What someone said about “junk hacking”

Yes, we get it. Cars, boats, buses, and those singing fish plaques are all hackable and have no security. **Most conferences these days have a whole track called "Junk I found around my house and how I am going to scare you by hacking it".** That stuff is always going to be hackable whetherornotyouarethecalvalry.org.

... 

**So in any case, enough with the Junk Hacking**, and enough with being amazed when people hack their junk.
IoT Attack Surface Mapping

Seeking a universal, surface-area approach to IoT testing

Daniel Miessler
IoT Village, DEFCON 23
August 2015
Junk Hacking and Vuln Shaming

Yes, we get it. Cars, boats, buses, and those singing fish plaques are all hackable and have no security. **Most conferences these days have a whole track called "Junk I found around my house and how I am going to scare you by hacking it".** That stuff is always going to be hackable whetherornotyouarethecalvalry.org.

...  

**So in any case, enough with the Junk Hacking**, and enough with being amazed when people hack their junk.
What’s in a name?

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

BETTER NAMES FOR IOT?

ANYTHING OTHER THAN "THE INTERNET OF THINGS"
Defining IoT

- [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.

- [MY PREFERRED] The interface between the physical and digital world that allows one to gather information from—and control—everyday objects.
What to do?
What to do?
What to do?
What to do?
What to do?
IoT Security != Device Security
Existing approaches...

- Look at a collection of common vulnerabilities, risks, etc.
- Pull up your go-to list
- Consider some bad scenarios
- Check for what others have found on other devices
The OWASP Internet of Things Top 10 (tentative) - 2014 is as follows:

- 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 Updates
- I10 Poor Physical Security

### Top 10 Risks

#### OWASP Mobile Top 10 Risks

<table>
<thead>
<tr>
<th></th>
<th>M1 - Insecure Data Storage</th>
<th>M6 - Improper Session Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>M2 - Weak Server Side Controls</td>
<td>M7 - Security Decisions Via Untrusted Inputs</td>
</tr>
<tr>
<td></td>
<td>M3 - Insufficient Transport Layer Protection</td>
<td>M8 - Side Channel Data Leakage</td>
</tr>
<tr>
<td></td>
<td>M4 - Client Side Injection</td>
<td>M9 - Broken Cryptography</td>
</tr>
<tr>
<td></td>
<td>M5 - Poor Authorization and Authentication</td>
<td>M10 - Sensitive Information Disclosure</td>
</tr>
</tbody>
</table>

(Click on the diagram for more details.)
The Previous Version

- Used the Top 10 name
- Mixed surfaces with vulnerability types
New OWASP IoT Project Structure

- IoT Project
- Attack Surface Areas
- Testing Guide
- Top Vulnerabilities
Subtle differences in approach
Different approaches to finding vulns

1. Let me check against this list of vulns
Different approaches

1. Let me check against this list of vulns.

2. Let me check my favorite go-to issues
Different approaches

1. Let me check against this list of vulns.

2. Let me check my favorite go-to issues

3. What common surface areas do IoT systems share that I need to make sure I don’t miss?
The IoT Attack Surfaces
Ecosystem Access Control

- Authentication
- Session management
- Implicit trust between components
- Enrollment security
- Decommissioning system
- Lost access procedures
Device Memory

- Cleartext usernames
- Cleartext passwords
- Third-party credentials
- Encryption keys
Device Physical Interfaces

- Firmware extraction
- User CLI
- Admin CLI
- Privilege escalation
- Reset to insecure state
Device Web Interface

- SQL injection
- Cross-site scripting
- Username enumeration
- Weak passwords
- Account lockout
- Known credentials
Device Firmware

- Hardcoded passwords
- Sensitive URL disclosure
- Encryption keys
Device Network Services

- Information disclosure
- User CLI
- Administrative CLI
- Injection
- Denial of Service
Administrative Interface

✓ SQL injection
✓ Cross-site scripting
✓ Username enumeration
✓ Weak passwords
✓ Account lockout
✓ Known credentials
Local Data Storage

- Unencrypted data
- Data encrypted with discovered keys
- Lack of data integrity checks
Cloud Web Interface

✓ SQL injection
✓ Cross-site scripting
✓ Username enumeration
✓ Weak passwords
✓ Account lockout
✓ Known credentials
Third-party Backend APIs

- ✓ Unencrypted PII sent
- ✓ Encrypted PII sent
- ✓ Device information leaked
- ✓ Location leaked
Update Mechanism

✓ Update sent without encryption
✓ Updates not signed
✓ Update location writable
Mobile Application

✓ Implicitly trusted by device or cloud
✓ Known credentials
✓ Insecure data storage
✓ Lack of transport encryption
Vendor Backend APIs

- Inherent trust of cloud or mobile application
- Weak authentication
- Weak access control
- Injection attacks
Ecosystem Communication

- ✓ Health checks
- ✓ Heartbeats
- ✓ Ecosystem commands
- ✓ Deprovisioning
- ✓ Update pushes
Network Traffic

- LAN
- LAN to Internet
- Short range
- Non-standard
IoT Attack Surface Areas

- Ecosystem Access Control
- Device Web Interface
- Administrative Interface
- Ecosystem Communication
- Update Mechanism
- Network Traffic
- Device Memory
- Device Firmware
- Local Data Storage
- Vendor Backend APIs
- Mobile Application
- Device Physical Interfaces
- Device Network Services
- Cloud Web Interface
- Third-party Backend APIs
- Vendor Backend APIs
The OWASP IoT Attack Surfaces Project

https://www.owasp.org/index.php/OWASP_IoT_Attack_Surface_Areas
## Surfaces $\rightarrow$ vulns $\rightarrow$ data

<table>
<thead>
<tr>
<th>Attack Surface</th>
<th>Vulnerability</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative interface</td>
<td>Weak password policy</td>
<td>Credentials</td>
</tr>
<tr>
<td></td>
<td>Lack of account lockout</td>
<td></td>
</tr>
<tr>
<td>Local data storage</td>
<td>Data stored without encryption</td>
<td>PII</td>
</tr>
<tr>
<td>Web Cloud Interface</td>
<td>SQLi</td>
<td>PII, Account data</td>
</tr>
<tr>
<td>Device Firmware</td>
<td>Sent over HTTP</td>
<td>Credentials, Application data</td>
</tr>
<tr>
<td></td>
<td>Hardcoded passwords</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardcoded encryption keys</td>
<td></td>
</tr>
<tr>
<td>Vendor Backend APIs</td>
<td>Permissive API Data Extraction</td>
<td>PII, Account data</td>
</tr>
<tr>
<td>Device Physical Interfaces</td>
<td>Unauthenticated root access</td>
<td>***</td>
</tr>
</tbody>
</table>
Back to the network…

Network Traffic

✓ LAN
✓ LAN to Internet
✓ Short range
✓ Non-standard
What people think they have
What people actually have

cleartext honeytoken

cleartext sensitive data

cleartext sensitive data

cleartext sensitive data
What I like to look for in pcaps

1. How many connections were made?

2. To how many destinations?

3. Was the sensitive data I entered into the ecosystem seen in the network traffic?

4. If so, that’s bad
A quick and dirty PCAP parser that helps you identify who your applications are sending sensitive data to without encryption.

---

*Added main code.*

**danielmiessler** authored 3 days ago

- **README.md**: Updated readme.
- **caparser.sh**: Added main code.

---

**README.md**

**caparser**

A quick and dirty PCAP parser created to assist network traffic analysis in IoT and Mobile security assessments, caparse shows you where your applications are sending cleartext sensitive data.
Getting your capz

Dualcomm DCGS-2005L
10/100/1000Base-T Gigabit Network TAP (Plastic Case)
by Dualcomm

⭐⭐⭐⭐⭐ 13 customer reviews
| 5 answered questions

Price: $179.95 ✓Prime | FREE One-Day

Only 13 left in stock.
Sold by Dualcomm and Fulfilled by Amazon. Gift-wrap available.

- USB Powered Gigabit Network Tap
- PoE Inline Power Pass-Through
- Also function as a 5-Port Gigabit Ethernet Switch
- No Software Configuration Needed. Plug & Play
- Portable.
ONE DOES NOT SIMPLY

DO INTERNET-BASED DEMOS AT DEFCON
daniel at evolus in ~/Development/caparser (master●●)
$
The OWASP IoT Attack Surfaces Project

https://www.owasp.org/index.php/OWASP_IoT_Attack_Surface_Areas
A quick and dirty PCAP parser that helps you identify who your applications are sending sensitive data to without encryption. — Edit

Added main code.

A quick and dirty PCAP parser created to assist network traffic analysis in IoT and Mobile security assessments, caparse shows you where your applications are sending cleartext sensitive data.
Sister projects

I Am The Cavalry

Build It Secure.ly
This is a Craig Smith Slide

Craig Smith
Takeaways and Goodies

1. IoT testing is the same as any other testing
Takeaways and Goodies

1. IoT testing is the same as any other testing
2. IoT security is NOT device security
Takeaways and Goodies

1. IoT testing is the same as any other testing
2. IoT security is NOT device security
3. The IoT Attack Surface area project is proposing a universal attack strategy for any kind of device
Takeaways and Goodies

1. IoT testing is the same as any other testing
2. IoT security is NOT device security
3. The IoT Attack Surface area project is proposing a universal attack strategy for any kind of device
4. **A big part of that is the network piece**
Takeaways and Goodies

1. IoT testing is the same as any other testing
2. IoT security is NOT device security
3. The IoT Attack Surface area project is proposing a universal attack strategy for any kind of device
4. A big part of that is the network piece
5. **Caparser is a tool that can do that analysis for you**
Takeaways and Goodies

1. IoT testing is the same as any other testing
2. IoT security is NOT device security
3. The IoT Attack Surface area project is proposing a universal attack strategy for any kind of device
4. A big part of that is the network piece
5. Caparser is a tool that can do that analysis for you
6. **Caparser is free, released today, and will be improved in the near future**
Takeaways and Goodies

1. IoT testing is the same as any other testing
2. IoT security is NOT device security
3. The IoT Attack Surface area project is proposing a universal attack strategy for any kind of device
4. A big part of that is the network piece
5. Caparser is a tool that can do that analysis for you
6. Caparser is free, released today, and will be improved in the near future
7. **Craig Smith is awesome**
Takeaways and Goodies

1. IoT testing is the same as any other testing
2. IoT security is NOT device security
3. The IoT Attack Surface area project is proposing a universal attack strategy for any kind of device
4. A big part of that is the network piece
5. Caparser is a tool that can do that analysis for you
6. Caparser is free, released today, and will be improved in the near future
7. Craig Smith is awesome
8. There’s a handout!
**IoT Testing Guidance**

**Insecure Web Interface**
- Assess any web interface to determine if weak passwords are allowed
- Assess the account lockout mechanism
- Assess the web interface for XSS, SQLi, and CSRF vulnerabilities and other web application vulnerabilities
- Assess the use of HTTPS to protect transmitted information

**Insufficient Authentication/Authorization**
- Assess the solution for the use of strong passwords where authentication is needed
- Assess the solution for implementation two-factor authentication where possible
- Assess password recovery mechanisms
- Assess the solution for the option to require strong passwords
- Assess the solution for the option to force password expiration after a specific period

**Privacy Concerns**
- Assess the solution to determine the amount of personal information collected
- Assess the solution to determine if collected personal data is properly protected using encryption at rest and in transit
- Assess the solution to determine if ensuring data is de-identified or anonymized

**Lack of Transport Encryption**
- Assess the solution to determine the use of encrypted communication between devices and between devices & internet
- Assess the solution to determine if accepted encryption practices are used and if proprietary protocols are avoided
- Assess the solution to determine if a firewall option is available

**Insecure Security Configurability**
- Assess the solution to determine if password security options are available
- Assess the solution to determine if encryption options (e.g. enabling AES-256 where AES-128 is the default setting) are available
- Assess the solution to determine if logging for security events

**Insecure Cloud Interface**
- Assess the cloud interfaces for security vulnerabilities
- Assess the cloud-based web interface to ensure it disallows weak passwords
- Assess the cloud-based web interface to ensure it includes an account lockout mechanism
- Assess the cloud-based web interface to determine if two-factor authentication is used
- Assess any cloud interfaces for XSS, SQLi, and CSRF vulnerabilities and other vulnerabilities
- Assess all cloud interfaces to ensure transport encryption is used
- Assess the cloud interfaces to determine if the option to require strong passwords is available

**Insecure Mobile Interface**
- Assess the mobile interface to ensure it disallows weak passwords
- Assess the mobile interface to ensure it includes an account lockout mechanism
- Assess the mobile interface to determine if it implements two-factor authentication
- Assess the mobile interface to determine if it uses transport encryption
- Assess the mobile interface to determine if the option to require strong passwords is available
- Assess the mobile interface to determine if the option to change the default username and password is available
- Assess the mobile interface to determine if the amount of personal information collected

**Poor Physical Security**
- Assess the device to ensure it utilizes a minimal number of physical external ports (e.g. USB ports) on the device
- Assess the device to determine if it can be accessed via unintended methods such as through an unnecessary USB port

**Insecure Software/Firmware**
- Assess the device to ensure it includes update capability & can be updated quickly when vulnerabilities are discovered
- Assess the device to ensure it uses encrypted update files and that the files are transmitted using encryption
- Assess the device to ensure it uses signed files and then validates that file before installation

**Insecure Network Services**
- Assess the solution to ensure network services don’t respond poorly to buffer overflow, fuzzing or denial of service attacks
- Assess the solution to ensure test ports are not present
Thank you!

The OWASP IoT Attack Surfaces Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Caparser
https://github.com/danielmiessler/caparser

@danielmiessler
@craigz28

TX to HP Fortify on Demand