



OWASP
AppSec Europe
London 2nd-6th June 2018

Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO



Dan Cornell

- Founder and CTO of Denim Group
- Software developer by background
- OWASP San Antonio co-leader
- 20 years experience in software architecture, development, and security



Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO



DENIM GROUP

Building a world where technology is trusted

Denim Group is solely focused on helping build resilient software that will withstand attacks.

- Since 2001, helping secure software
- Development background
- Tools + services model

How we can help:



Advisory
Services



Assessment
Services



Remediation
Services



ThreadFix

Powered by Denim Group

Vulnerability Resolution
Platform

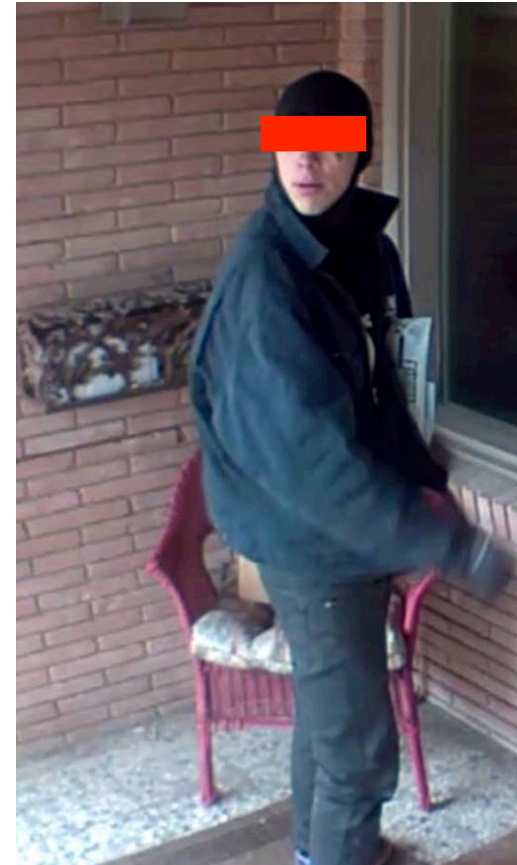


OWASP
AppSec Europe
London 2nd-6th June 2018

Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

This Wasn't
In My IoT
Threat Model



Agenda

IoT Overview

Goals of Threat Modeling

Why Threat Model IoT?

Threat Modeling Overview

IoT Threat Modeling Particulars

Conclusion/Questions

IoT Overview

Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

IoT is Cool



nest™



amazon alexa



ring



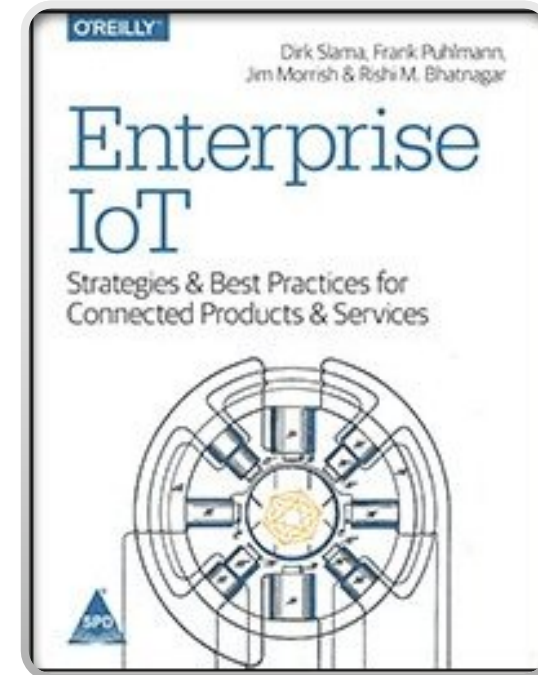
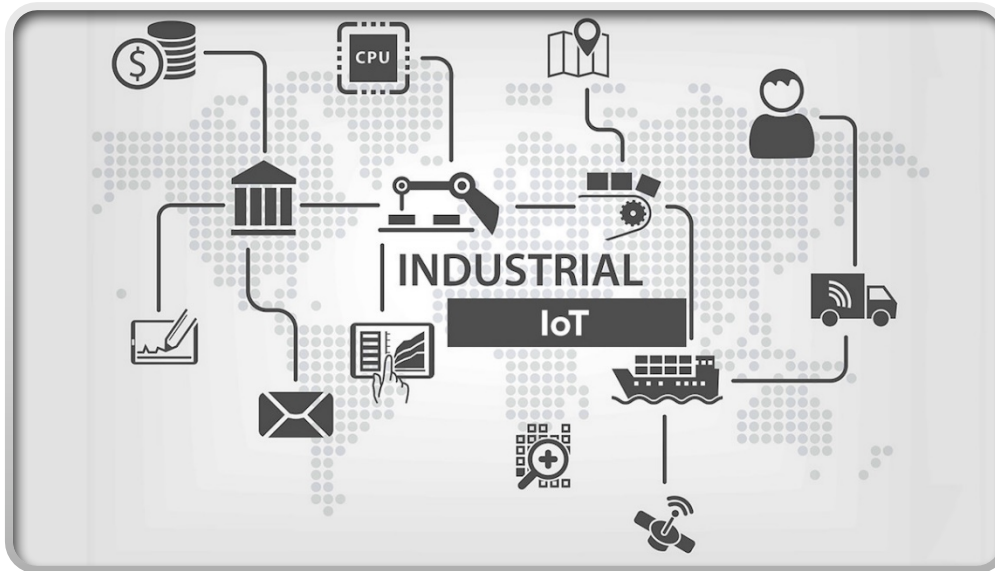
fitbit



Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

But IoT Isn't Just Consumer IoT



- <http://zinnov.com/how-startups-are-driving-an-iiot-revolution/>
- <https://www.amazon.in/Enterprise-IoT-Dirk-Slama/dp/9352132513>

Definitions (That I Made Up)

- Consumer IoT
 - IoT systems sold to the general populace. Front-door cameras, exercise trackers, personal assistants, etc
- Enterprise IoT
 - Enterprise organizations deploying IoT systems – largely consumer-focused – into enterprise environments
- Industrial IoT
 - More specialized IoT systems sold to industrial environments. Smart lighting, hyper-connected control systems, industrial equipment enhancements, etc

So Why Are YOU Concerned About IoT Security?

Consumer: I'm using IoT devices. Is that safe?

Enterprise and Industry: I'm deploying IoT devices in my environment. What are my risks?

Developer: I'm building IoT systems. What should I worry about?

So Let's Talk About (My) Bias

My view of this topic is skewed by my experience – which is acting as a consulting firm helping organizations deal with the risks associated with IoT

Consumers don't pay us because they're too poor

BUT people that sell things to consumers do occasionally pay us in order to protect their brands

Enterprises pay us to help them be safer when deploying IoT into their enterprise IT infrastructures

Industrial organizations pay us to help them be safer when deploying IoT into their industrial environments

IoT system builders pay us to help them build safer IoT systems – when there are appropriate economic incentives to do so

Consumers

- Sophisticated consumers might informally threat model IoT systems they let into their lives
- But really they just kinda get what they're going to get...
- Rely on brand to make trust decisions

Enterprise and Industry

- This is largely a supply-chain concern
- Threat modeling can be used to identify potential risks during the acquisition process
- Assessments can be used to identify vulnerabilities during the acquisition process
- Note that I said “acquisition” not “deployment” or “even later”
 - Because once you have purchased then it is your problem

Developers

- Threat model during development to avoid huge issues that are expensive to fix and embarrassing to have publicly revealed
- Threat model after development to target internal red team activities
- Use security as a differentiator for discerning customers

Goals of Threat Modeling

Why Threat Model?

- Avoid introducing vulnerabilities
- Identify vulnerabilities in an existing system
- Understand the system

Avoid Introducing Vulnerabilities

- It is cheaper to identify vulnerabilities on the whiteboard than to fix them at the keyboard
- Threat modeling is a great way to proactively identify potential issues and address them during the design process



Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

Find Existing Vulnerabilities

- Threat modeling provides a structured way to look at systems
- This structure can provide consistency to assessments



Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

Understand the System

- What are the parts?
- How do they fit together?
- "If I change this, what happens to that?"
- Encourages critical thinking – especially with developers

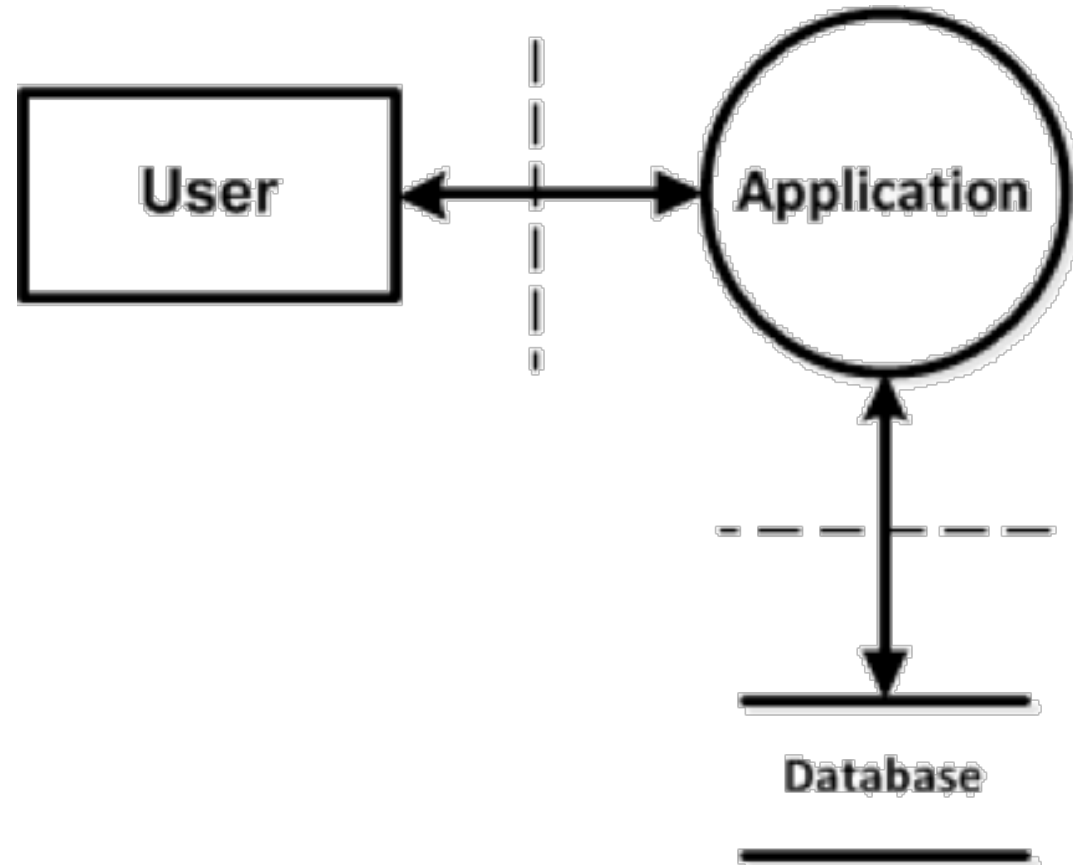
Why Threat Model IoT?



Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

The Good Old Days

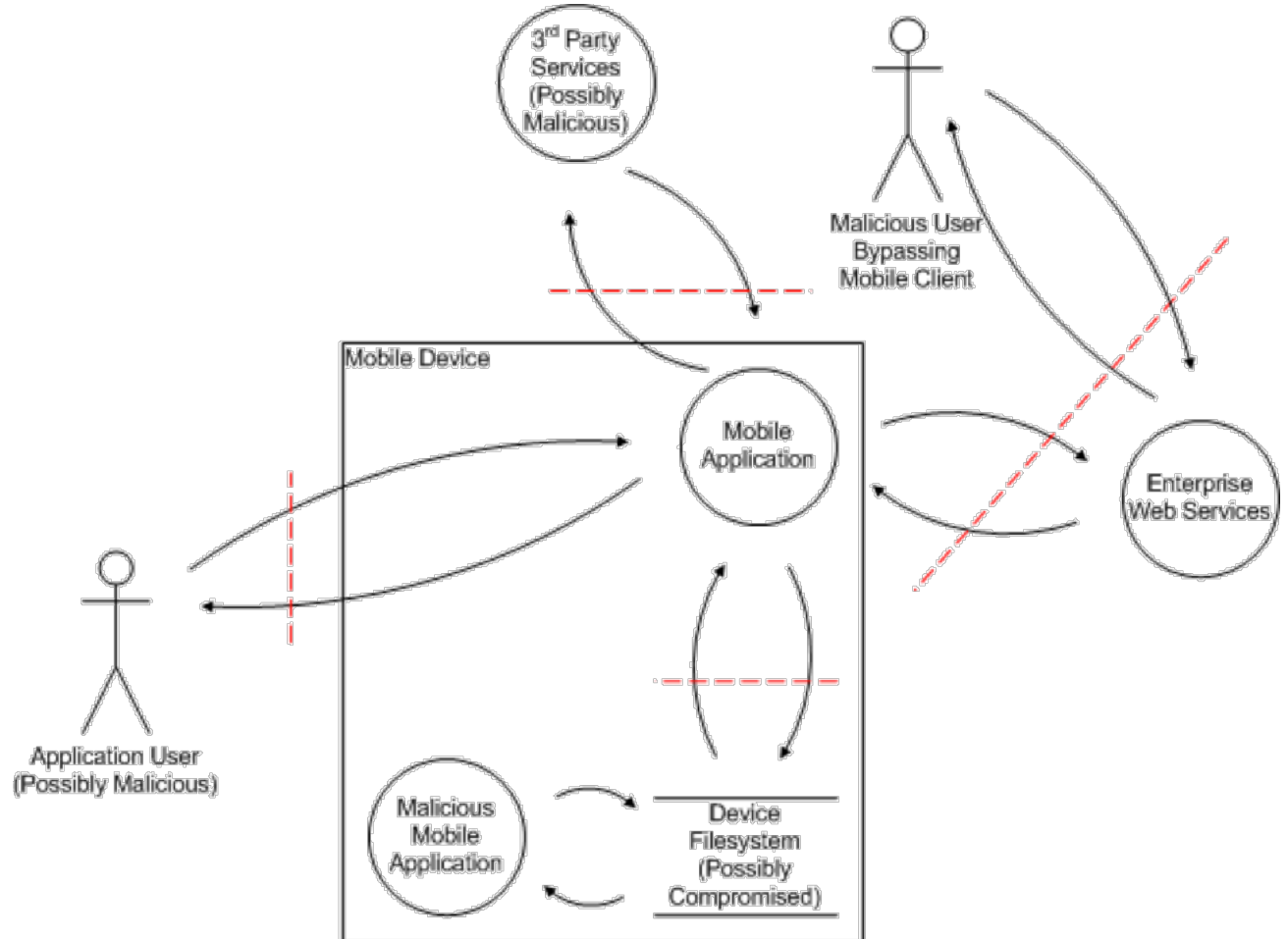




Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

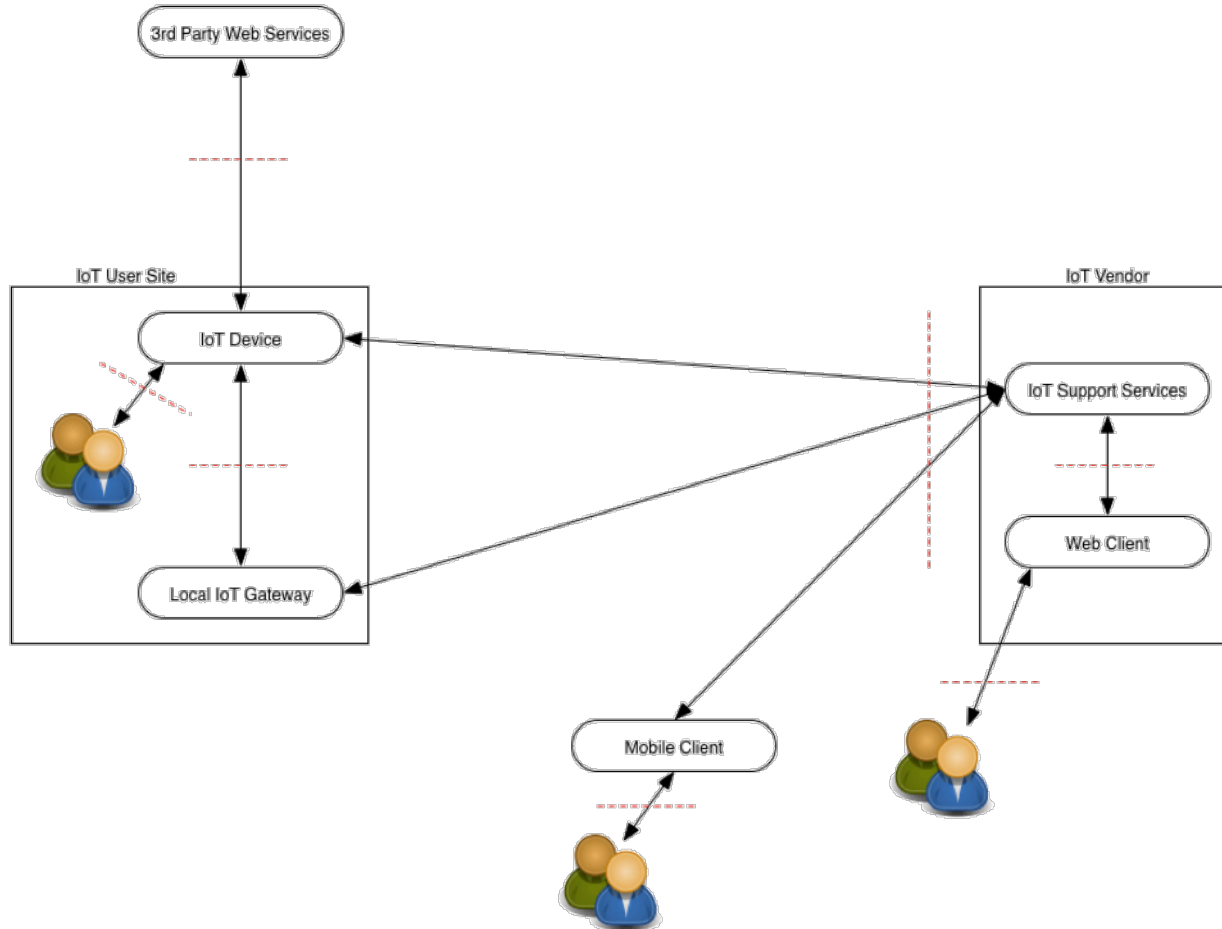
Oh Crap, Mobile!





Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO



Argh!
IoT!

How I Realized the World Had Changed

- Mobile application assessments:
 - Sensible template threat model, easy statistics collection
 - Where in the system are vulnerabilities found?
 - What technique (static/dynamic, automated/manual) was used to find them?
 - Fun and valuable research presented at:
 - RSA:
https://www.rsaconference.com/writable/presentation/s/file_upload/mbs-f02-mobile-application-assessments-by-the-numbers-v2.pdf
 - OWASP AppSecEU:
<https://www.slideshare.net/denimgroup/application-security-assessments-by-the-numbers-owaspappseceu20151>



How I Realized the World Had Changed (Cont'd)

- IoT application assessments
 - Created initial sensible threat model based on a consumer example
 - Start looking at statistics collection
 - “Oh, crap. That doesn’t work for this enterprise case. Let’s revise.”
 - “Oh, crap. That works even worse for this industrial case. Let’s revise again.”
 - “Sensible” threat model template no longer looks sensible
- Here is a starting point:
 - <https://denimgroup.com/resources/blog/2017/11/getting-started-with-iot-security-with-threat-modeling/>

So Where Does That Leave Us?

- IoT environments are complicated
- Potentially significantly more so that what most are used to
- Threat modeling is more valuable – and more necessary – than ever

Threat Modeling Overview

High Level Threat Modeling Concepts

1

Decide on
scope

2

Build your
dataflow
diagrams

3

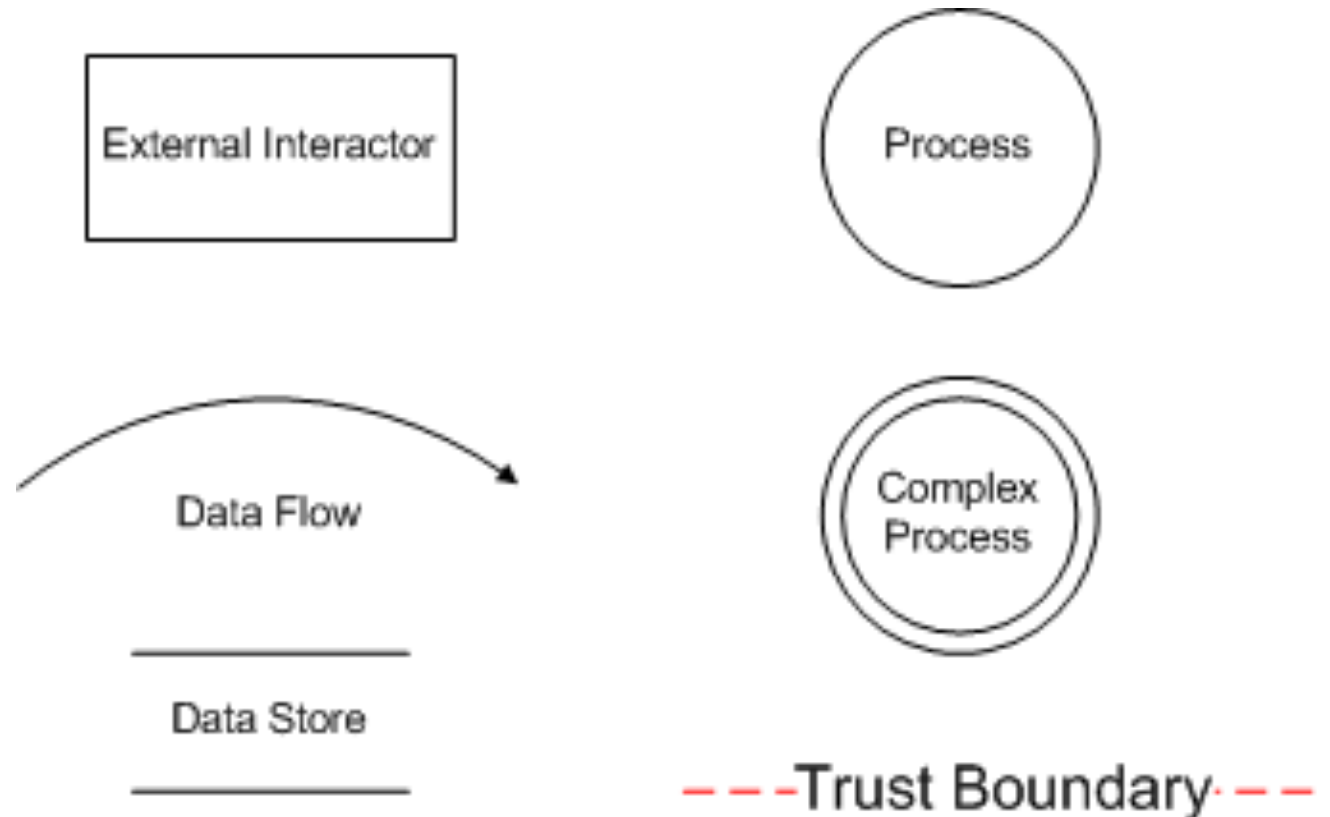
Enumerate
threats

4

Decide on
mitigations

Creating Data Flow Diagrams (DFDs)

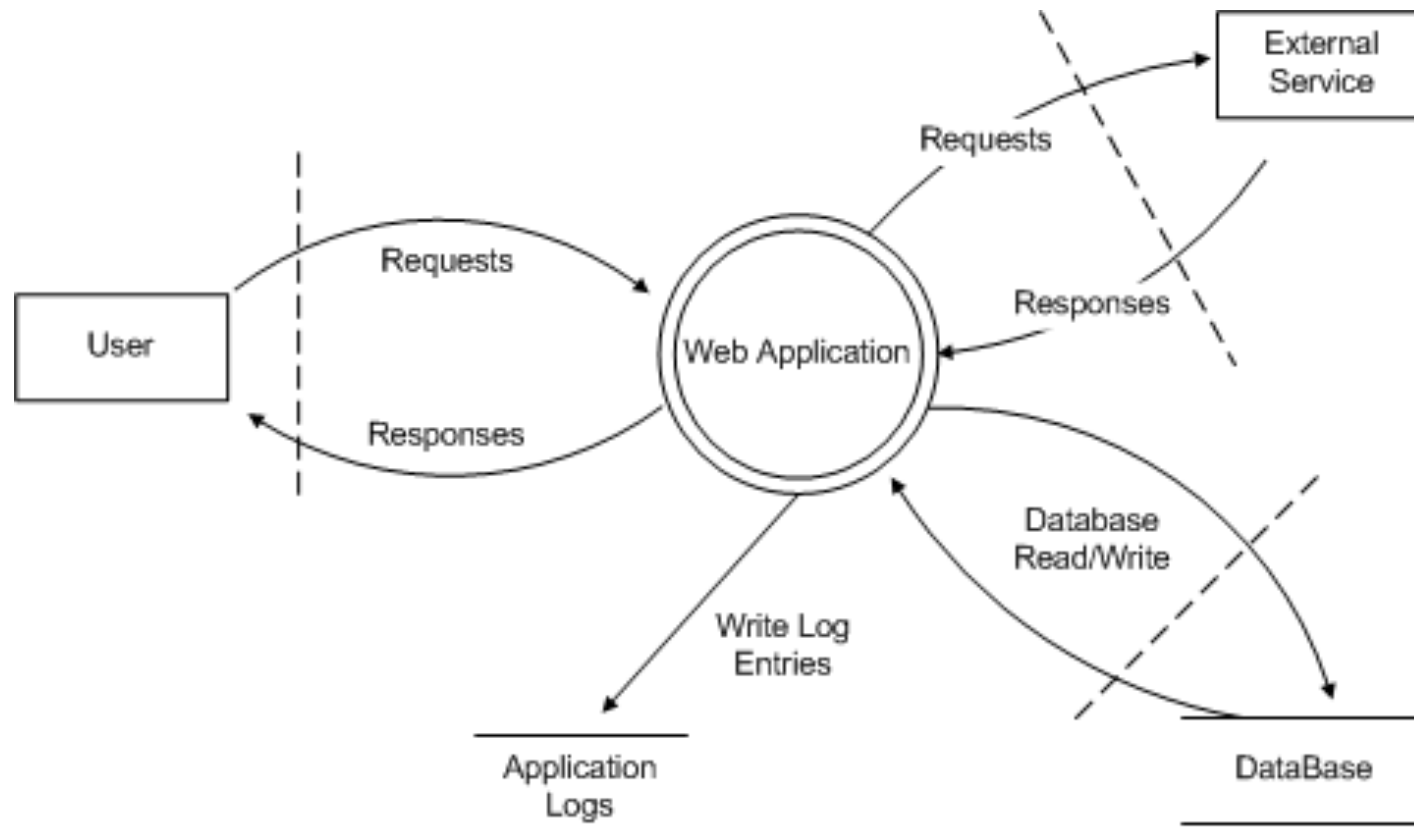
- Decompose the system into a series of processes and data flows
- Explicitly identify trust boundaries



Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

Example Data Flow Diagram





Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

Identifying Threats from the Data Flow

STRIDE is expansion
of the common CIA
threat types

- Confidentiality
- Integrity
- Availability

STRIDE

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Mapping Threats to Asset Types

Threat Type	External Interactor	Process	Data Flow	Data Store
S – Spoofing	Yes	Yes		
T – Tampering		Yes	Yes	Yes
R – Repudiation	Yes	Yes		Yes
I – Information Disclosure		Yes	Yes	Yes
D – Denial of Service		Yes	Yes	Yes
E – Elevation of Privilege		Yes		

So What Does That Leave Us?

Take all the assets

Associate threat types with each asset

Voila! List of things we need to worry about

Countermeasures

- Do nothing
- Remove the feature
- Turn off the feature
- Warn the user
- Counter the threat with Operations
 - Accountability
 - Separation of Duties
- Counter the threat with Technology
 - Change in Design
 - Change in Implementation
- There is no “catch all” countermeasure

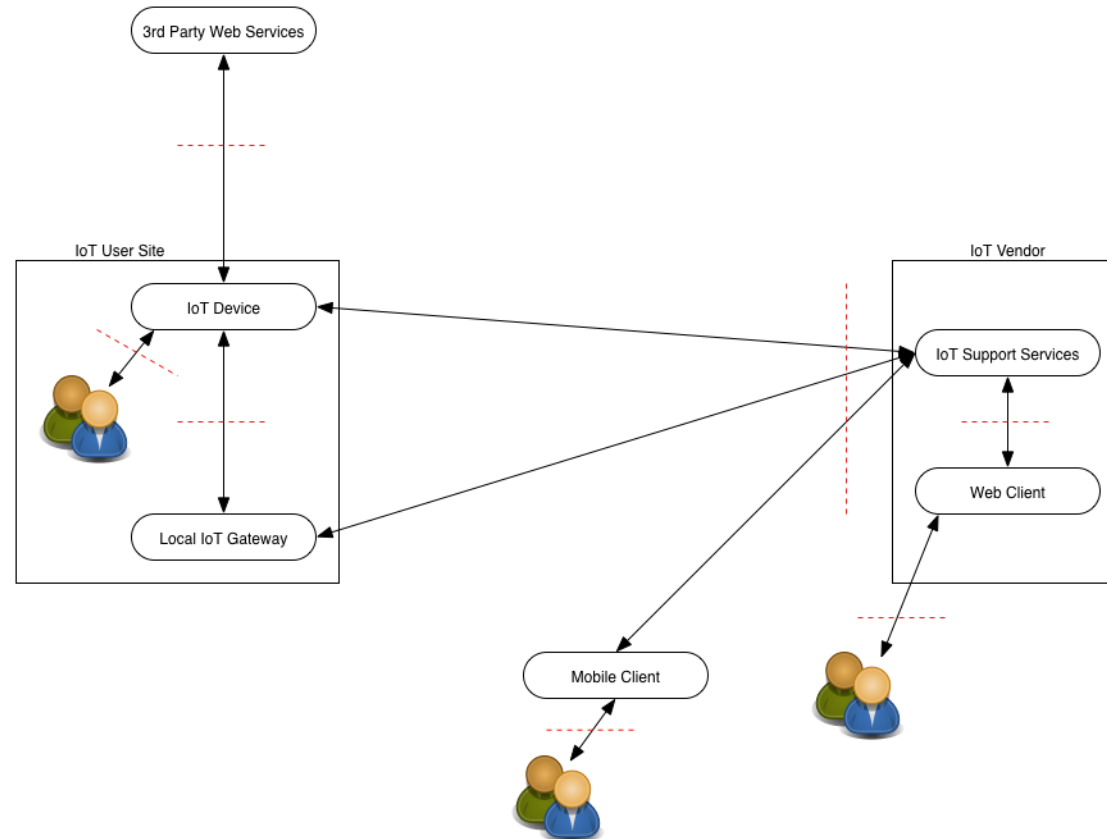
IoT Threat Modeling Particulars



Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

Example Consumer IoT Threat Model



Use Cases to Watch

- “Weird” interfaces
- Initial provisioning and deployment
- Configuration updates
- Software updates
- Integration into enterprise AuthX infrastructure

Using Threat Models to Scope Assessments

- IoT systems have many different parts and kinds of parts
 - Web applications, web services, custom hardware, esoteric protocols
- Creating a test plan can be challenging - you will never have the resources to be exhaustive
- Threat modeling can help drive decisions about trade-offs
- “Should I fuzz-test the device Zigby stack or run SAST on the web services“

Safety Concerns

- Confidentiality, Integrity, and Availability
- Everywhere else: Confidentiality breaches of regulated information
- IoT (especially industrial): Integrity or availability breaches impacting the kinetic environment

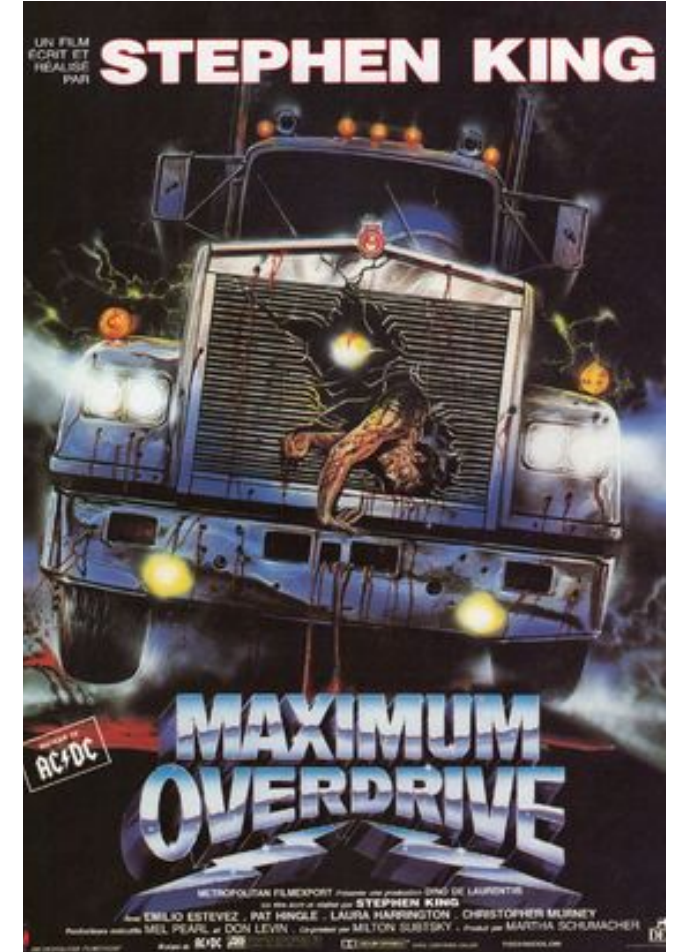
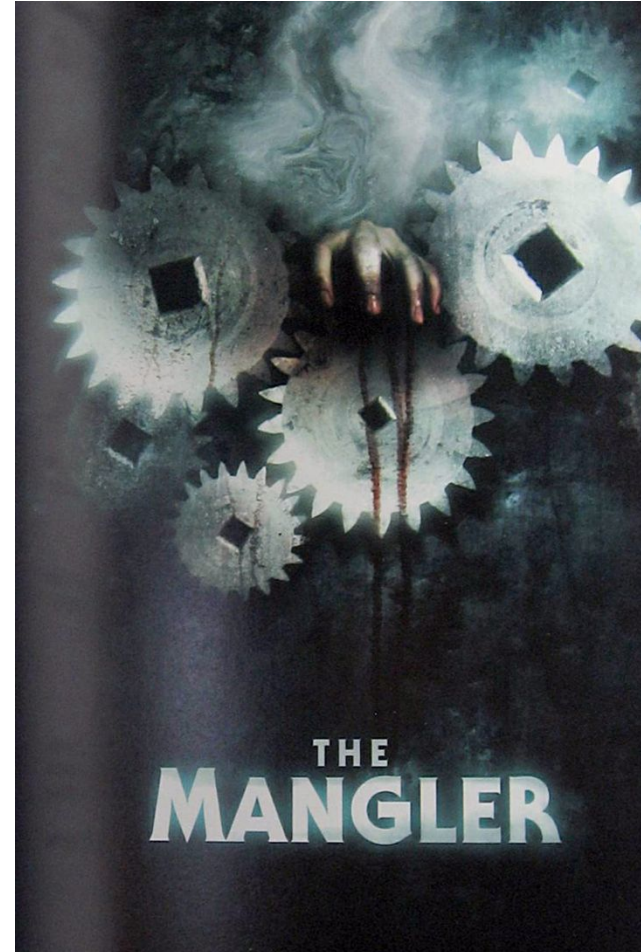


OWASP
AppSec Europe
London 2nd-6th June 2018

Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

What Could Possibly Go Wrong?





Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

Medical Device Risks

- <https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/>
- https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf
- <https://www.cso.com.au/slideshow/397747/10-scariest-hacks-from-black-hat-defcon/>



Safety Concerns with IoT

- Materials from Joshua Corman and We Are the Cavalry
 - <https://www.iamthecavalry.org/5star/>
 - <https://www.iamthecavalry.org/oath/>
 - <https://www.iamthecavalry.org/iotdifferences>
 - <https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things>

An Encouraging Trend

- arm – Platform Security Architecture (PSA)

arm



Asset Tracker TMSA



Smart Water Meter TMSA



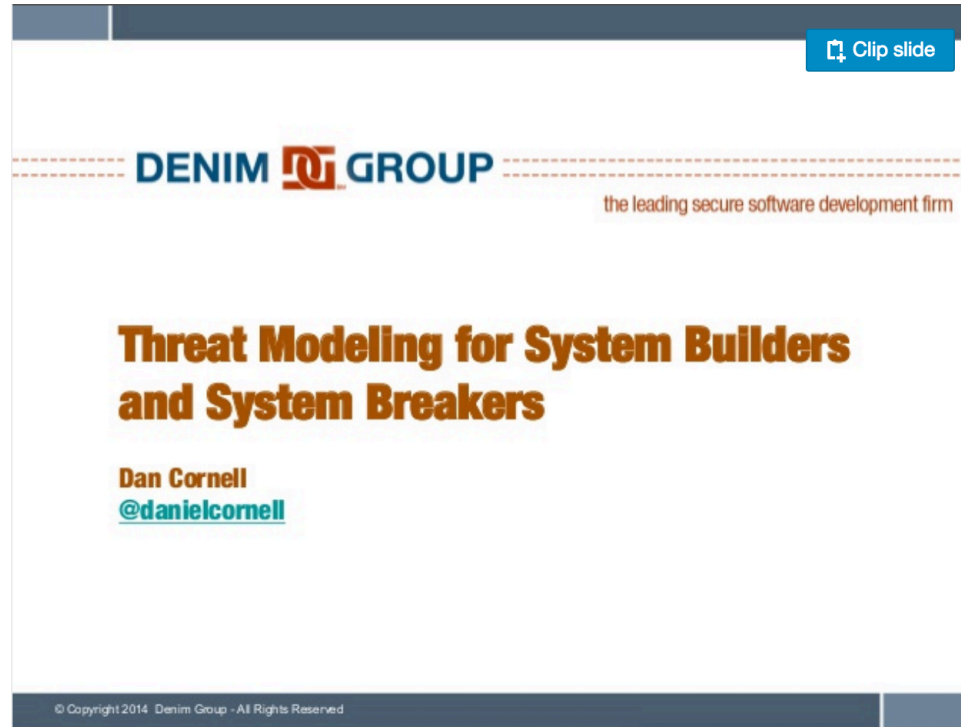
Network Camera TMSA

- <https://pages.arm.com/psa-resources.html>

Threat Modeling for IoT Systems

Dan Cornell, Denim Group CTO

More Threat Modeling Materials



Clip slide

DENIM GROUP
the leading secure software development firm

**Threat Modeling for System Builders
and System Breakers**

Dan Cornell
[@danielcornell](#)

© Copyright 2014 Denim Group - All Rights Reserved

<https://www.slideshare.net/denimgroup/threat-modeling-for-system-builders-and-system-breakers-contentv21>

Closing Thoughts

- IoT systems are varied and complicated
 - And will increasingly have safety implications
- Threat modeling is a valuable technique for
 - Avoiding introducing vulnerabilities
 - Structuring assessments to find vulnerabilities
- If you are building or considering deploying significant IoT systems – save yourself a lot of headaches and use threat modeling



DENIM GROUP

Questions?

Dan Cornell

dan@denimgroup.com

[@danielcornell](#)

denimgroup.com

threadfix.it