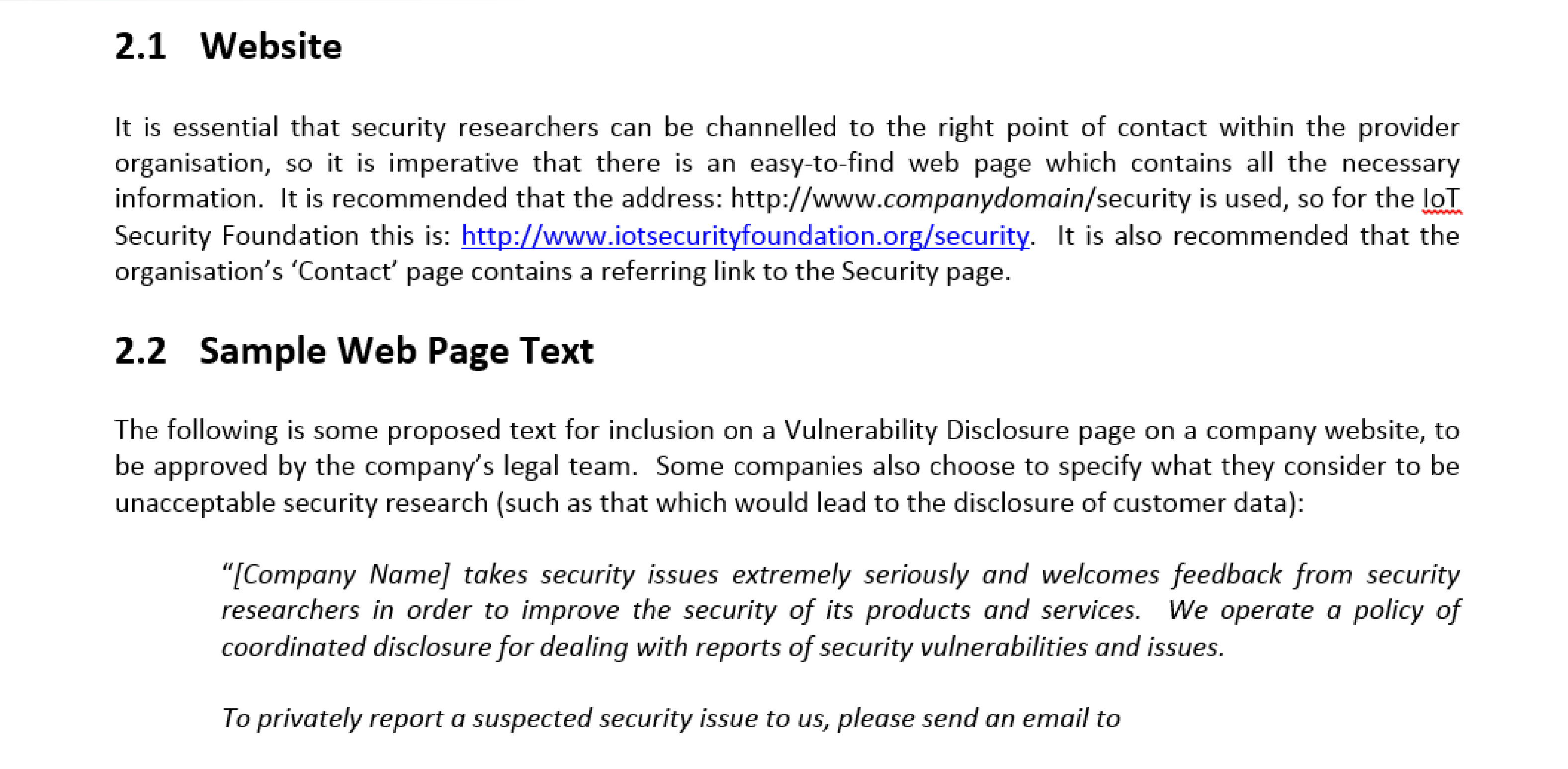
Is a Vulnerability Disclosure policy and process in place?

- Can you respond before your Company makes the…

Key Areas

- Point of contact
- Methods of contact
- Communications
- Resolving conflict
- Speed of response
- Acknowledgement and reward

Point of contact



2.1 Website

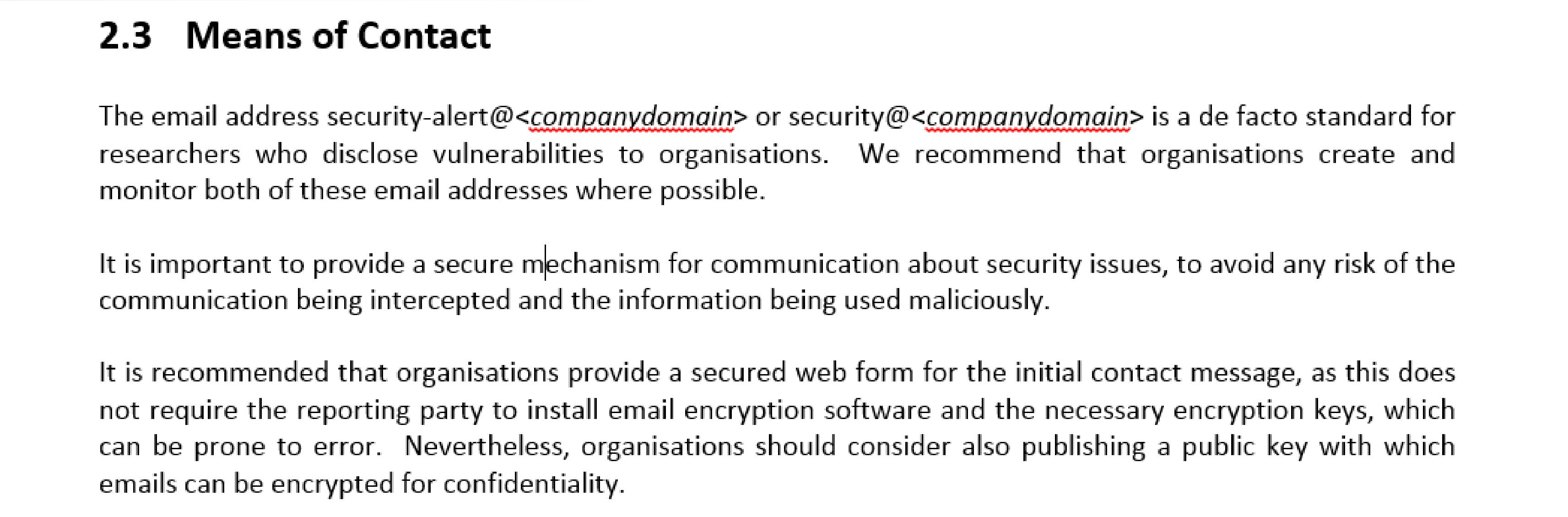
It is essential that security researchers can be channelled to the right point of contact within the provider organisation, so it is imperative that there is an easy-to-find web page which contains all the necessary information. It is recommended that the address: http://www.*companydomain*/security is used, so for the IoT Security Foundation this is: http://www.iotsecurityfoundation.org/security. It is also recommended that the organisation's 'Contact' page contains a referring link to the Security page.

2.2 Sample Web Page Text

The following is some proposed text for inclusion on a Vulnerability Disclosure page on a company website, to be approved by the company's legal team. Some companies also choose to specify what they consider to be unacceptable security research (such as that which would lead to the disclosure of customer data):

> *"[Company Name] takes security issues extremely seriously and welcomes feedback from security researchers in order to improve the security of its products and services. We operate a policy of coordinated disclosure for dealing with reports of security vulnerabilities and issues.*
>
> *To privately report a suspected security issue to us, please send an email to*

Methods of contact



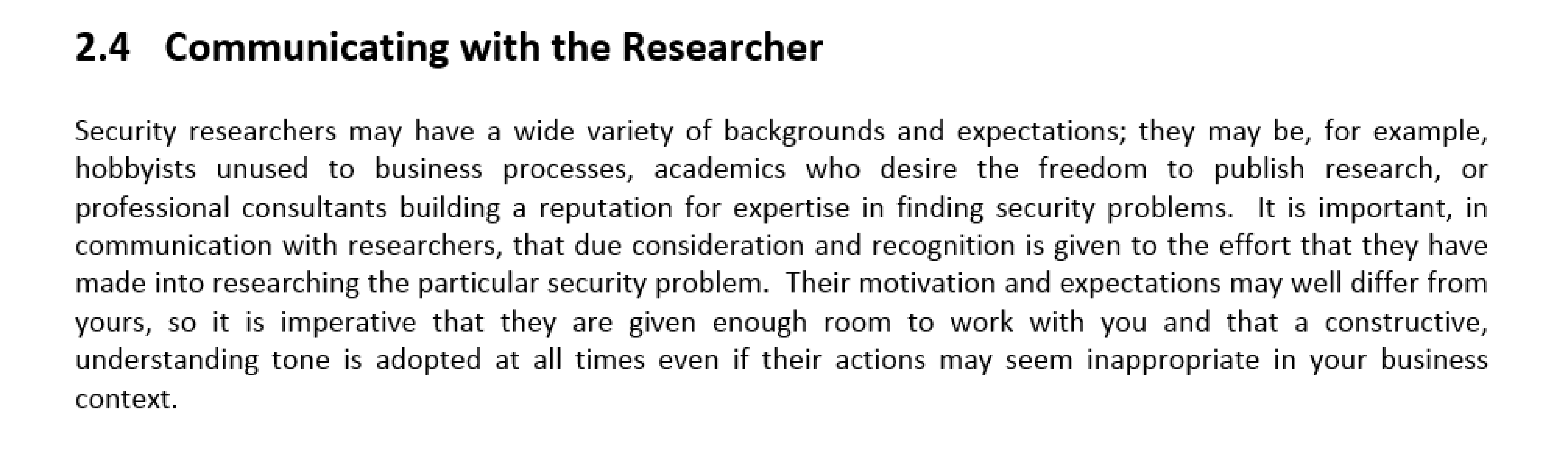
2.3 Means of Contact

The email address security-alert@<*companydomain*> or security@<*companydomain*> is a de facto standard for researchers who disclose vulnerabilities to organisations. We recommend that organisations create and monitor both of these email addresses where possible.

It is important to provide a secure mechanism for communication about security issues, to avoid any risk of the communication being intercepted and the information being used maliciously.

It is recommended that organisations provide a secured web form for the initial contact message, as this does not require the reporting party to install email encryption software and the necessary encryption keys, which can be prone to error. Nevertheless, organisations should consider also publishing a public key with which emails can be encrypted for confidentiality.

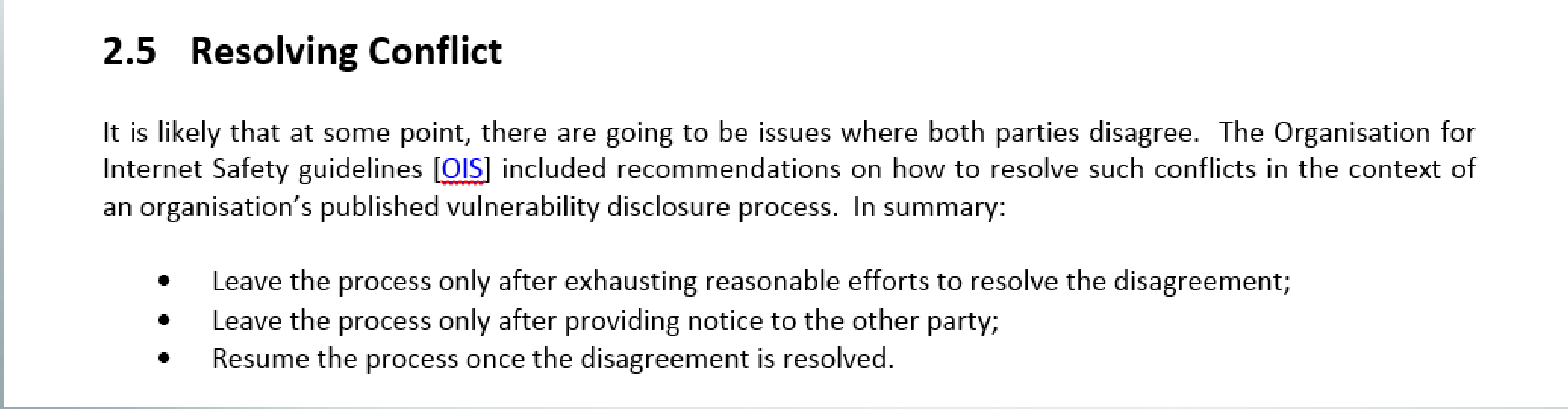
Communications



2.4 Communicating with the Researcher

Security researchers may have a wide variety of backgrounds and expectations; they may be, for example, hobbyists unused to business processes, academics who desire the freedom to publish research, or professional consultants building a reputation for expertise in finding security problems. It is important, in communication with researchers, that due consideration and recognition is given to the effort that they have made into researching the particular security problem. Their motivation and expectations may well differ from yours, so it is imperative that they are given enough room to work with you and that a constructive, understanding tone is adopted at all times even if their actions may seem inappropriate in your business context.

Resolving Conflict

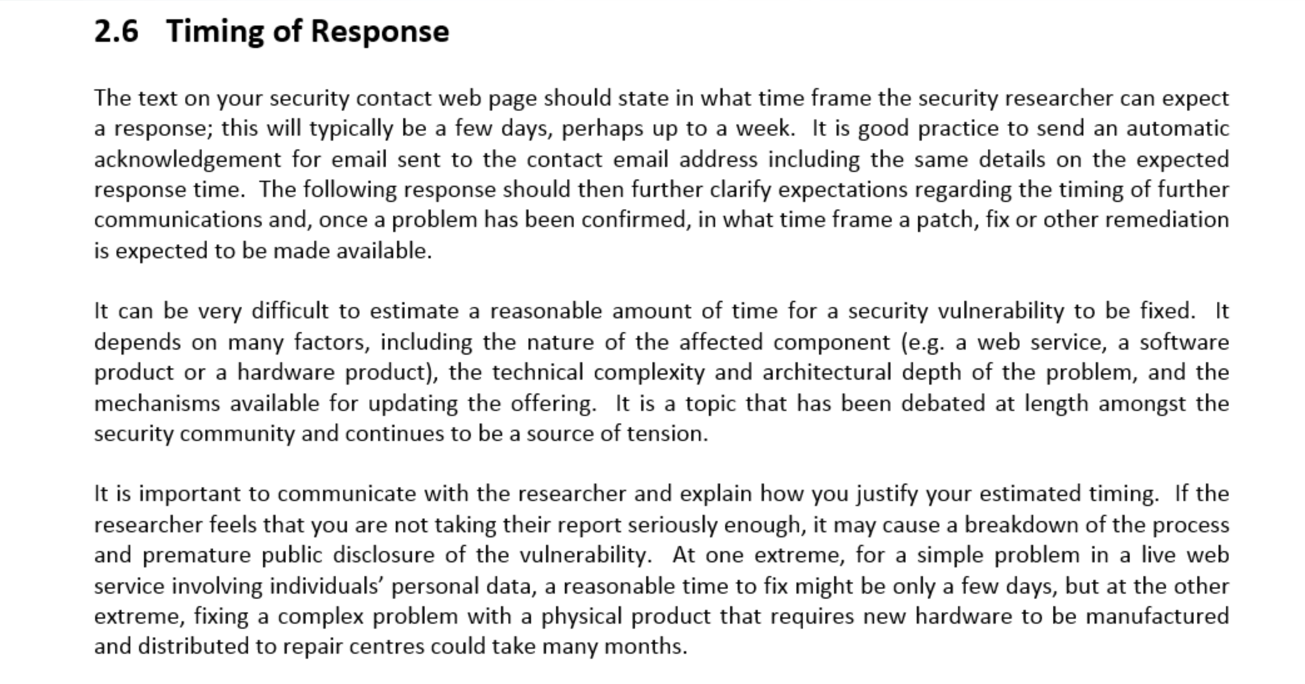


2.5 Resolving Conflict

It is likely that at some point, there are going to be issues where both parties disagree. The Organisation for Internet Safety guidelines [OIS] included recommendations on how to resolve such conflicts in the context of an organisation's published vulnerability disclosure process. In summary:

- Leave the process only after exhausting reasonable efforts to resolve the disagreement;
- Leave the process only after providing notice to the other party;
- Resume the process once the disagreement is resolved.

Speed of response



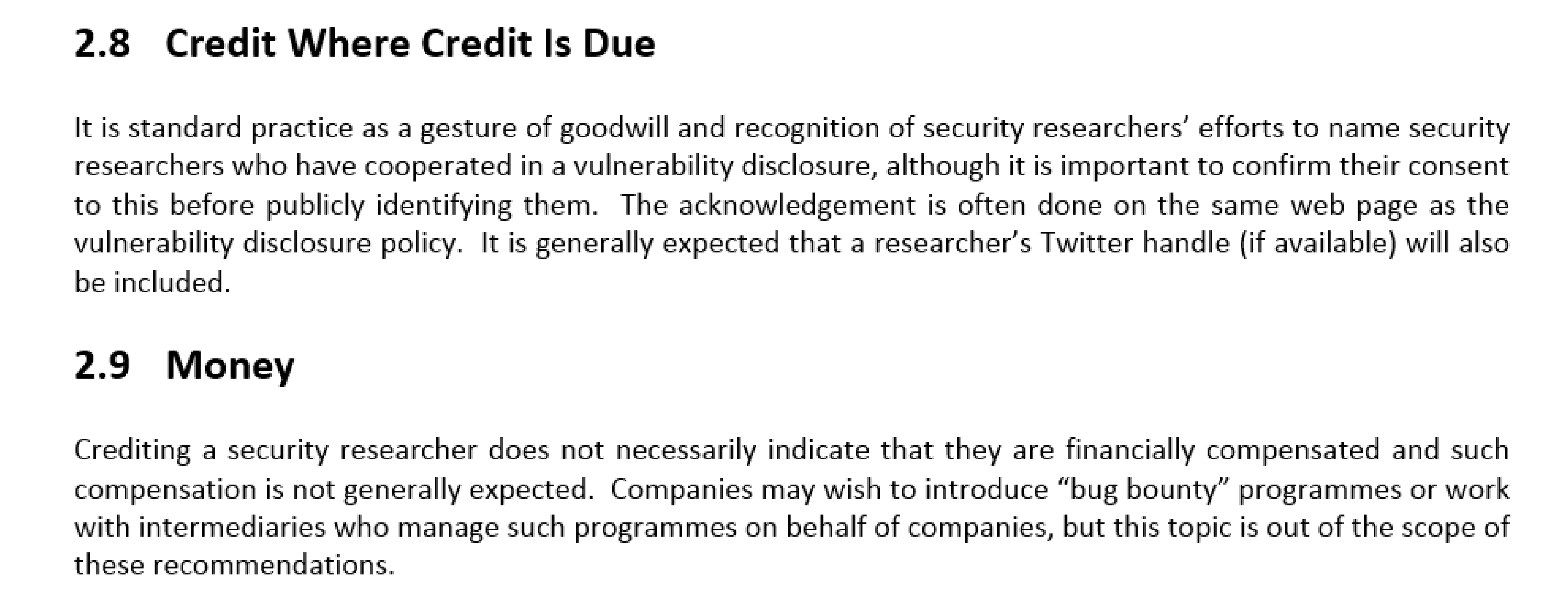
2.6 Timing of Response

The text on your security contact web page should state in what time frame the security researcher can expect a response; this will typically be a few days, perhaps up to a week. It is good practice to send an automatic acknowledgement for email sent to the contact email address including the same details on the expected response time. The following response should then further clarify expectations regarding the timing of further communications and, once a problem has been confirmed, in what time frame a patch, fix or other remediation is expected to be made available.

It can be very difficult to estimate a reasonable amount of time for a security vulnerability to be fixed. It depends on many factors, including the nature of the affected component (e.g. a web service, a software product or a hardware product), the technical complexity and architectural depth of the problem, and the mechanisms available for updating the offering. It is a topic that has been debated at length amongst the security community and continues to be a source of tension.

It is important to communicate with the researcher and explain how you justify your estimated timing. If the researcher feels that you are not taking their report seriously enough, it may cause a breakdown of the process and premature public disclosure of the vulnerability. At one extreme, for a simple problem in a live web service involving individuals' personal data, a reasonable time to fix might be only a few days, but at the other extreme, fixing a complex problem with a physical product that requires new hardware to be manufactured and distributed to repair centres could take many months.

Acknowledgement and reward



2.8 Credit Where Credit Is Due

It is standard practice as a gesture of goodwill and recognition of security researchers' efforts to name security researchers who have cooperated in a vulnerability disclosure, although it is important to confirm their consent to this before publicly identifying them. The acknowledgement is often done on the same web page as the vulnerability disclosure policy. It is generally expected that a researcher's Twitter handle (if available) will also be included.

2.9 Money

Crediting a security researcher does not necessarily indicate that they are financially compensated and such compensation is not generally expected. Companies may wish to introduce "bug bounty" programmes or work with intermediaries who manage such programmes on behalf of companies, but this topic is out of the scope of these recommendations.

Key Takeaways

- Implement a Vulnerability Policy
- Executive backing and awareness is essential
- Assign responsibilities for the communication and response roles

Smart Buildings activities

Engaging with IoT Security Best Practices

James Willison & Sarb Sembhi

Unified Security and Virtually Informed

Smart Buildings

- Enterprise
- Consumer
- Others…

Goal of Working Group

- The goal of this Working Group is to establish a comprehensive set of guidelines to help each of the supply chain participants to specify, procure, install, integrate, operate and maintain IoT securely in buildings.

- This includes intelligent buildings equipment and controls such as CCTV, audio visual (AV), fire, HVAC, lighting and building security e.g. access control & biometric systems.

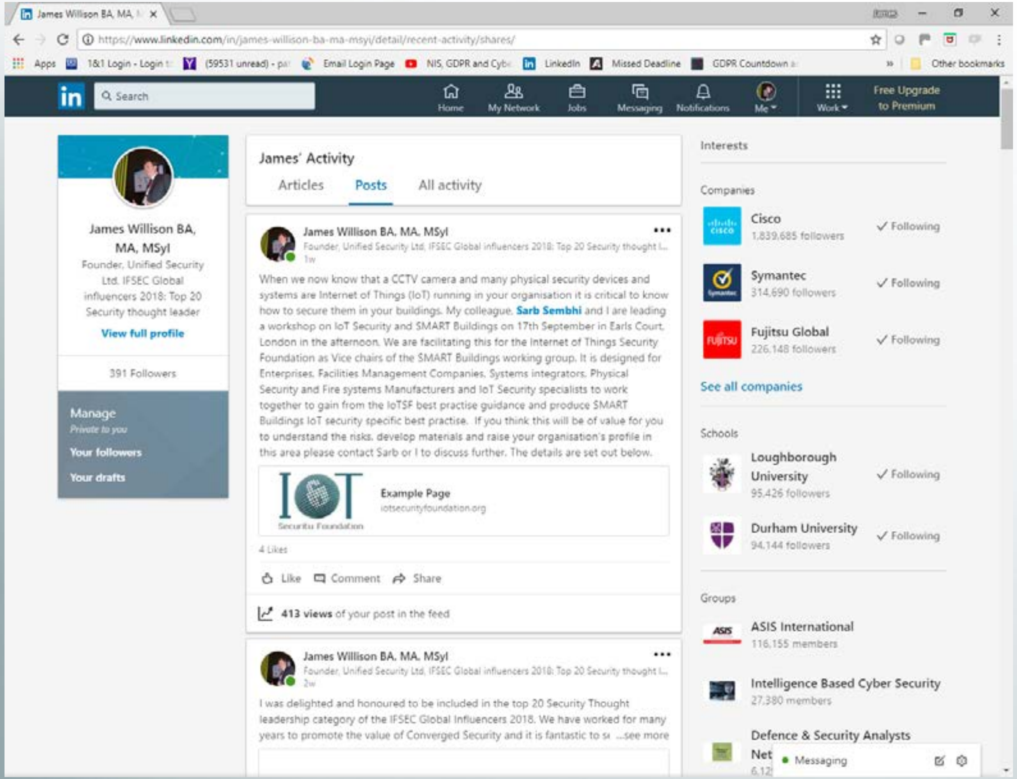
How we got here

- Meeting with Paul Dorey in March
- Agreed approach
- Meet with Jenny Devoy & team at InfoSecurity in June
- Launched September Workshop at IFSEC in June
- Participated in IoT SF Plenary session in July
- Agreed invitee target list
- Invited participants for workshop

IoT Security, Privacy and Surveillance: IFSEC 2018 : Launch of IoTSF Smart Buildings workshop

Video of panel discussion with Paul Dorey, Sarb Sembhi, James Willison (IoTSF Smart Buildings Group), Steven Kenny (AXIS Communications) and Mike Hurst (ASIS UK) due out w/c 09/07/18.
https://www.ifsecglobal.com

Promoted on Social Media and IoTSF website



James Willison BA. MA. MSyl
Founder, Unified Security Ltd, IFSEC Global influencers 2018: Top 20 Security thought l...
1w

When we now know that a CCTV camera and many physical security devices and systems are Internet of Things (IoT) running in your organisation it is critical to know how to secure them in your buildings. My colleague, Sarb Sembhi and I are leading a workshop on IoT Security and SMART Buildings on 17th September in Earls Court, London in the afternoon. We are facilitating this for the Internet of Things Security Foundation as Vice chairs of the SMART Buildings working group. It is designed for Enterprises, Facilities Management Companies, Systems integrators, Physical Security and Fire systems Manufacturers and IoT Security specialists to work together to gain from the IoTSF best practise guidance and produce SMART Buildings IoT security specific best practise. If you think this will be of value for you to understand the risks, develop materials and raise your organisation's profile in this area please contact Sarb or I to discuss further. The details are set out below.

Example Page
iotsecurityfoundation.org

4 Likes

Like Comment Share

413 views of your post in the feed

James Willison BA. MA. MSyl
Founder, Unified Security Ltd, IFSEC Global influencers 2018: Top 20 Security thought l...
2w

I was delighted and honoured to be included in the top 20 Security Thought leadership category of the IFSEC Global Influencers 2018. We have worked for many years to promote the value of Converged Security and it is fantastic to s ...see more

- IoTSF blog and news announcing the workshop.
- This was posted on Linkedin and reshared by Sarb : total views : 1053
- Personal invites to contacts in the target audience.
- How can IoTSF plenary help spread the message and invite others?

IFSEC 2018 : June 21st

The Converged Security Centre: Protecting IoT in real time.

Converged Security Centre In Actic
Delivers real-time data visualization and actionable intelligence
true situation manage
INCIDENT DETECTION & ANALYTICS
RESPONSE
REPORTI

SMART BUILDINGS CYBER SECURITY WORKSHOP

Monday 17 Sept 2018: 1230 – 1645: IBIS Hotel Earls Court.

John Moor, Managing Director, IoTSF

Paul Dorey, Chair, IoTSF

Jenny Devoy, Head of Membership Development, IoTSF

Sarb Sembhi & James Willison, IoTSF Smart Buildings Working Group Vice chairs.

Delegates: 23 senior representatives from End Users, Facilities Managers, Designers, Manufacturers, Integrators, Auditors, Installers and IoT Specialists/Researchers.

Follow up call: 8th October 2018

Follow-up call (8th October). 15 people on the call. We agreed the following four sub-groups to be set up, and for any interested people to indicate which one (or more of the four) groups they would like to be involved in.

- The Groups are:
- Strategic
- Awareness
- Research
- Guidance

- The first two will be supported by Sarb Sembhi, and the last two will be supported by James Willison. We will identify up to four sub chairs and look for a Chair.

Four sub groups

Strategic	Language / definitions
Strategic	Stakeholders
Strategic	What do we want to achieve in stakeholder conversations?
Strategic	Assurance - Certification
Strategic	Roadmap Risk management journey
Strategic	Liaising with other professional bodies

Awareness	What is a smart building?
Awareness	Simple "Awareness training course" for all
Awareness	Attack surface of Smart Buildings
Awareness	Make buildings people-proof
Awareness	Gaining buy-in
Awareness / Guidance	Create use cases

Sub groups (cont.)

Research - academic	Current academic research
Research - knowledge	Current standards
Research - knowledge	Current Guidance
Standard	Integration with other Standards and Frameworks

Guidance	Create a body of knowledge
Guidance	Reference architecture
Guidance	Common reference framework
Guidance	Security of key devices (mini-systems)
Guidance/maturity model	Contractual requirements

Next steps

- Sub-Group calls on the 11th December
- Draw up list of projects
- Provide guidance on Framework specific to Smart Buildings
- Provide some quick wins for Q1
- Finalise deliverables for 2019

Architecture Whitepapers

Engaging with IoT Security Best Practices

Richard Marshall

IoTSF Plenary Chair

Architecture Whitepapers

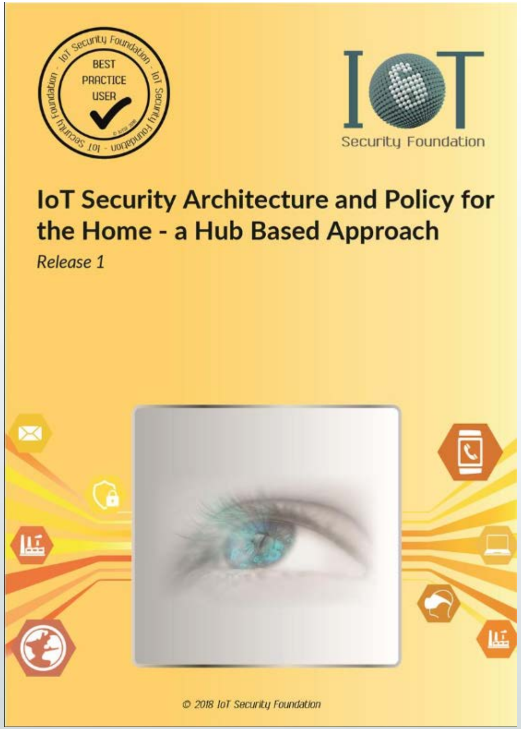
BEST PRACTICE USER

IoT Security Foundation

IoT Security Architecture and Policy for the Enterprise - a Hub Based Approach

Release 1

© 2018 IoT Security Foundation



BEST PRACTICE USER

IoT Security Foundation

IoT Security Architecture and Policy for the Home - a Hub Based Approach

Release 1

© 2018 IoT Security Foundation

Health care

Enterprise

Intended audience:

- CxOs and IoT purchasers
- IT departments
- Developers
- OEM Product Management

IoT Security Foundation BEST PRACTICE USER

IoT Security Foundation

IoT Security Architecture and Policy for the Enterprise - a Hub Based Approach

Release 1

© 2018 IoT Security Foundation

Enterprise

Intent:

- Simplifying implementation options
- Illustrate what a good security regime looks like
- Show the benefits of a hub-based approach

BEST PRACTICE USER

IoT Security Foundation

IoT Security Architecture and Policy for the Enterprise - a Hub Based Approach

Release 1

© 2018 IoT Security Foundation

Home

Intended audience:

- IoT Service Providers
- Developers
- OEM Product Management

IoT Security Foundation - IoT Security Foundation - IoT Security Foundation

BEST PRACTICE USER

IoT Security Foundation

IoT Security Architecture and Policy for the Home - a Hub Based Approach

Release 1

Home

Intent:

- Simplifying implementation options
- Illustrate what a good home security regime looks like
- Demonstrate how to support IoT with minimal reliance on users
- Show the benefits of a hub-based approach
- Foster growth by making security part of the purchasing process

IoT Security Foundation BEST PRACTICE USER

IoT Security Foundation

IoT Security Architecture and Policy for the Home - a Hub Based Approach

Release 1

© 2018 IoT Security Foundation

Future Activities

Engaging with IoT Security Best Practices

Richard Marshall

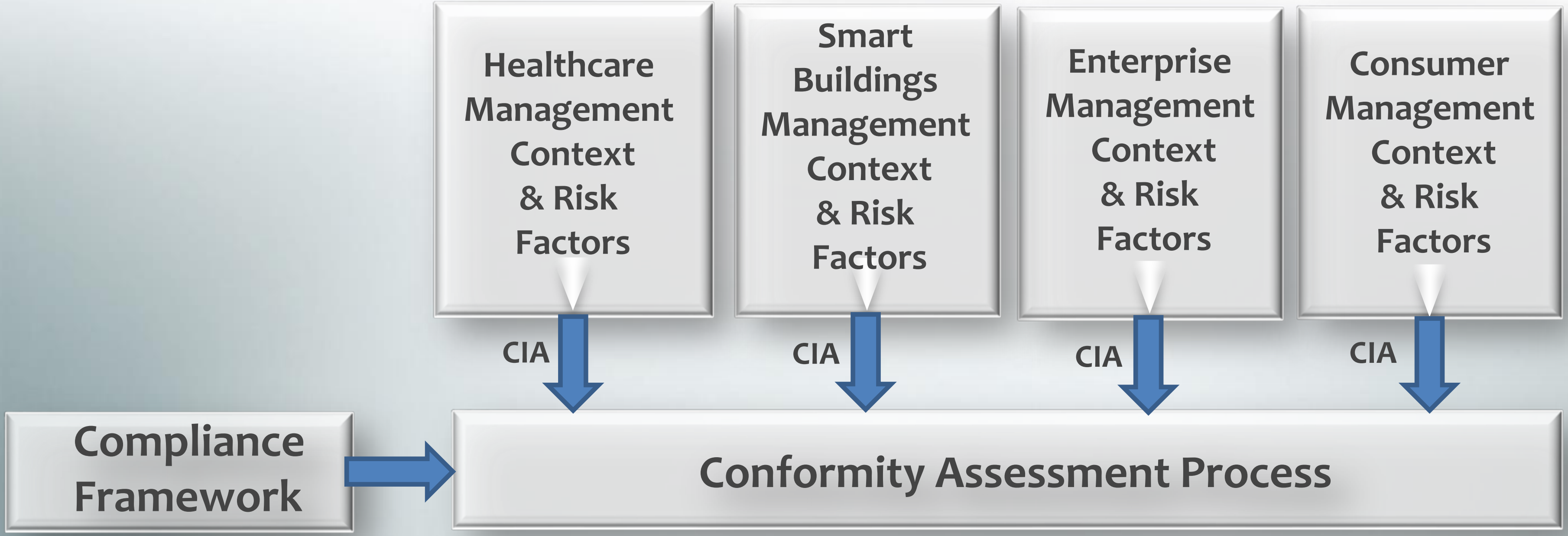
IoTSF Plenary Chair

Conformance

- Create ‘certifications’ derived from the IoT Compliance Framework
  - fit within a recognised framework / standard (Eu/ISO/IEC etc)
- First goal: MVP - Satisfy DCMS Consumer Code of Practice
  - Determine the Conformity Assessment System
    - “rules, procedures and management for carrying out conformity assessment”
  - Determine the Conformity Assessment Scheme for consumer
- More schemes may follow if successful
  - E.g. Industrial products

Conformity Document Map

Security Foundation



Healthcare Management Context & Risk Factors

Smart Buildings Management Context & Risk Factors

Enterprise Management Context & Risk Factors

Consumer Management Context & Risk Factors

CIA

CIA

CIA

CIA

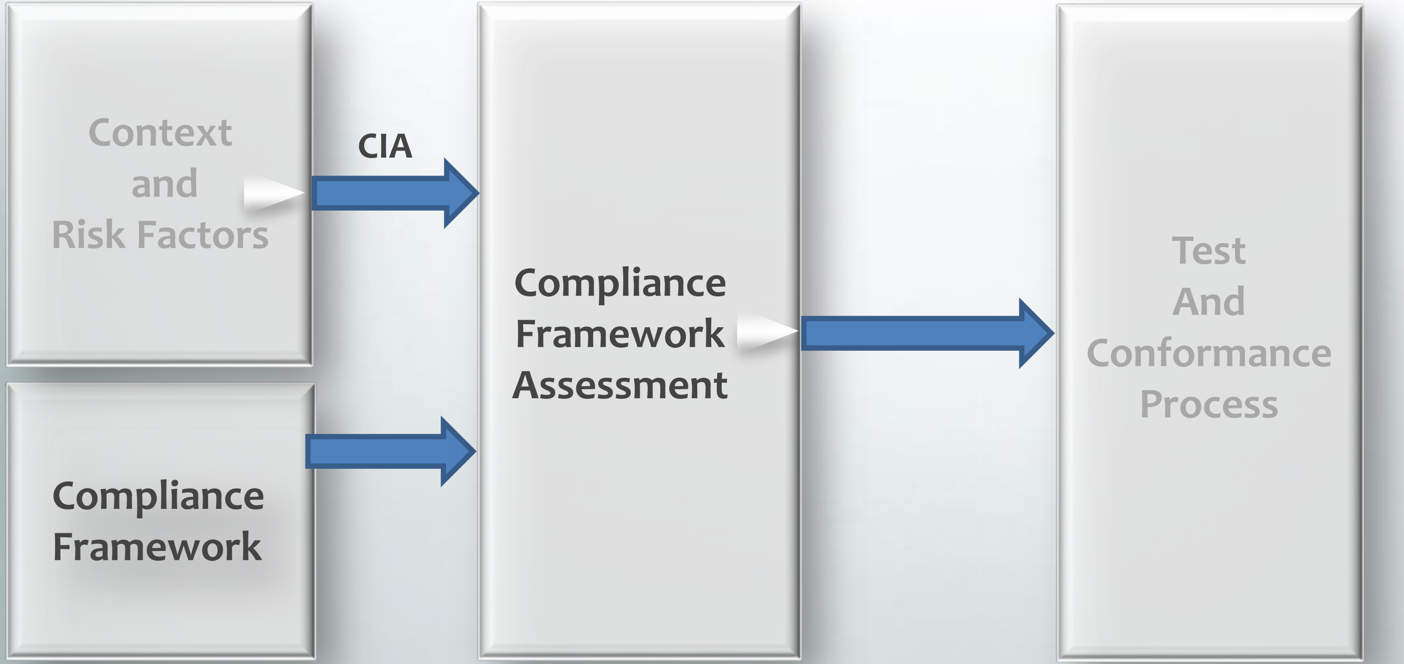
Compliance Framework

Conformity Assessment Process

Conformity Assessment

- The official definition is: *“Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled”* (definition in EN ISO/IEC 17000:2004 Conformity assessment – Vocabulary and general principles).
- http://www.european-accreditation.org/what-is-accreditation#3

Conformance Assessment Process



Context and Risk Factors

CIA

Compliance Framework

Compliance Framework Assessment

Test And Conformance Process

Accreditation entity/ schemes

- Accreditation is a third-party evaluation and demonstration of competence. It is the assessment of independence, objectivity and competence of an entity for the performance of defined activities.
- Accreditation is a public authority activity. *It is the last level of public authority control.* The purpose of accreditation is to provide an authoritative statement of the competence of a body to perform conformity assessment activities.
- http://www.european-accreditation.org/what-is-accreditation#1

Thank You!

https://iotsecurityfoundation.org/