RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: ASD-T10

Securing the Internet of Things: Mapping Attack Surface Areas Using the OWASP IoT Top 10

Daniel Miessler

Security Research
HP Fortify on Demand
@danielmiessler

Daniel Miessler
@DanielMiessler

technology | philosophy | politics

San Francisco, CA
danielmiessler.com/about/
Joined March 2007

- HP Fortify on Demand
- Security Research & Development
- Penetration Testing
- OWASP Project Leader (IoT, Mobile)

The Plan

- Let’s Talk About Naming
- A Vision of the Future (Universal Daemonization)
- Why IoT is Currently Broken
- Examples From Research
- The OWASP IoT Project
- Applying What We’ve Learned
- One more thing…

What does it mean?

What does it mean?

- [WIKIPEDIA] The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices.

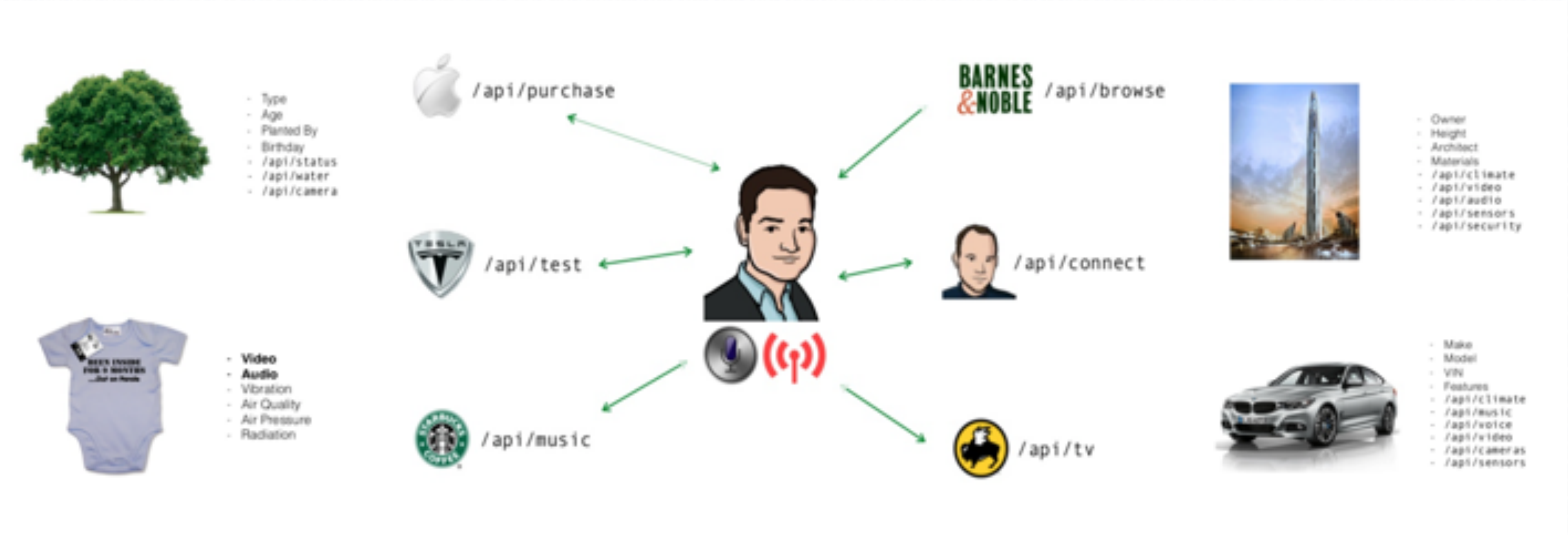
- [OXFORD] A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.

Better Names

- Universal Daemonization
- Universal Object Interaction
- Programmable Object Interfaces (POIs)
- Transfurigated Phase Inversion

The Real Internet of Things

The Real Internet of Things



- Type
- Age
- Planted By
- Birthday
- /api/status
- /api/water
- /api/camera

/api/purchase

/api/test

/api/music

/api/browse

/api/connect

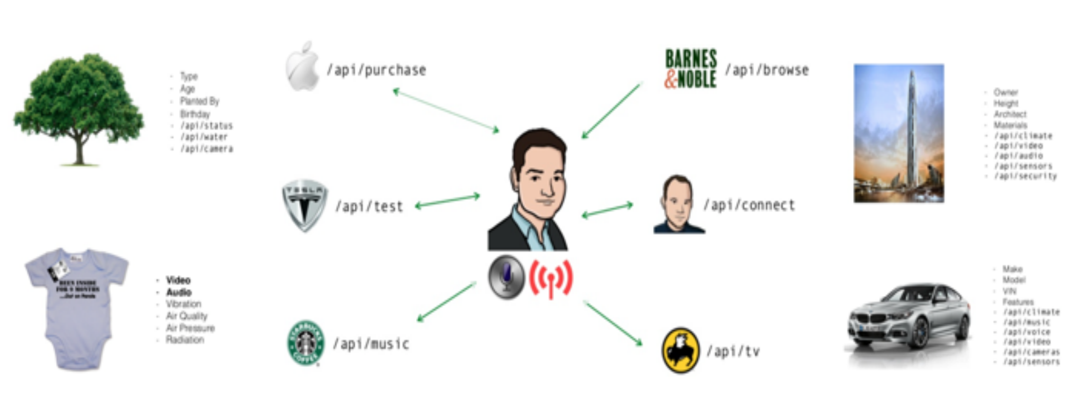
/api/tv

- Owner
- Height
- Architect
- Materials
- /api/climate
- /api/video
- /api/audio
- /api/sensors
- /api/security

- **Video**
- **Audio**
- Vibration
- Air Quality
- Air Pressure
- Radiation

- Make
- Model
- VIN
- Features
- /api/climate
- /api/music
- /api/voice
- /api/video
- /api/cameras
- /api/sensors

Universal Daemonization



- Type
- Age
- Planted By
- Birthday
- /api/status
- /api/water
- /api/camera

/api/purchase

/api/browse

- Owner
- Height
- Architect
- Materials
- /api/climate
- /api/video
- /api/audio
- /api/sensors
- /api/security

/api/test

/api/connect

- **Video**
- **Audio**
- Vibration
- Air Quality
- Air Pressure
- Radiation

/api/music

/api/tv

- Make
- Model
- VIN
- Features
- /api/climate
- /api/music
- /api/voice
- /api/video
- /api/cameras
- /api/sensors

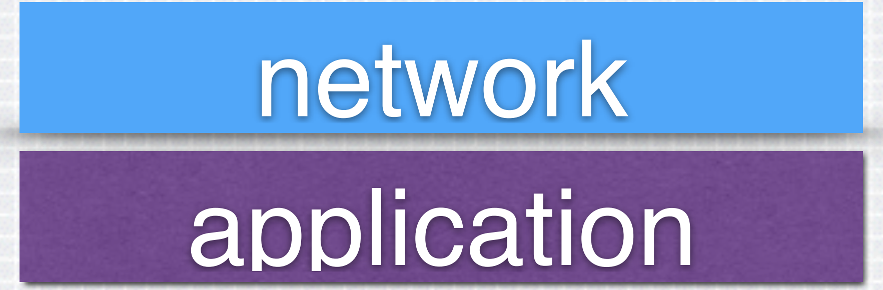
The Current IoT Security Problem

The Current IoT Security Problem

network

- services, encryption, firewall, input…

The Current IoT Security Problem



- authN, authZ, input validation, etc.

The Current IoT Security Problem

network

application

mobile

- insecure APIs, lack of encryption, etc.

The Current IoT Security Problem

network

application

mobile

cloud

- yadda yadda AuthSessionAccess

IoT Security is the Worst-of-All-Worlds

network	◆ services, encryption, firewall, input…
application	◆ authN, authZ, input validation, etc.
mobile	◆ insecure APIs, lack of encryption, etc.
cloud	◆ yadda yadda AuthSessionAccess
IoT	◆ **net + app + mobile + cloud = IoT**

The Current IoT Security Problem

network

application

mobile

cloud

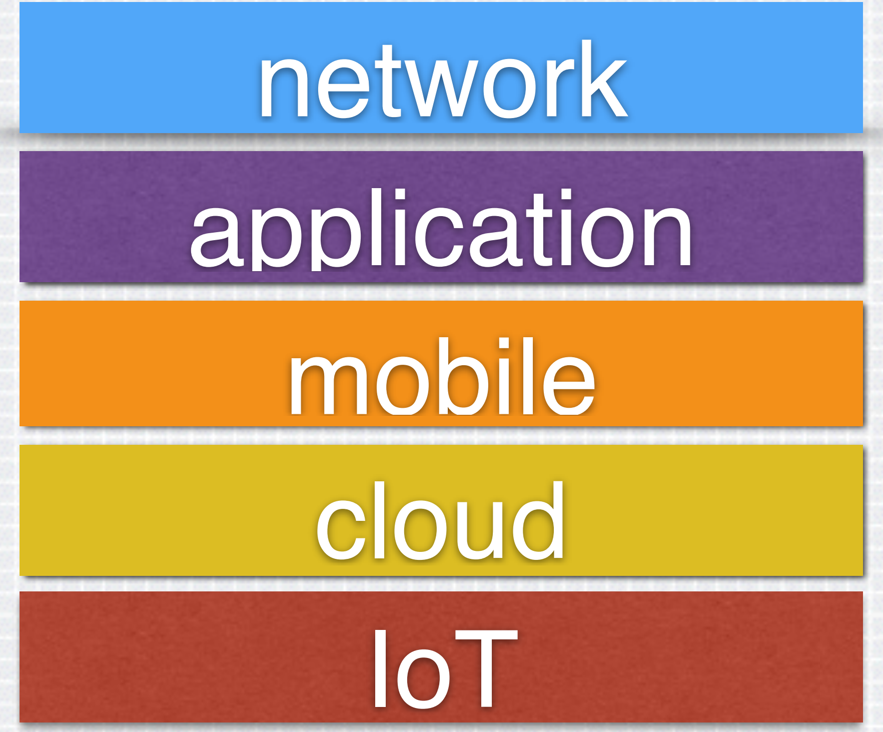
IoT

1 + 1 = 5

IoT Security Fail Examples

- network
- application
- mobile
- cloud
- IoT

IoT Security Fail Examples (Authentication)



network

application

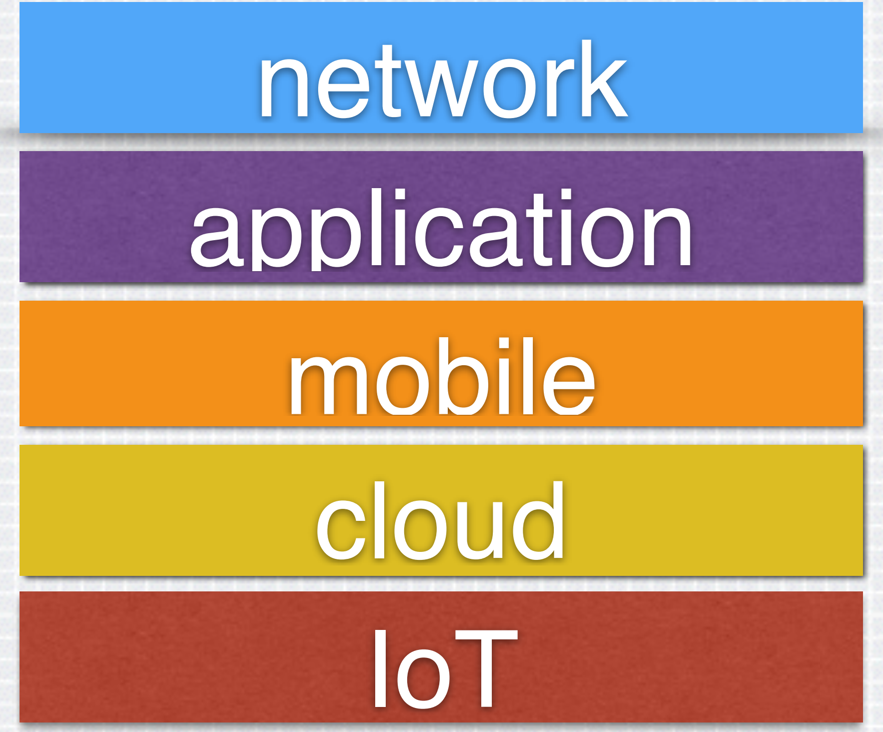
mobile

cloud

IoT

- 10/10 security systems accept ‘123456’
- Account enumeration
- Lack of account lockout

IoT Security Fail Examples (Update Systems)



network

application

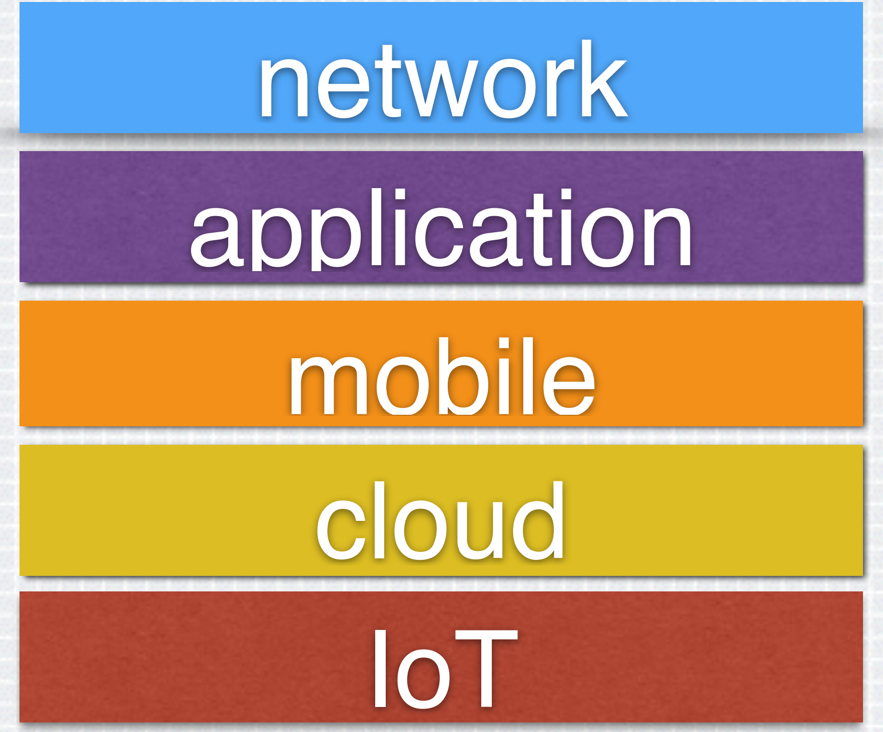
mobile

cloud

IoT

- No signing of updates
- Download over FTP
- Server was world-writeable
- Server held ALL products

IoT Security Fail Examples



network

application

mobile

cloud

IoT

- 10/10 security systems accept ‘123456’
- 10/10 security systems with no lockout
- 10/10 security systems with enumeration
- SSH listeners with root/“” access
- 6/10 web interfaces with XSS/SQLi
- 70% of devices not using encryption
- 8/10 collected personal information
- 9/10 had no two-factor options
- Unauthenticated video streaming
- *Completely flawed* software update systems

The Need for a Methodology

network

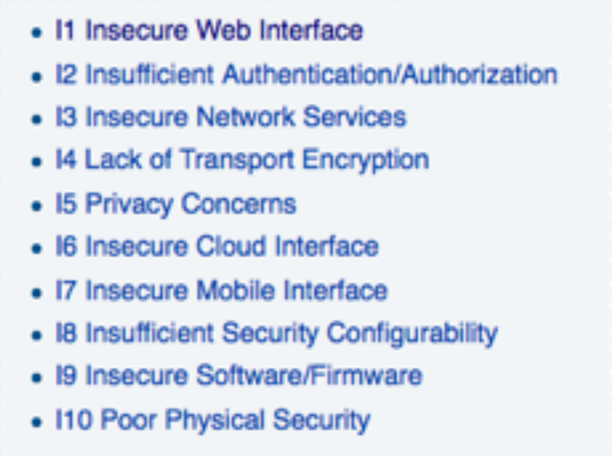
application

mobile

cloud

IoT

Mapping IoT Attack Surface Areas

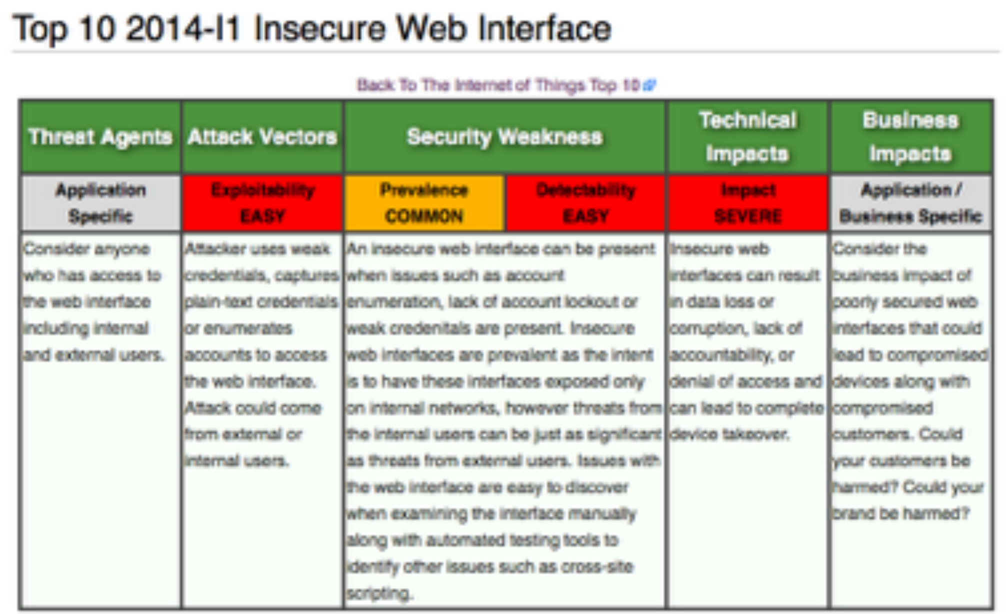


- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

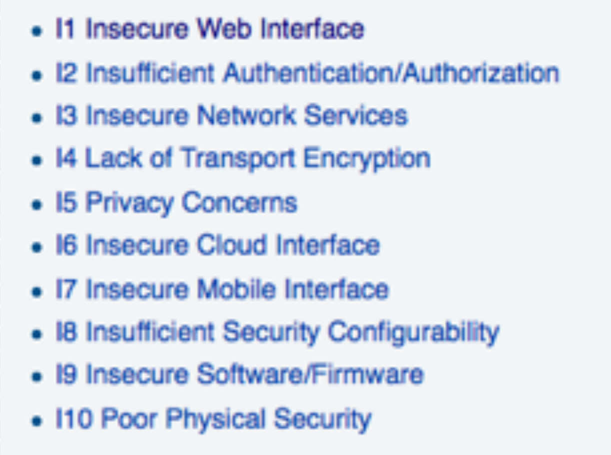
OWASP IoT: I1 — Insecure Web Interface



Top 10 2014-I1 Insecure Web Interface

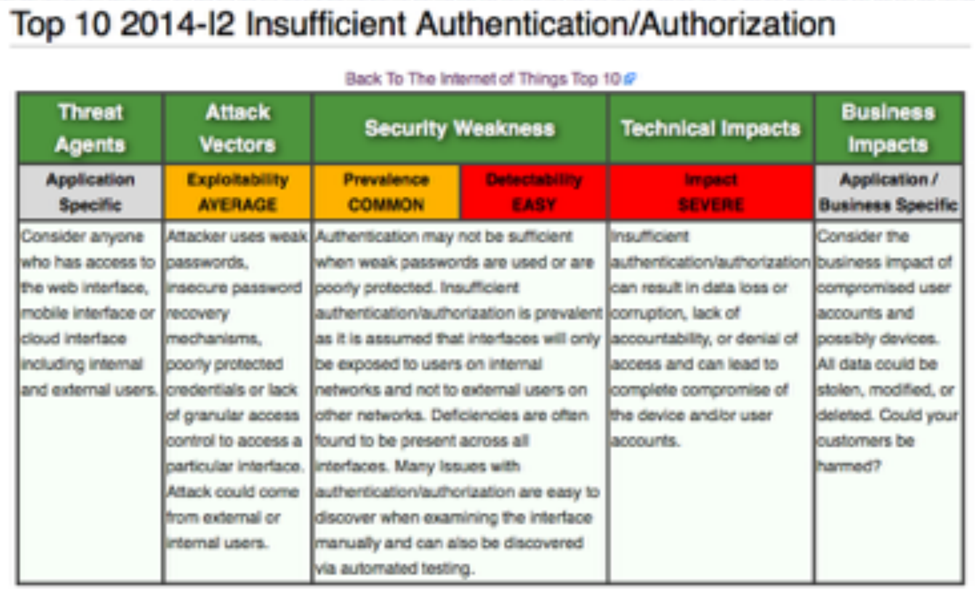
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the web interface including internal and external users.	Attacker uses weak credentials, captures plain-text credentials or enumerates accounts to access the web interface. Attack could come from external or internal users.	An insecure web interface can be present when issues such as account enumeration, lack of account lockout or weak credenitals are present. Insecure web interfaces are prevalent as the intent is to have these interfaces exposed only on internal networks, however threats from the internal users can be just as significant as threats from external users. Issues with the web interface are easy to discover when examining the interface manually along with automated testing tools to identify other issues such as cross-site scripting.		Insecure web interfaces can result in data loss or corruption, lack of accountability, or denial of access and can lead to complete device takeover.	Consider the business impact of poorly secured web interfaces that could lead to compromised devices along with compromised customers. Could your customers be harmed? Could your brand be harmed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP IoT: I1 — Insecure Web Interface



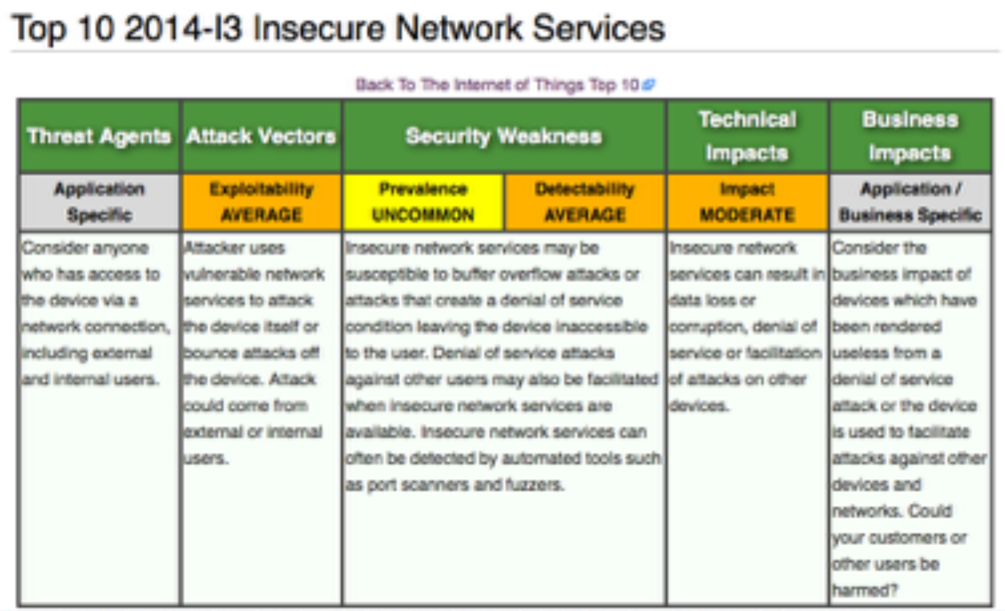
Top 10 2014-I2 Insufficient Authentication/Authorization

Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the web interface, mobile interface or cloud interface including internal and external users.	Attacker uses weak passwords, insecure password recovery mechanisms, poorly protected credentials or lack of granular access control to access a particular interface. Attack could come from external or internal users.	Authentication may not be sufficient when weak passwords are used or are poorly protected. Insufficient authentication/authorization is prevalent as it is assumed that interfaces will only be exposed to users on internal networks and not to external users on other networks. Deficiencies are often found to be present across all interfaces. Many issues with authentication/authorization are easy to discover when examining the interface manually and can also be discovered via automated testing.		Insufficient authentication/authorization can result in data loss or corruption, lack of accountability, or denial of access and can lead to complete compromise of the device and/or user accounts.	Consider the business impact of compromised user accounts and possibly devices. All data could be stolen, modified, or deleted. Could your customers be harmed?

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

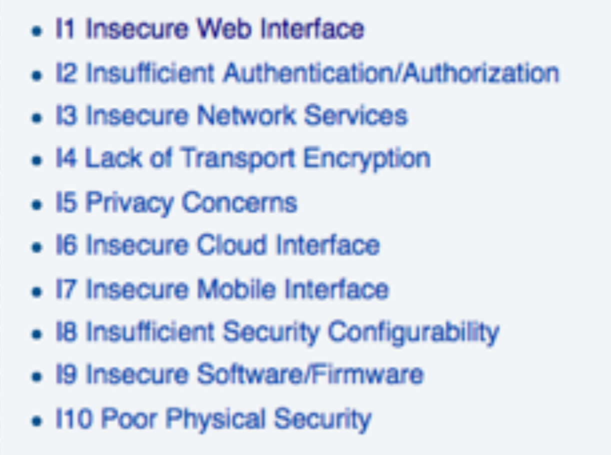
OWASP IoT: I2 — Insecure Network Services



Top 10 2014-I3 Insecure Network Services

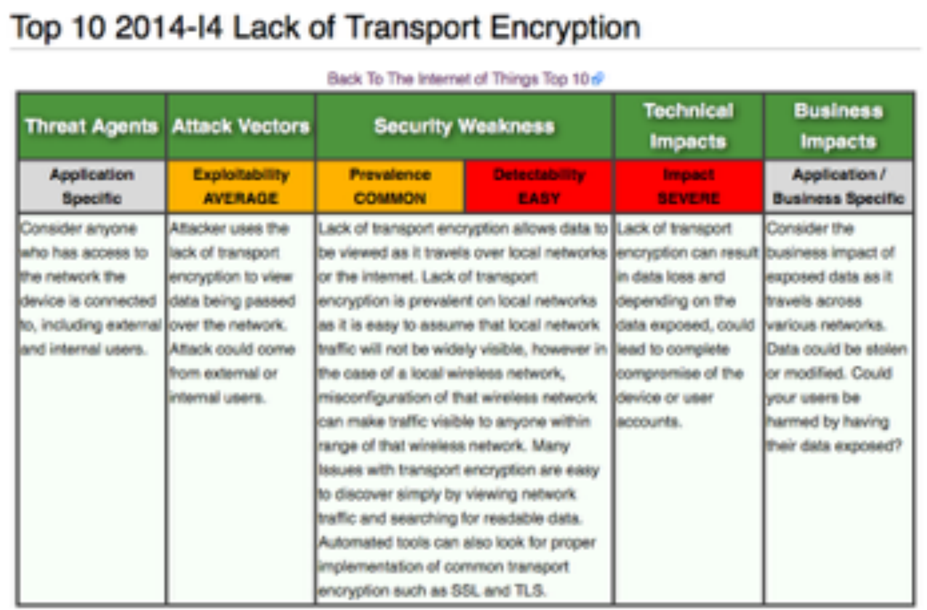
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence UNCOMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific
Consider anyone who has access to the device via a network connection, including external and internal users.	Attacker uses vulnerable network services to attack the device itself or bounce attacks off the device. Attack could come from external or internal users.	Insecure network services may be susceptible to buffer overflow attacks or attacks that create a denial of service condition leaving the device inaccessible to the user. Denial of service attacks against other users may also be facilitated when insecure network services are available. Insecure network services can often be detected by automated tools such as port scanners and fuzzers.		Insecure network services can result in data loss or corruption, denial of service or facilitation of attacks on other devices.	Consider the business impact of devices which have been rendered useless from a denial of service attack or the device is used to facilitate attacks against other devices and networks. Could your customers or other users be harmed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

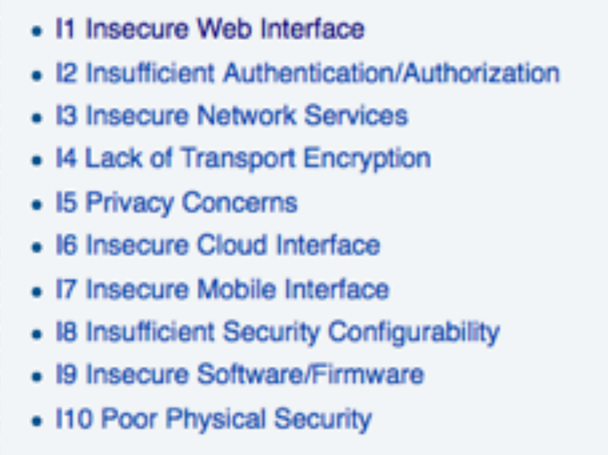
OWASP IoT: I3 — Lack of Transport Encryption



Top 10 2014-I4 Lack of Transport Encryption

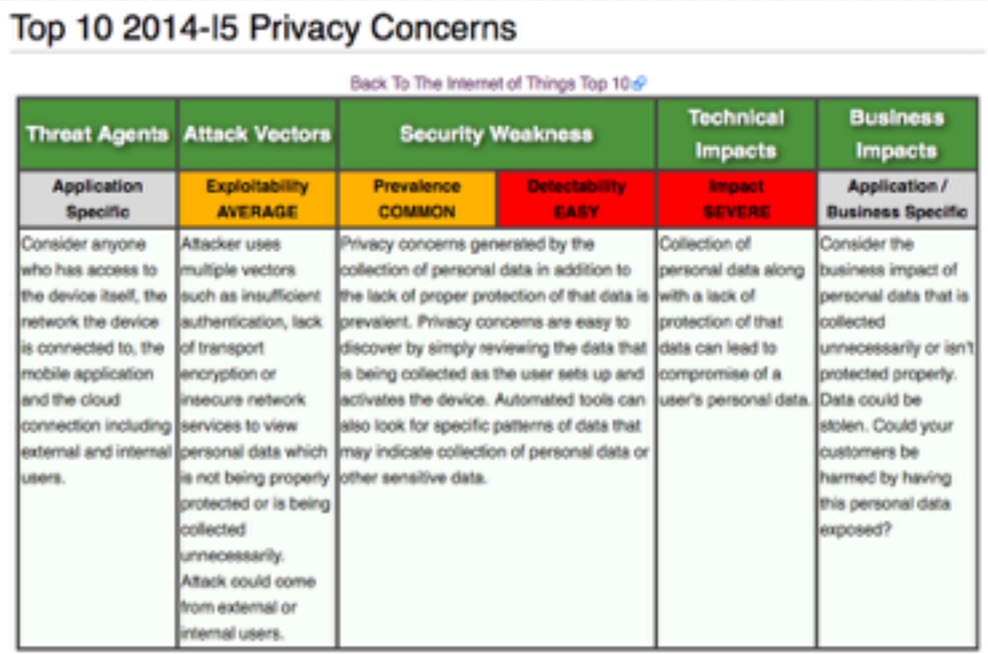
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the network the device is connected to, including external and internal users.	Attacker uses the lack of transport encryption to view data being passed over the network. Attack could come from external or internal users.	Lack of transport encryption allows data to be viewed as it travels over local networks or the internet. Lack of transport encryption is prevalent on local networks as it is easy to assume that local network traffic will not be widely visible, however in the case of a local wireless network, misconfiguration of that wireless network can make traffic visible to anyone within range of that wireless network. Many issues with transport encryption are easy to discover simply by viewing network traffic and searching for readable data. Automated tools can also look for proper implementation of common transport encryption such as SSL and TLS.		Lack of transport encryption can result in data loss and depending on the data exposed, could lead to complete compromise of the device or user accounts.	Consider the business impact of exposed data as it travels across various networks. Data could be stolen or modified. Could your users be harmed by having their data exposed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

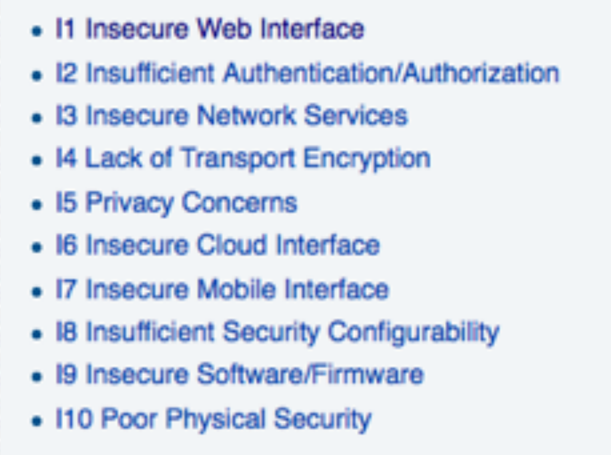
OWASP IoT: I5 — Privacy Concerns



Top 10 2014-I5 Privacy Concerns

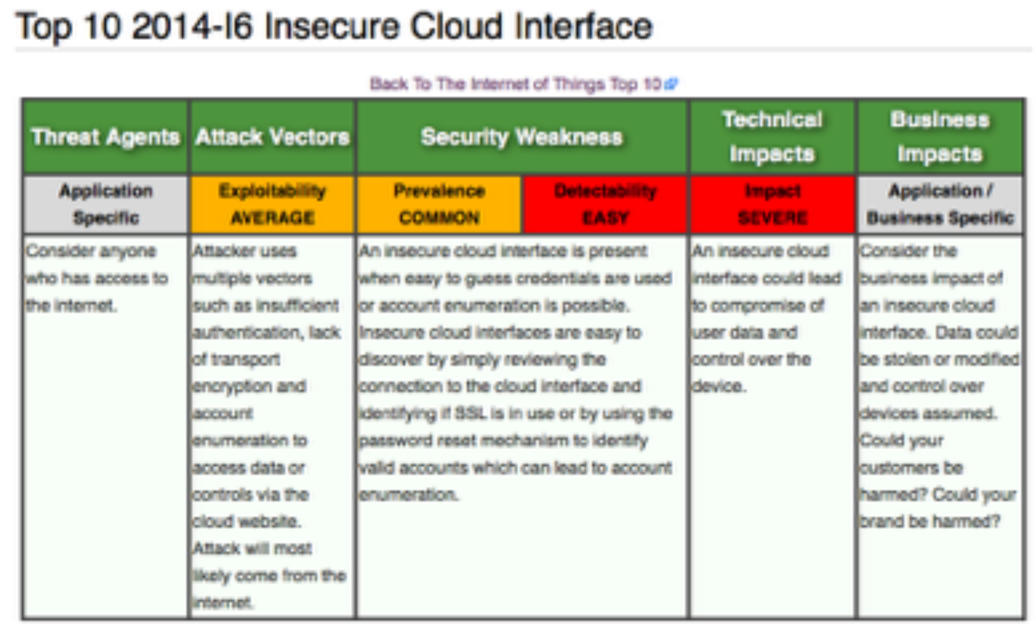
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the device itself, the network the device is connected to, the mobile application and the cloud connection including external and internal users.	Attacker uses multiple vectors such as insufficient authentication, lack of transport encryption or insecure network services to view personal data which is not being properly protected or is being collected unnecessarily. Attack could come from external or internal users.	Privacy concerns generated by the collection of personal data in addition to the lack of proper protection of that data is prevalent. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device. Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data.		Collection of personal data along with a lack of protection of that data can lead to compromise of a user's personal data.	Consider the business impact of personal data that is collected unnecessarily or isn't protected properly. Data could be stolen. Could your customers be harmed by having this personal data exposed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

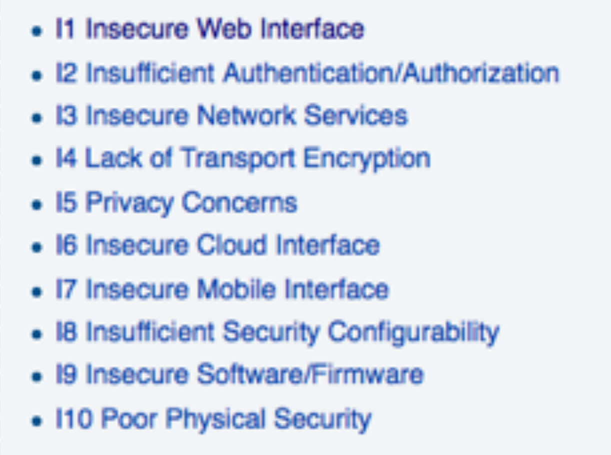
OWASP IoT: I6 — Insecure Cloud Interface



Top 10 2014-I6 Insecure Cloud Interface

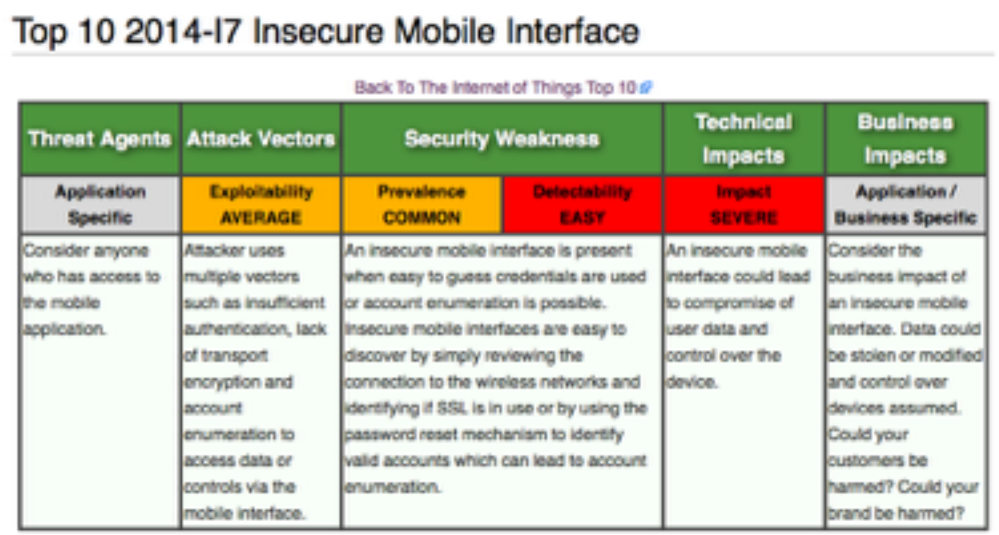
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the internet.	Attacker uses multiple vectors such as insufficient authentication, lack of transport encryption and account enumeration to access data or controls via the cloud website. Attack will most likely come from the internet.	An insecure cloud interface is present when easy to guess credentials are used or account enumeration is possible. Insecure cloud interfaces are easy to discover by simply reviewing the connection to the cloud interface and identifying if SSL is in use or by using the password reset mechanism to identify valid accounts which can lead to account enumeration.		An insecure cloud interface could lead to compromise of user data and control over the device.	Consider the business impact of an insecure cloud interface. Data could be stolen or modified and control over devices assumed. Could your customers be harmed? Could your brand be harmed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

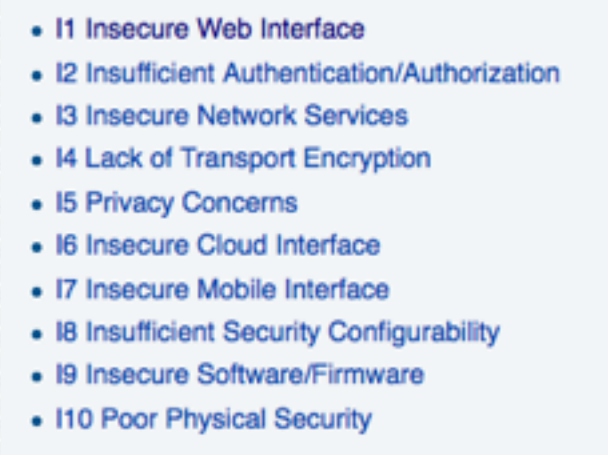
OWASP IoT: I7 — Insecure Mobile Interface



Top 10 2014-I7 Insecure Mobile Interface

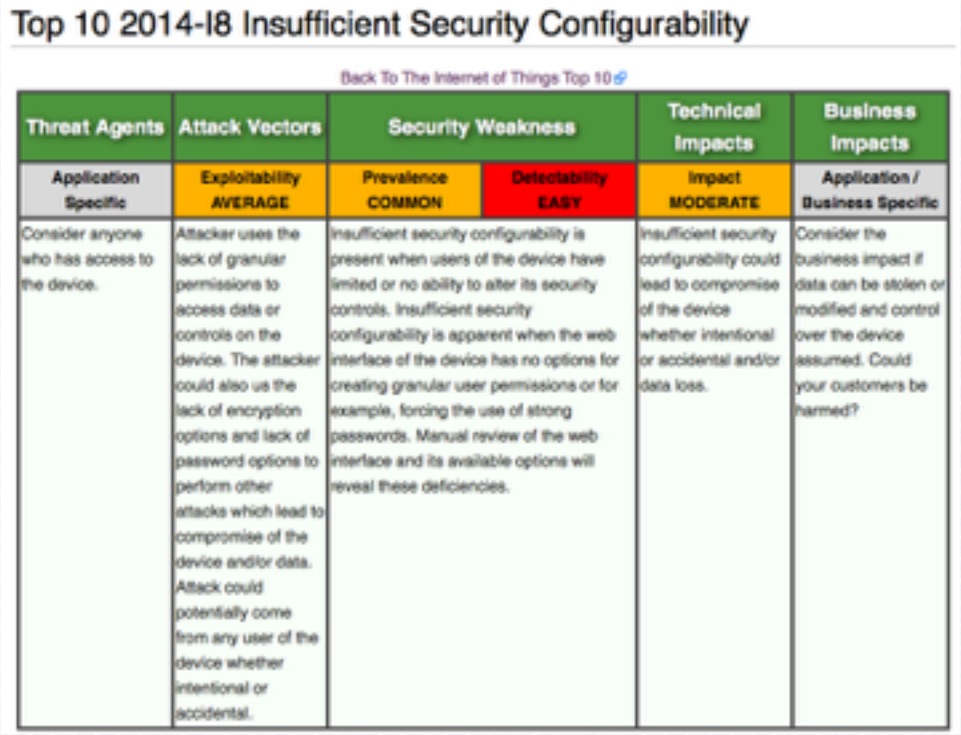
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the mobile application.	Attacker uses multiple vectors such as insufficient authentication, lack of transport encryption and account enumeration to access data or controls via the mobile interface.	An insecure mobile interface is present when easy to guess credentials are used or account enumeration is possible. Insecure mobile interfaces are easy to discover by simply reviewing the connection to the wireless networks and identifying if SSL is in use or by using the password reset mechanism to identify valid accounts which can lead to account enumeration.		An insecure mobile interface could lead to compromise of user data and control over the device.	Consider the business impact of an insecure mobile interface. Data could be stolen or modified and control over devices assumed. Could your customers be harmed? Could your brand be harmed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

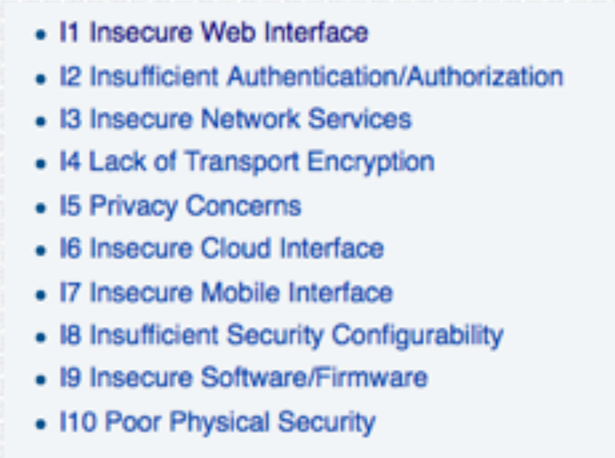
OWASP IoT: I8 — Insufficient Security Configurability



Top 10 2014-I8 Insufficient Security Configurability

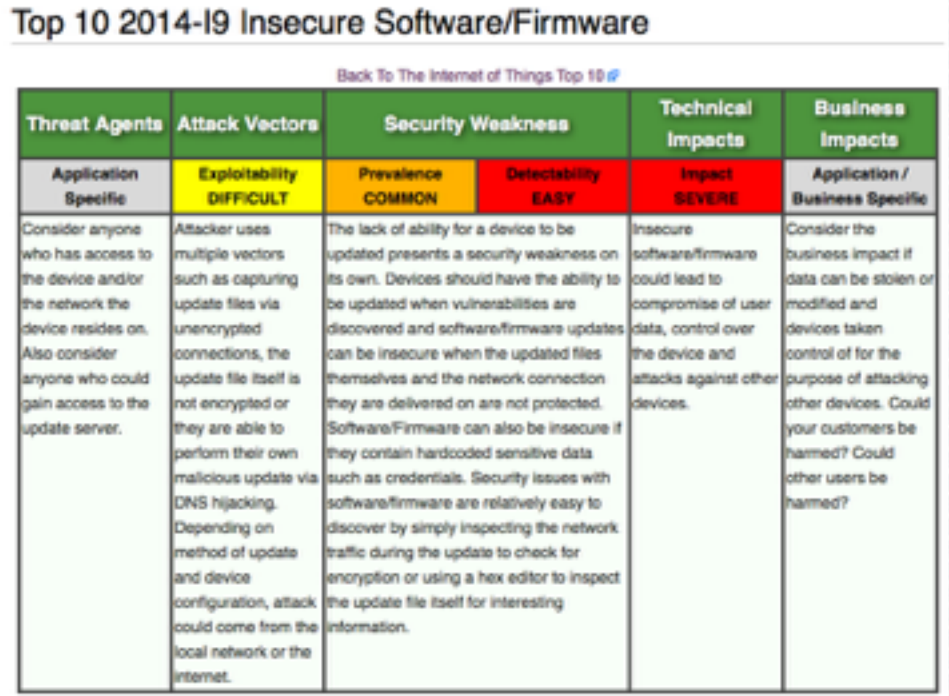
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anyone who has access to the device.	Attacker uses the lack of granular permissions to access data or controls on the device. The attacker could also us the lack of encryption options and lack of password options to perform other attacks which lead to compromise of the device and/or data. Attack could potentially come from any user of the device whether intentional or accidental.	Insufficient security configurability is present when users of the device have limited or no ability to alter its security controls. Insufficient security configurability is apparent when the web interface of the device has no options for creating granular user permissions or for example, forcing the use of strong passwords. Manual review of the web interface and its available options will reveal these deficiencies.		Insufficient security configurability could lead to compromise of the device whether intentional or accidental and/or data loss.	Consider the business impact if data can be stolen or modified and control over the device assumed. Could your customers be harmed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

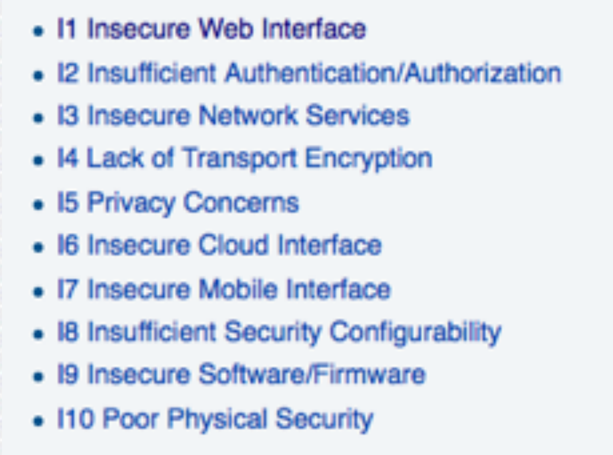
OWASP IoT: I9 — Insecure Software/Firmware



Top 10 2014-I9 Insecure Software/Firmware

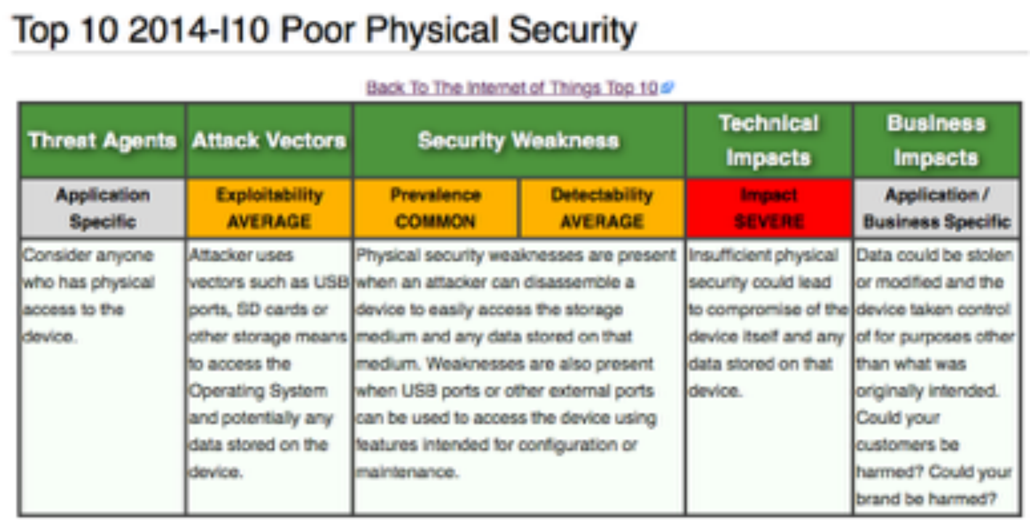
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability DIFFICULT	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has access to the device and/or the network the device resides on. Also consider anyone who could gain access to the update server.	Attacker uses multiple vectors such as capturing update files via unencrypted connections, the update file itself is not encrypted or they are able to perform their own malicious update via DNS hijacking. Depending on method of update and device configuration, attack could come from the local network or the internet.	The lack of ability for a device to be updated presents a security weakness on its own. Devices should have the ability to be updated when vulnerabilities are discovered and software/firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/Firmware can also be insecure if they contain hardcoded sensitive data such as credentials. Security issues with software/firmware are relatively easy to discover by simply inspecting the network traffic during the update to check for encryption or using a hex editor to inspect the update file itself for interesting information.		Insecure software/firmware could lead to compromise of user data, control over the device and attacks against other devices.	Consider the business impact if data can be stolen or modified and devices taken control of for the purpose of attacking other devices. Could your customers be harmed? Could other users be harmed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

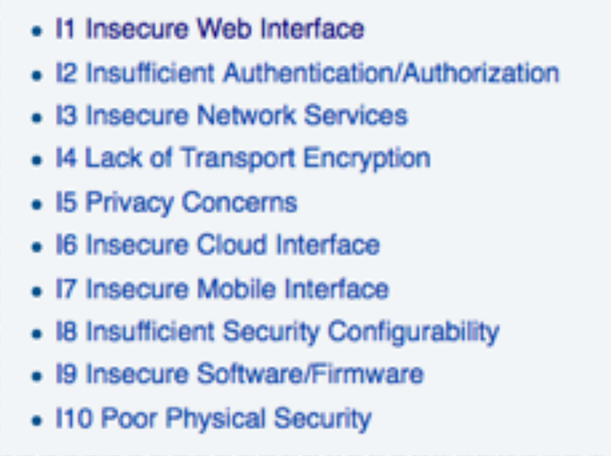
OWASP IoT: I10 — Poor Physical Security



Top 10 2014-I10 Poor Physical Security

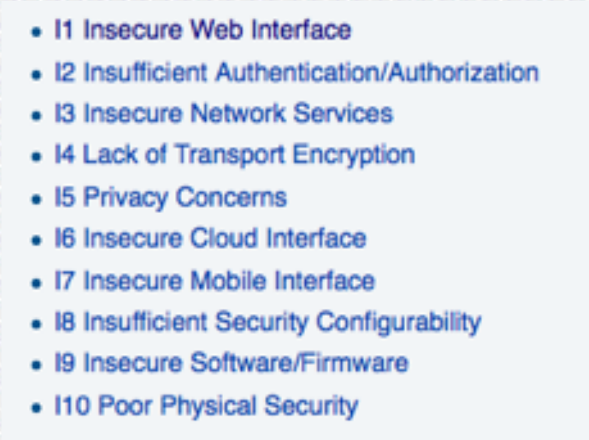
Back To The Internet of Things Top 10

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
Consider anyone who has physical access to the device.	Attacker uses vectors such as USB ports, SD cards or other storage means to access the Operating System and potentially any data stored on the device.	Physical security weaknesses are present when an attacker can disassemble a device to easily access the storage medium and any data stored on that medium. Weaknesses are also present when USB ports or other external ports can be used to access the device using features intended for configuration or maintenance.		Insufficient physical security could lead to compromise of the device itself and any data stored on that device.	Data could be stolen or modified and the device taken control of for purposes other than what was originally intended. Could your customers be harmed? Could your brand be harmed?



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP IoT Project Goals



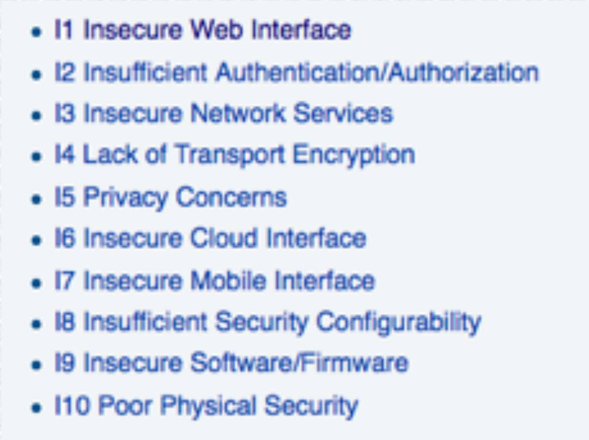
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. **Understand the main attack surface areas** for any IoT device or ecosystem

OWASP IoT Project Goals



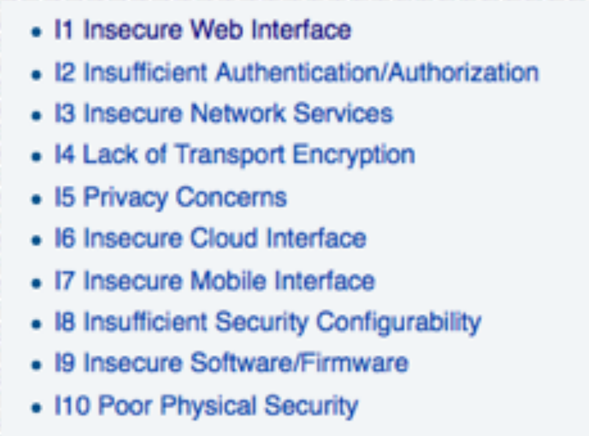
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. Understand the main attack surface areas for any IoT device or ecosystem
2. **As a tester**, be able to hit the major issues for each surface area for the product you're testing

OWASP IoT Project Goals



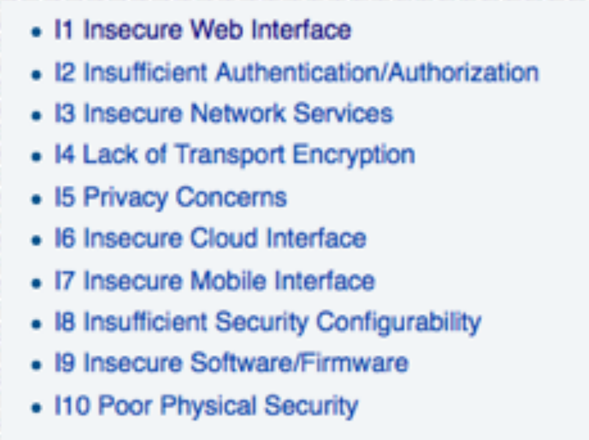
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. Understand the main attack surface areas for any IoT device or ecosystem
2. As a tester, be able to hit the major issues for each surface area for the product you're testing
3. **As a manufacturer**, be able to ensure that you've done your due diligence in security across the main surface areas

OWASP IoT Project Goals



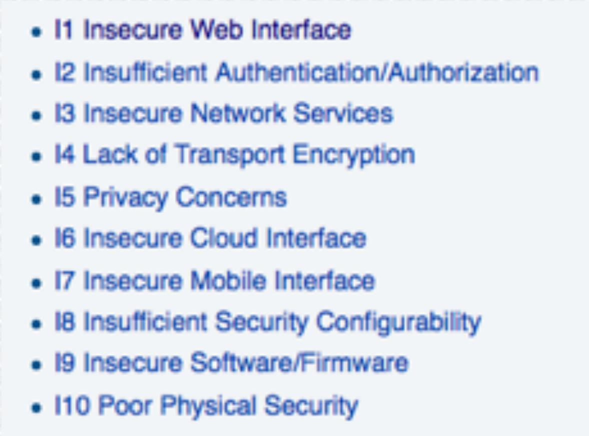
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. Understand the main attack surface areas for any IoT device or ecosystem
2. As a tester, be able to hit the major issues for each surface area for the product you're testing
3. As a manufacturer, be able to ensure that you've done your due diligence in security across the main surface areas
4. **As a developer**, be able to ensure that you're avoiding the top security issues while building your particular component

OWASP IoT Project Goals

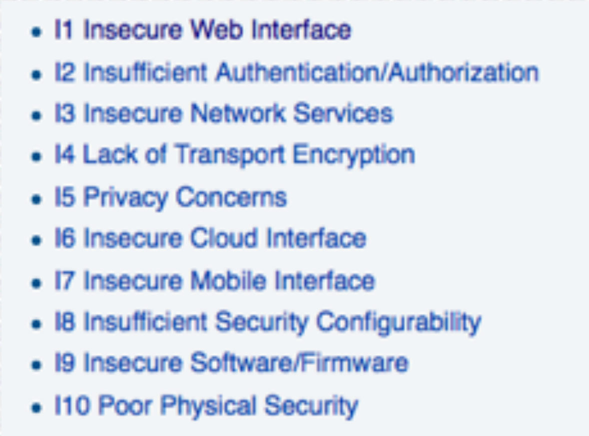


- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP
Internet of Things Top 10

1. Understand the main attack surface areas for any IoT device or ecosystem
2. As a tester, be able to hit the major issues for each surface area for the product you're testing
3. As a manufacturer, be able to ensure that you've done your due diligence in security across the main surface areas
4. As a developer, be able to ensure that you're avoiding the top security issues while building your particular component
5. **As a consumer**, ensure you're using the technology safely

OWASP IoT Project Goals



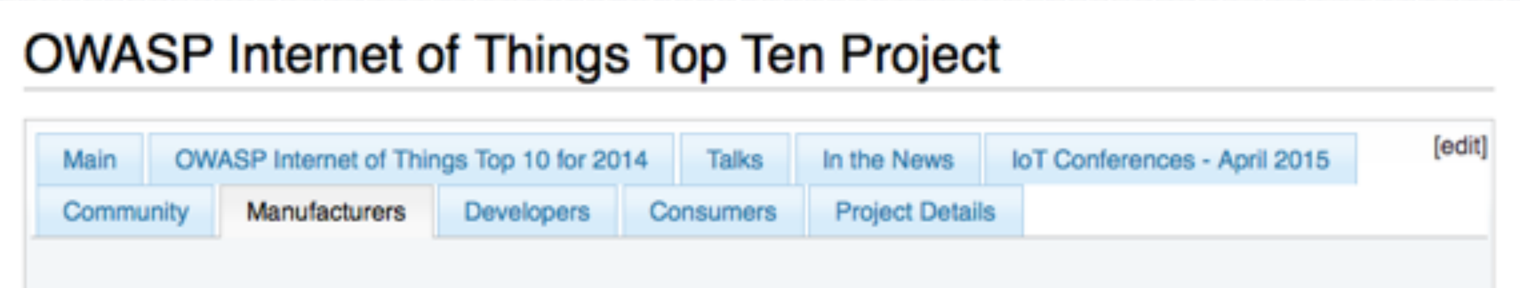
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. Understand the main attack surface areas for any IoT device or ecosystem
2. As a tester, be able to hit the major issues for each surface area for the product you're testing
3. As a manufacturer, be able to ensure that you've done your due diligence in security across the main surface areas
4. As a developer, be able to ensure that you're avoiding the top security issues while building your particular component
5. As a consumer, ensure you're using the technology safely

OWASP IoT Project Organization

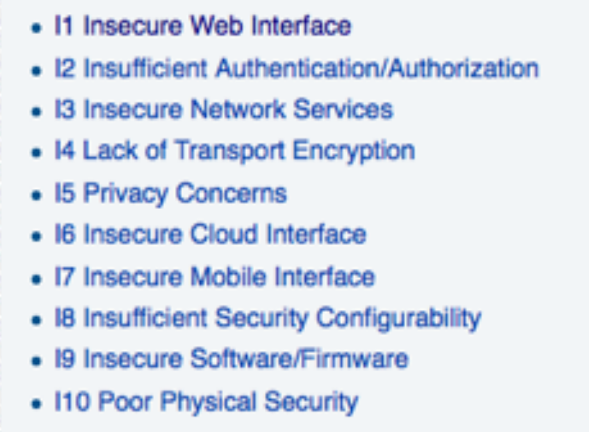


OWASP Internet of Things Top Ten Project

OWASP

Internet of Things Top 10

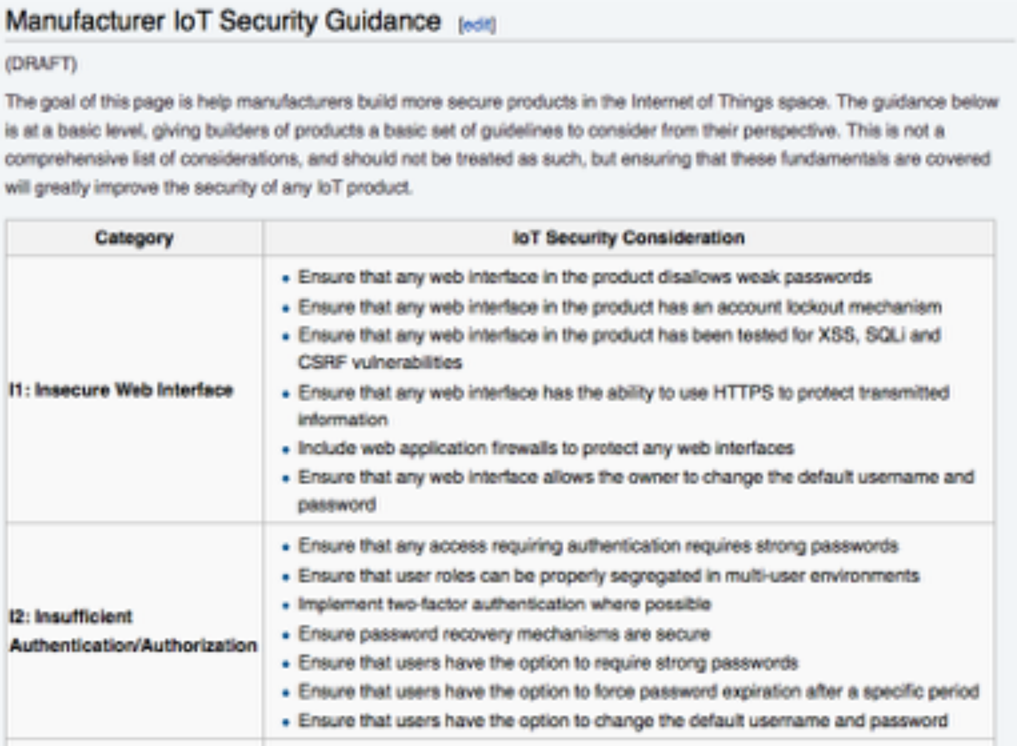
OWASP IoT Project (Context-based Recommendations)



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10



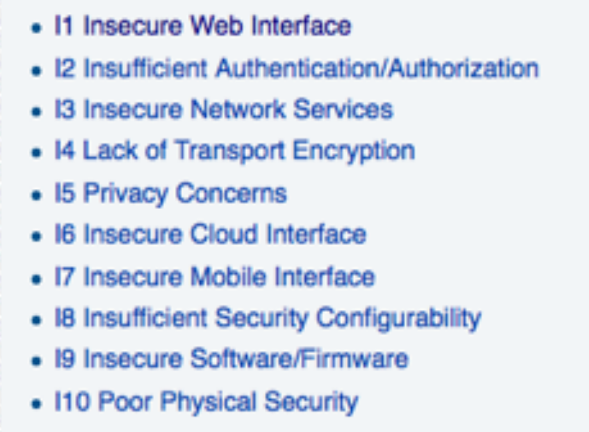
Manufacturer IoT Security Guidance [edit]

(DRAFT)

The goal of this page is help manufacturers build more secure products in the Internet of Things space. The guidance below is at a basic level, giving builders of products a basic set of guidelines to consider from their perspective. This is not a comprehensive list of considerations, and should not be treated as such, but ensuring that these fundamentals are covered will greatly improve the security of any IoT product.

Category	IoT Security Consideration
I1: Insecure Web Interface	• Ensure that any web interface in the product disallows weak passwords • Ensure that any web interface in the product has an account lockout mechanism • Ensure that any web interface in the product has been tested for XSS, SQLi and CSRF vulnerabilities • Ensure that any web interface has the ability to use HTTPS to protect transmitted information • Include web application firewalls to protect any web interfaces • Ensure that any web interface allows the owner to change the default username and password
I2: Insufficient Authentication/Authorization	• Ensure that any access requiring authentication requires strong passwords • Ensure that user roles can be properly segregated in multi-user environments • Implement two-factor authentication where possible • Ensure password recovery mechanisms are secure • Ensure that users have the option to require strong passwords • Ensure that users have the option to force password expiration after a specific period • Ensure that users have the option to change the default username and password

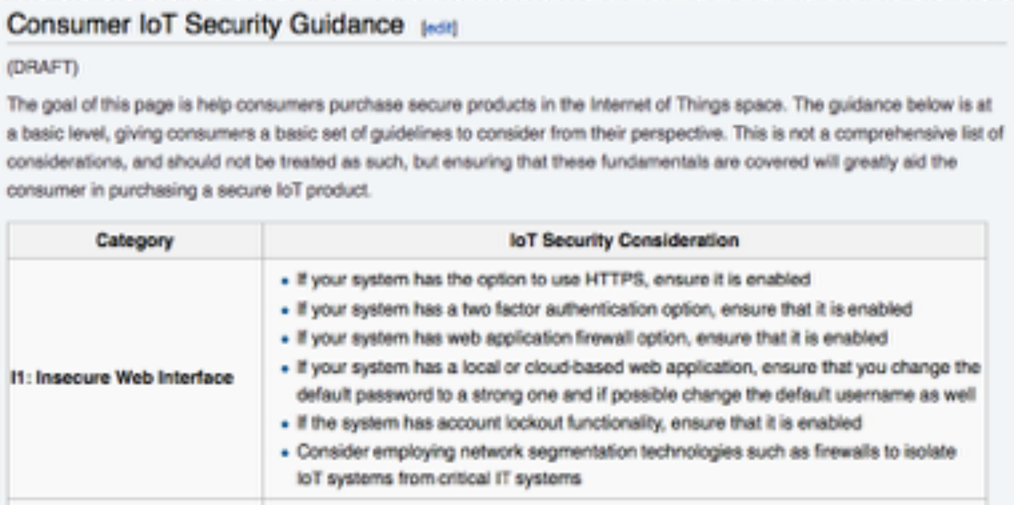
OWASP IoT Project (Consumer Recommendations)



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10



Consumer IoT Security Guidance [edit]

(DRAFT)

The goal of this page is help consumers purchase secure products in the Internet of Things space. The guidance below is at a basic level, giving consumers a basic set of guidelines to consider from their perspective. This is not a comprehensive list of considerations, and should not be treated as such, but ensuring that these fundamentals are covered will greatly aid the consumer in purchasing a secure IoT product.

Category	IoT Security Consideration
I1: Insecure Web Interface	• If your system has the option to use HTTPS, ensure it is enabled • If your system has a two factor authentication option, ensure that it is enabled • If your system has web application firewall option, ensure that it is enabled • If your system has a local or cloud-based web application, ensure that you change the default password to a strong one and if possible change the default username as well • If the system has account lockout functionality, ensure that it is enabled • Consider employing network segmentation technologies such as firewalls to isolate IoT systems from critical IT systems

OWASP IoT Project (FAQ)

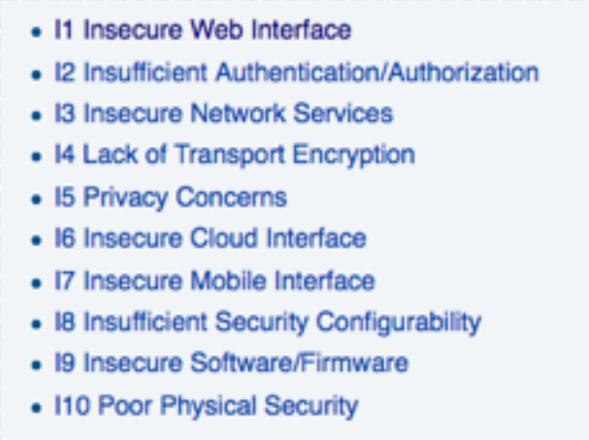
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. If IoT is just a collection of other technologies, why not just use existing OWASP projects?

OWASP IoT Project (FAQ)



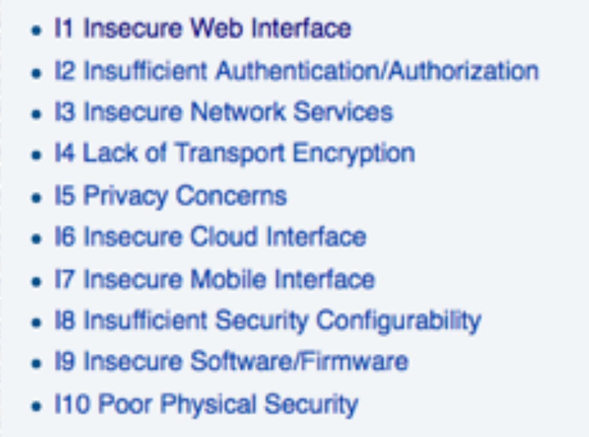
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. If IoT is just a collection of other technologies, why not just use existing OWASP projects? (one place, multiple spaces)
2. Why call it a Top 10 List, which is traditionally a list of vulnerabilities?

OWASP IoT Project (FAQ)



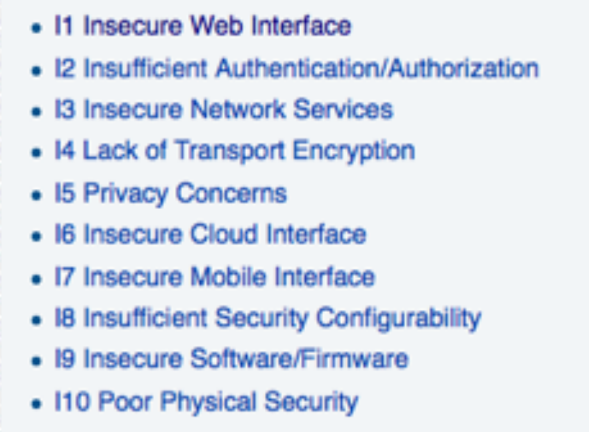
- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP

Internet of Things Top 10

1. If IoT is just a collection of other technologies, why not just use existing OWASP projects? (one place, multiple spaces)
2. Why call it a Top 10 List, which is traditionally a list of vulnerabilities? (tradition, approachability)
3. Why not have X category, or Y category, or you should move I7 to I2, etc.

OWASP IoT Project (FAQ)



- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

OWASP
Internet of Things Top 10

1. If IoT is just a collection of other technologies, why not just use existing OWASP projects? (one place, multiple spaces)
2. Why call it a Top 10 List, which is traditionally a list of vulnerabilities? (tradition, approachability)
3. Why not have X category, or Y category, or you should move I7 to I2, etc. (excellent, come help)

https://lists.owasp.org/mailman/listinfo/owasp_internet_of_things_top_ten_project

How to Apply This

Concept	Application

How to Apply This

Concept	Application
The Internet of Things is not just about sensors and machines. It's about people, and how they will continuously interact with their environments through their personal assistants and Universal Daemonization.	

How to Apply This

Concept	Application
The Internet of Things is not just about sensors and machines. It's about people, and how they will continuously interact with their environments through their personal assistants and Universal Daemonization.	You now know the future before others do, and can use that knowledge to inform better decisions.

How to Apply This

Concept	Application
The Internet of Things is not just about sensors and machines. It's about people, and how they will continuously interact with their environments through their personal assistants and Universal Daemonization.	You now know the future before others do, and can and use that knowledge to inform better decisions.
IoT Security is broken for three reasons: it's worst-of-all-worlds scenario, nobody is paid to secure IoT, and 1+1=5 when it comes to security and complexity.	

How to Apply This

Concept	Application
The Internet of Things is not just about sensors and machines. It's about people, and how they will continuously interact with their environments through their personal assistants and Universal Daemonization.	You now know the future before others do, and can use that knowledge to inform better decisions.
IoT Security is broken for three reasons: it's worst-of-all-worlds scenario, nobody is paid to secure IoT, and 1+1=5 when it comes to security and complexity.	You can now identify the common causes for the mistakes, and look out for them in projects you consult on.

OWASP
Internet of Things Top 10

How to Apply This

Concept	Application
The Internet of Things is not just about sensors and machines. It's about people, and how they will continuously interact with their environments through their personal assistants and Universal Daemonization.	Know the future before others do, and use that knowledge to inform better decisions.
IoT Security is broken for three reasons: it's worst-of-all-worlds scenario, nobody is paid to secure IoT, and 1+1=5 when it comes to security and complexity.	You can now identify the common causes for the mistakes, and look out for them in projects you consult on.
The OWASP IoT Top 10 Project maps IoT attack surface areas and gives contextual and prescriptive guidance on how to avoid vulnerabilities within each.	

OWASP
Internet of Things Top 10

How to Apply This

Concept	Application
The Internet of Things is not just about sensors and machines. It's about people, and how they will continuously interact with their environments through their personal assistants and Universal Daemonization.	Know the future before others do, and use that knowledge to inform better decisions.
IoT Security is broken for three reasons: it's worst-of-all-worlds scenario, nobody is paid to secure IoT, and 1+1=5 when it comes to security and complexity.	You can now identify the common causes for the mistakes, and look out for them in projects you consult on.
The OWASP IoT Top 10 Project maps IoT attack surface areas and gives contextual and prescriptive guidance on how to avoid vulnerabilities within each.	You can now use the OWASP IoT Project as a tangible guide to securing the IoT systems you work with.

OWASP
Internet of Things Top 10

Other IoT Resources

- Build It Securely Project (connects SMBs with researchers)
  - Mark Stanislav and Zach Lanier
- I am the Cavalry (focuses on automotive IoT security)
  - Josh Corman
- IoT Firmware Testing Training
  - Paul Asadoorian (BlackHat)

Just One More Thing…

HELPING SECURE THE INTERNET OF THINGS WITH THE

OWASP INTERNET OF THINGS TOP 10

VULNERABILITY CATEGORIES

1 Insecure Web Interface

covers IoT device administrative interfaces

Obstacles

- Default usernames and passwords
- No account lockout
- XSS, CSRF, SQLi vulnerabilities

Solutions

- Allow default usernames and password to be changed
- Enable account lockout
- Conduct web application assessments

2 Insufficient Authentication/Authorization

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

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

- **OWASP IoT Top 10 Mini-poster !**
  - Card stock
  - Two-sided
  - Covers Top 10 Surface Areas
  - Available for download as well

OWASP

Internet of Things Top 10

Thank you!

OWASP

Internet of Things Top 10

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

Daniel.Miessler@owasp.org

daniel@hp.com

daniel@danielmiessler.com
https://danielmiessler.com
@danielmiessler