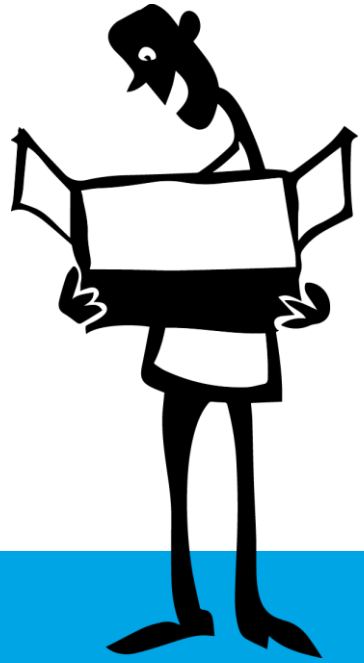
# Security Testing

Harri Susi
06.04.2018



**Connected cars have an 'indefensible' security vulnerability**
Network World - 23 Aug 2017
In a blog post published last week, "The Crisis of Connected Cars: When **Vulnerabilities** Affect the CAN Standard," the company publicized an ...

**Security flaw in IoT solar equipment could disrupt Europe's electricity ...**
The Internet of Business (blog) - 11 Aug 2017
A Dutch security researcher claims to have found **vulnerabilities** in internet-connected solar panel equipment installed throughout Europe, ...

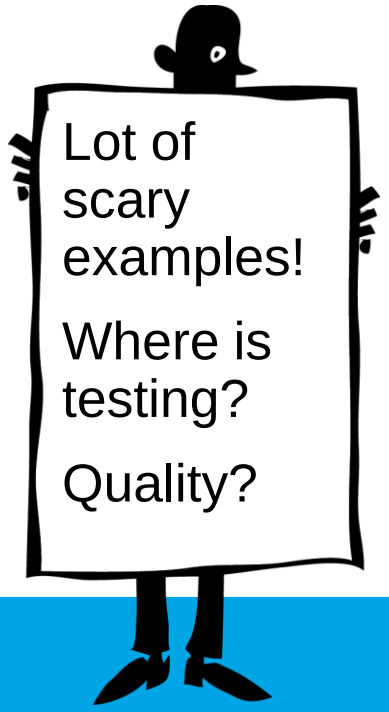
**Industrial Cobots Might Be The Next Big IoT Security Mess**
Threatpost - 22 Aug 2017
Researchers at IOActive have found nearly 50 **vulnerabilities** in industrial collaborative robots, machines that work side-by-side with people in ...

Popular Robots are Dangerously Easy to Hack, Researchers Say
SuperSite for Windows - 23 Aug 2017

**Router flaws put AT&T customers at hacking risk**
ZDNet - 23 minutes ago
Among the **vulnerabilities** are hardcoded credentials, which can allow ... Rapid7 reported the **vulnerability** as an 8/10, on the higher end of the ...

**For cybercriminals, IoT devices are big business, part two**
TechTarget (blog) - 17 Aug 2017
The **Internet of Things** (**IoT**) world may be exciting, but there are serious ... That's because these attacks targeted a **vulnerability** for which a ...

3 ways developers can improve **IoT** security on their devices
Network World - 18 Aug 2017



# 3 Principles of Data Security, CIA triad

1. Confidentiality
   - Data privacy issues: encryption (AES256), tamperproof system…
   - Authentication, e.g. IPSec
   - GDPR: Privacy/security by design, right to have data removed, …
2. Integrity
   - Data can be trusted, checksums are included & verified, data is validated (secure hashes, SHA256). Use e.g. IPSec/&TLS1.2
   - data cannot be modified by accidentally (e.g. system crash/electricity lost) or by any malicious factors
   - GDPR: data may not change unless the individual says so
3. Availability
   - The system/devices are stabile
   - The system/devices have enough bandtwidth/capacity (DoS attacks?)
   - Failover/recover mechanism for hardware issues
   - Devices are easy to maintain, e.g. batteries
   - GDPR: the individual must have access to her/his personal data at all times

# Threat Model Driven Testing

There are threats…

… ways to mitigate them

and you need to validate mitigations

-> threat model driven testing!

# Threat Modelling – what is that?

- Threat modelling is a process/workshop where a team plans how to design the system the way it makes it a hard target for the attackers
- WHY? Understanding how an attacker can compromise the system helps the team to analyze the design and make appropriate design decisions to mitigate the potential threats
- https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-architecture
- Two different level of threat modelling workshops: upper-level (business-risks) and technical for the software/application(s) / devices

# Threat Modelling process

- Model the solution/system/application
  - Draw it on a white board together with the team! (e.g. use data flow diagram)
- Enumerate Threats
  - STRIDE: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of priviledge
- Mitigate threats by changing your design
  - Create security user stories
  - Create evil-user stories
  - Create test cases
- Validate the mitigations
  - Test it!

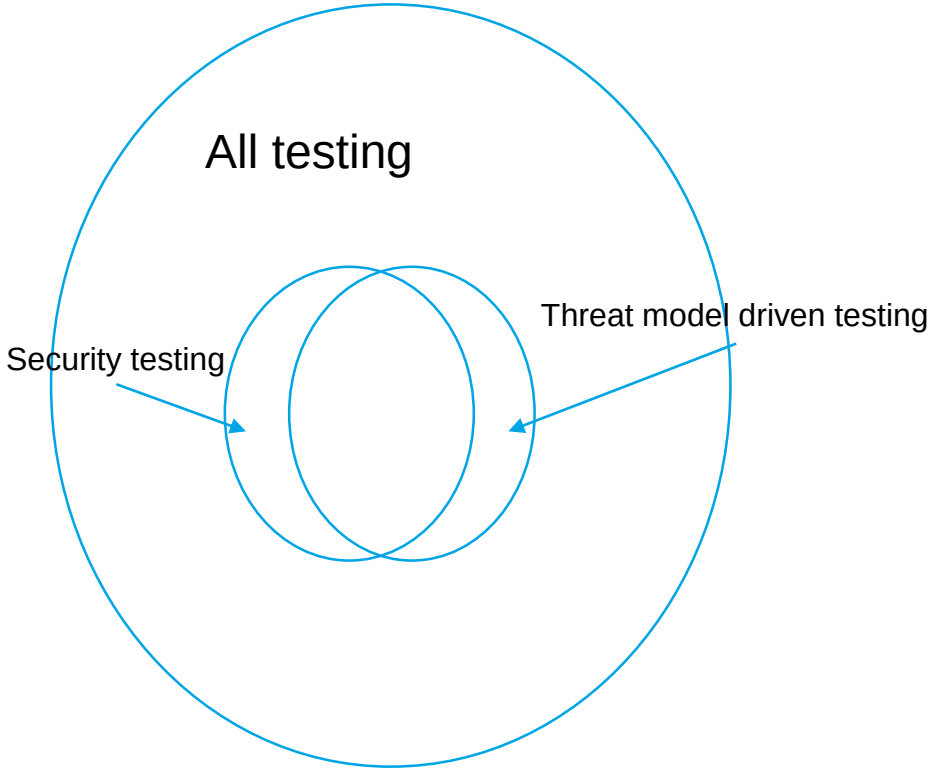
# Theat Modelling: STRIDE

## the method to detect threats

1) Spoofing identity
2) Tampering with data
3) Repudation
4) Information disclosure
5) Denial of service
6) Elevation of Priviledge

# Verifying threat mitigations, testing

## Types of testing




Validating threat mitigations needs to be part of testing. It is not just security testing but also verifying other cases found during threat modelling

# Some other types of security testing

# Security testing: negative testing

- Behave like a bad user or malicious user
- What if I put SQL commands here instead of proper plain text?
- SQL -, HTML - , Javascript injections
- Stress testing
- How error messages are shown? Any sensitive information revealed in the error message, e.g. SQL table names?

# Security testing, positive testing

Verifying the proper implementations of security features…

- Is traffic encrypted?
- Is the stored data encrypted?
- Test authentication and authorization process…

# Security testing: boundary tests

- JUST INSIDE – JUST OUTSIDE – think about corner cases
- If the expected value is something between 1 – 100 try values 0 (= just outside) or 100 (just inside)
- But never forgot to test typical values and error values also (strings into integer fields, etc…)

# Security testing: vulnerability scanning

- The idea of vulnerability scanners is to scan the DUT againsts known vulnerabilities but also check all open ports and offered services
- There are some good commercial vulnerability scanners available, e.g. F-Secure RADAR.  Or you can create your own tool (reading tip: Black Hat Python book)
- https://www.shodan.io/ Search engine for IoT! Is your system visible? How does it respond? Too friendly?
- Other related tools, e.g. network scanning tools: Wireshark, Nessus, …

# Security testing: Fuzzing

Fuzz testers taking less time to spot **vulnerabilities** in **IoT** protocols
SC Magazine UK - 10 Aug 2017
The study also found a common protocol used in **IoT** devices, which are notorious for being plagued with **vulnerabilities**, was significantly more ...

- Fuzzing (*fin*: ”sumea testaus”) is about sending malicious input to the system under test. The input is sent by specific tool (the fuzzer). The sent data is generated with help of fuzzing algorithms. The test engineer feeds the tool with the proper seed data…
- Use the best possible tools but quite often you need to do some customization…
- Radamssa, Burp Suite, etc…

# Security testing…

can be also about **penetration testing** – everything white hat hackers do...

E.g. combination of vulnerability scanning, negative testing and some social engineering (reconnaissance)

but that’s another story!

# Security testing

Is also about professional software development process including static code analysis, unit tests, code reviews…

# Finally…

# DevOps is Dead – Long Live DevSecOps!

# Thank You!

# Any questions?


Etteplan