OWASP AppSec Europe
London 2nd-6th July 2018

Deconstructing Threat Modelling

Ciaran Conliffe

Deconstructing Threat

Ciaran Conliffe

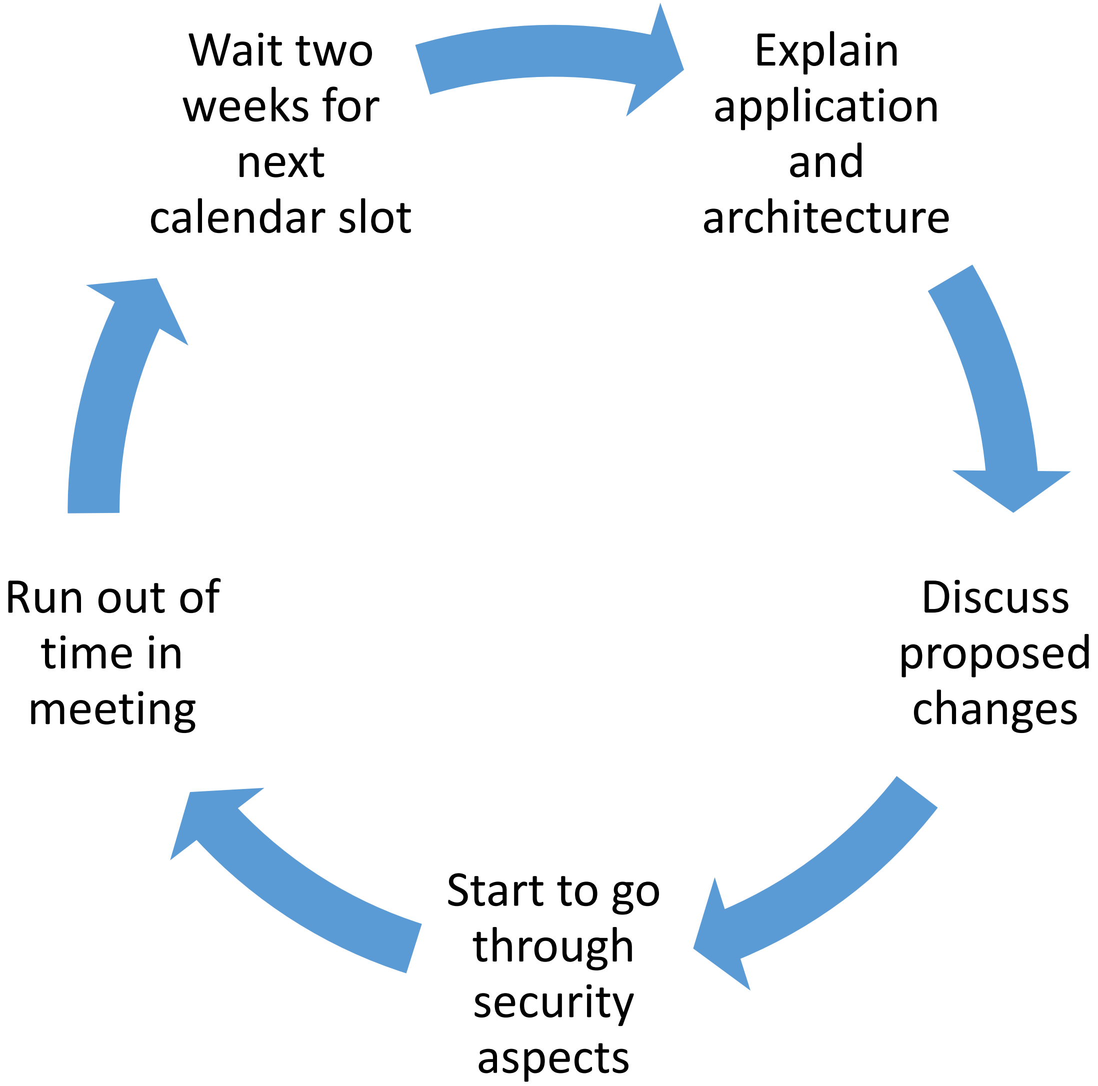
- Technologist and engineer
- Focus on software solutions to security problems
- Fascinated with history and the deep causes of events

Liberty™ Information Technology

- Develop specialist and enterprise scale applications for Liberty Mutual.
- Based in Belfast and Dublin
- Design and implement innovative solutions using both existing and emerging technologies.

Deconstructing Threat Modelling

Ciaran Conliffe



Wait two weeks for next calendar slot

Explain application and architecture

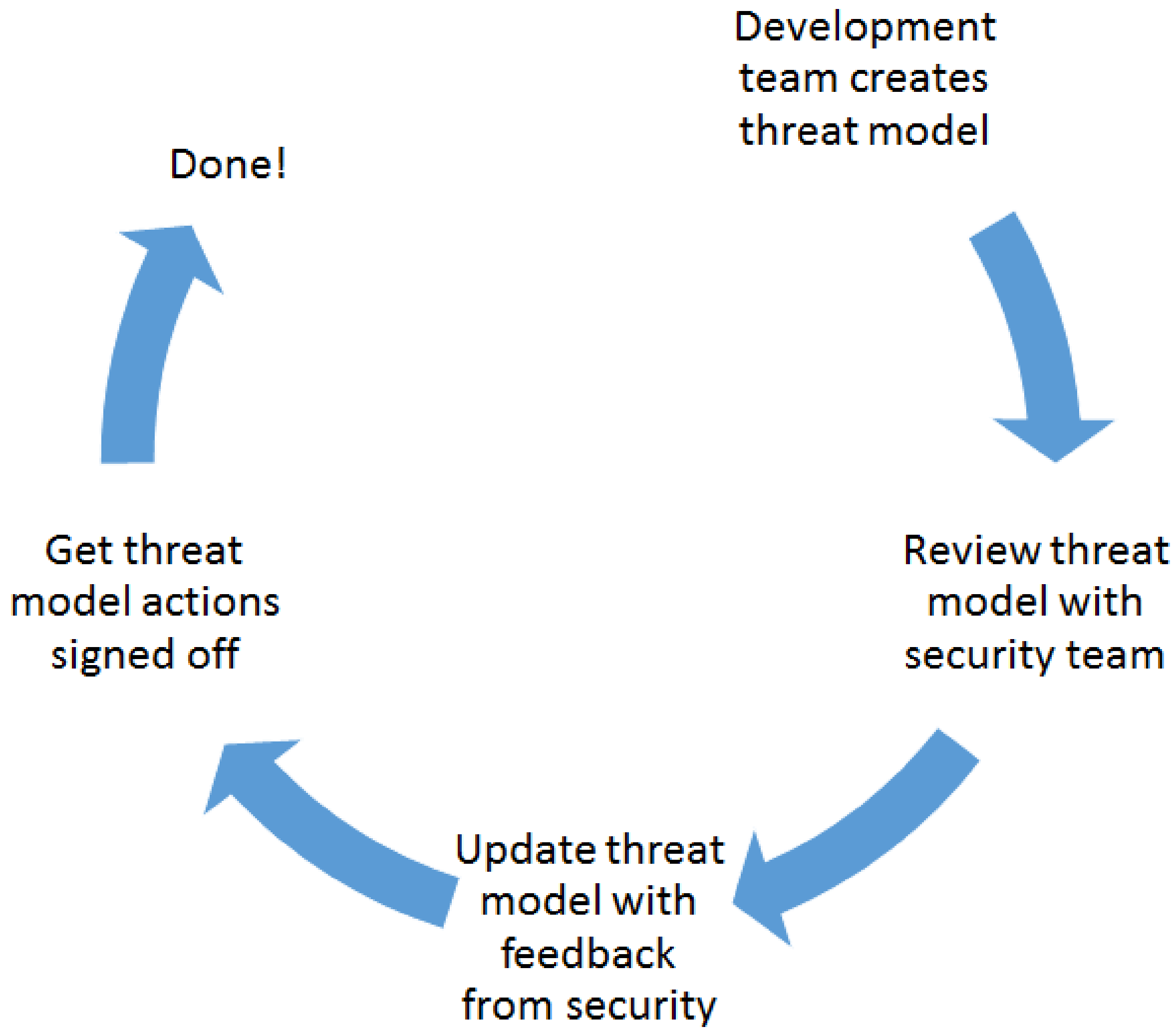
Discuss proposed changes

Start to go through security aspects

Run out of time in meeting

Deconstructing Threat Modelling

Ciaran Conliffe



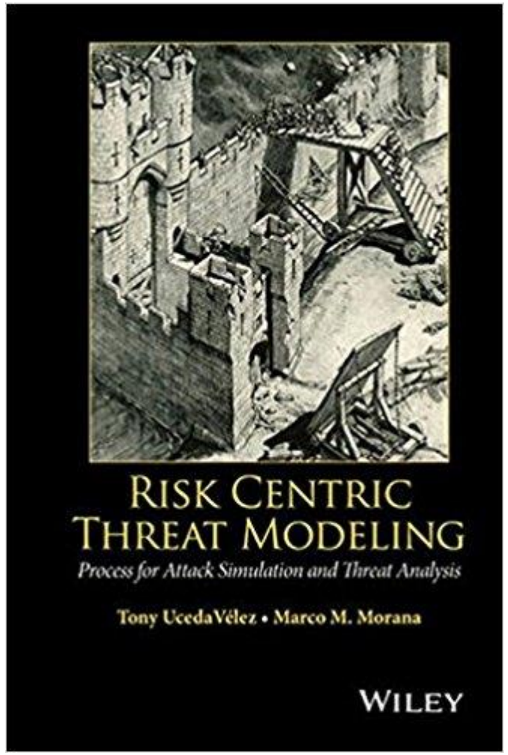
Development team creates threat model

Review threat model with security team

Update threat model with feedback from security

Get threat model actions signed off

Done!

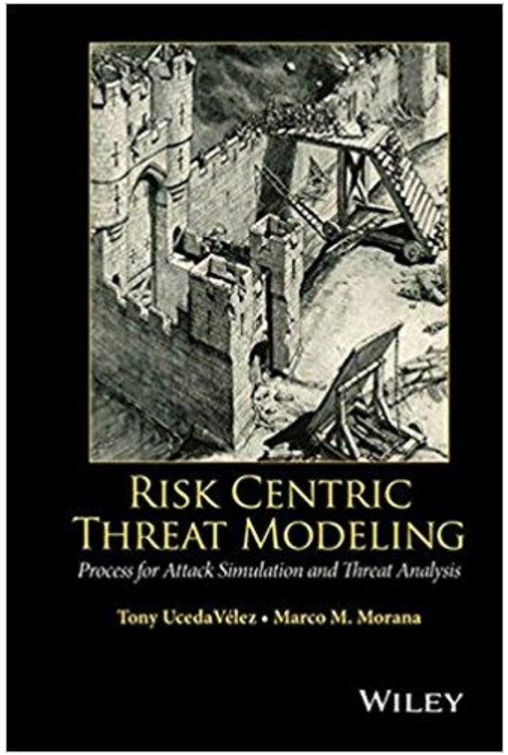


RISK CENTRIC THREAT MODELING

Process for Attack Simulation and Threat Analysis

Tony UcedaVélez • Marco M. Morana

WILEY



RISK CENTRIC
THREAT MODELING

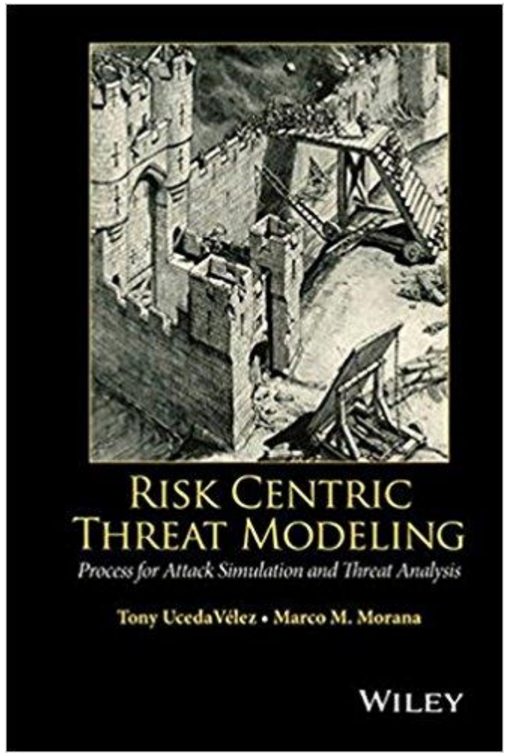
Process for Attack Simulation and Threat Analysis

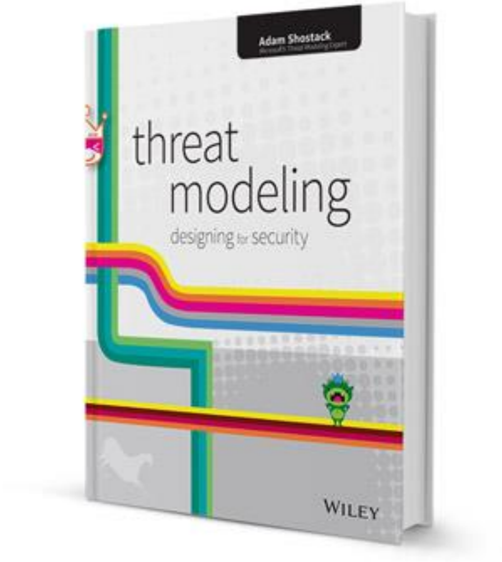
Tony UcedaVélez • Marco M. Morana

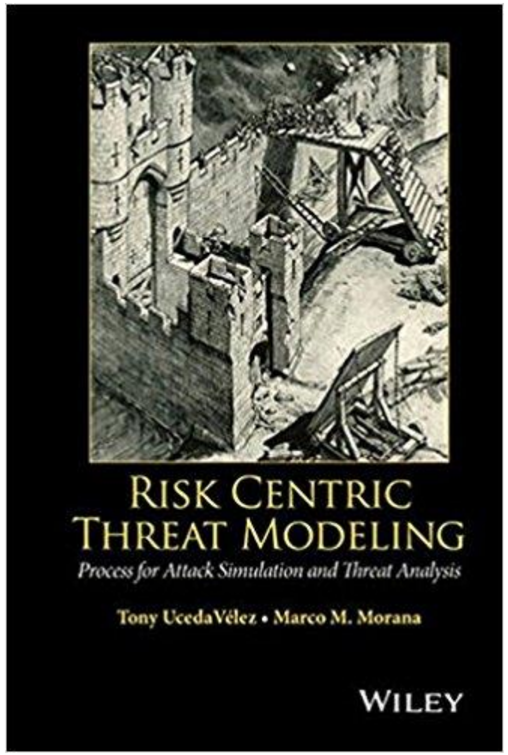
WILEY

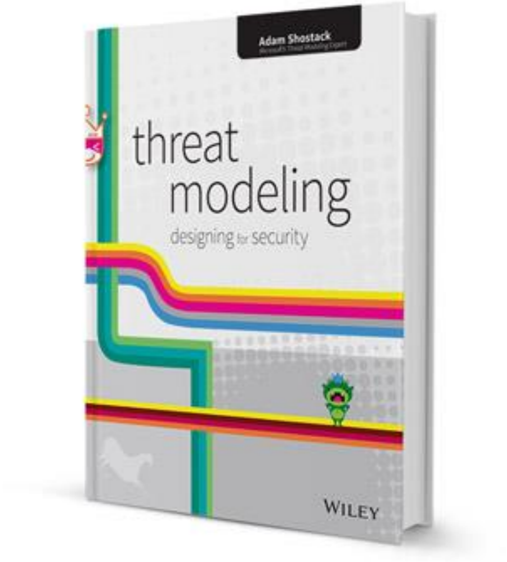
Deconstructing Threat Modelling

Ciaran Conliffe


RISK CENTRIC
THREAT MODELING
Process for Attack Simulation and Threat Analysis
Tony UcedaVélez • Marco M. Morana
WILEY



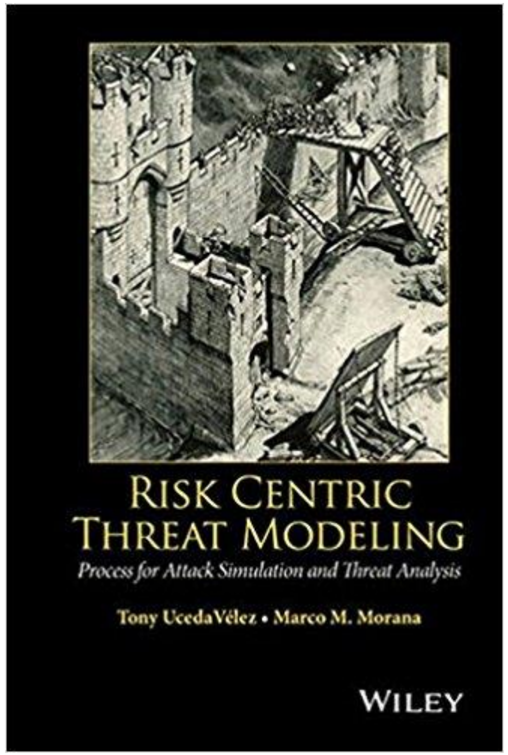

RISK CENTRIC THREAT MODELING
Process for Attack Simulation and Threat Analysis
Tony UcedaVélez • Marco M. Morana
WILEY


Adam Shostack
threat modeling
designing for security
WILEY

µCon
THE MICROSERVICES CONFERENCE
7-8 NOV 2016

Deconstructing Threat Modelling

Ciaran Conliffe

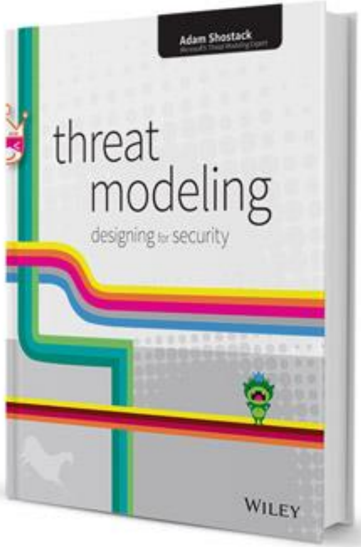


RISK CENTRIC THREAT MODELING

Process for Attack Simulation and Threat Analysis

Tony UcedaVélez • Marco M. Morana

WILEY



Adam Shostack

threat modeling

designing for security

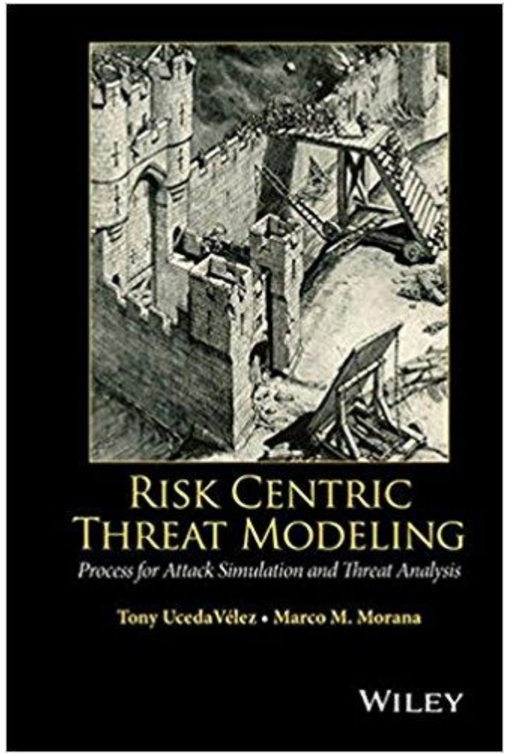
WILEY

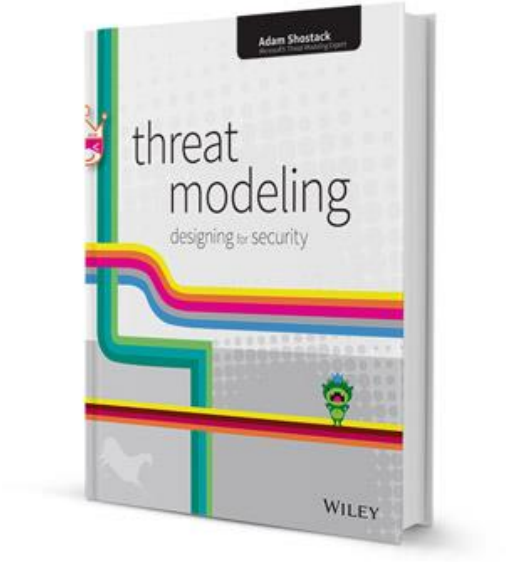
DevSecCon

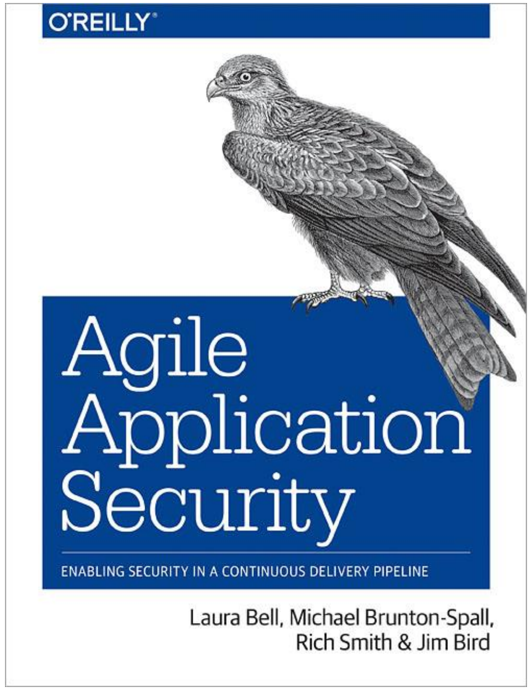
OWASP
AppSec Europe
London 2nd-6th July 2018

Deconstructing Threat Modelling

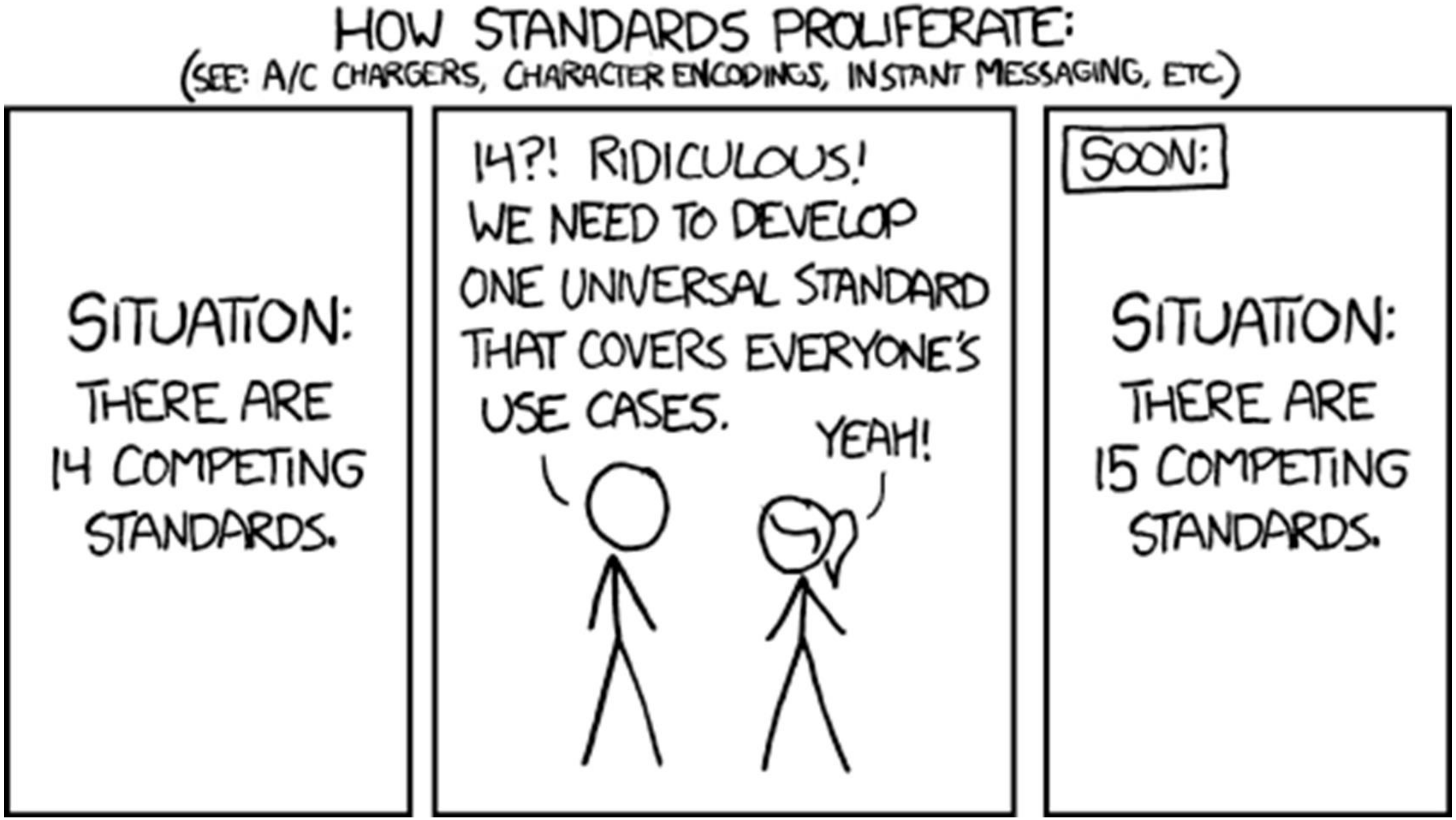
Ciaran Conliffe


RISK CENTRIC THREAT MODELING
Process for Attack Simulation and Threat Analysis
Tony UcedaVélez • Marco M. Morana
WILEY


Adam Shostack
threat modeling
designing for security
WILEY

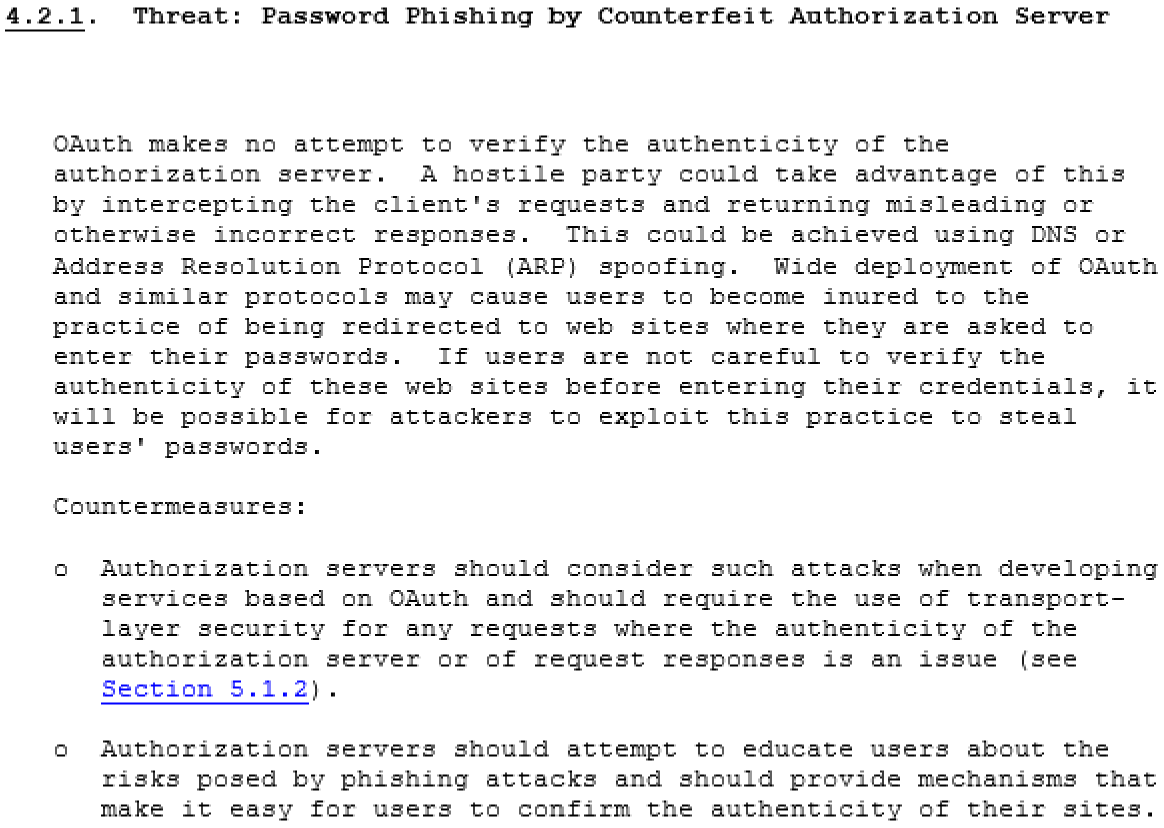

O'REILLY
Agile Application Security
ENABLING SECURITY IN A CONTINUOUS DELIVERY PIPELINE
Laura Bell, Michael Brunton-Spall, Rich Smith & Jim Bird

DevSecCon


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Eureka!

The IETF OAuth Threat Model



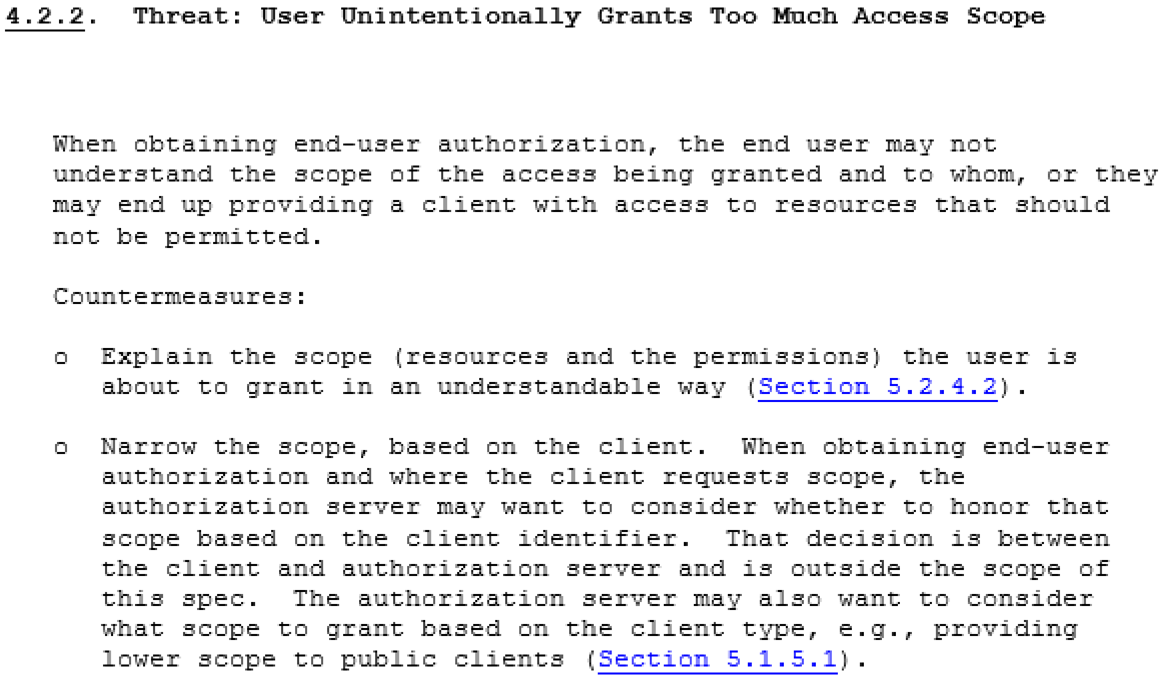
4.2.1. Threat: Password Phishing by Counterfeit Authorization Server

OAuth makes no attempt to verify the authenticity of the authorization server. A hostile party could take advantage of this by intercepting the client's requests and returning misleading or otherwise incorrect responses. This could be achieved using DNS or Address Resolution Protocol (ARP) spoofing. Wide deployment of OAuth and similar protocols may cause users to become inured to the practice of being redirected to web sites where they are asked to enter their passwords. If users are not careful to verify the authenticity of these web sites before entering their credentials, it will be possible for attackers to exploit this practice to steal users' passwords.

Countermeasures:

o Authorization servers should consider such attacks when developing services based on OAuth and should require the use of transport-layer security for any requests where the authenticity of the authorization server or of request responses is an issue (see Section 5.1.2).

o Authorization servers should attempt to educate users about the risks posed by phishing attacks and should provide mechanisms that make it easy for users to confirm the authenticity of their sites.



4.2.2. Threat: User Unintentionally Grants Too Much Access Scope

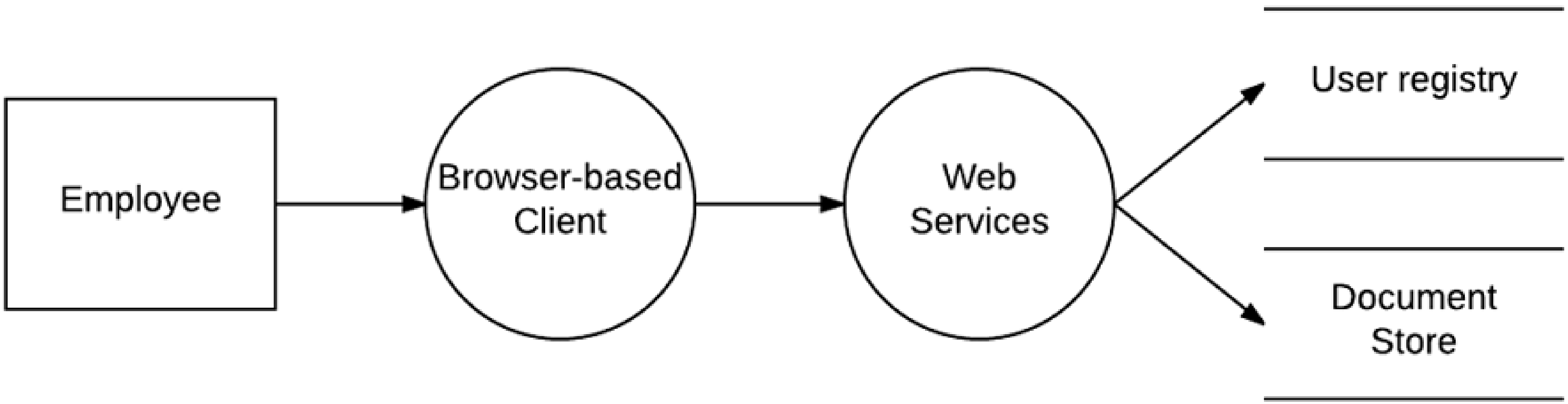
When obtaining end-user authorization, the end user may not understand the scope of the access being granted and to whom, or they may end up providing a client with access to resources that should not be permitted.

Countermeasures:

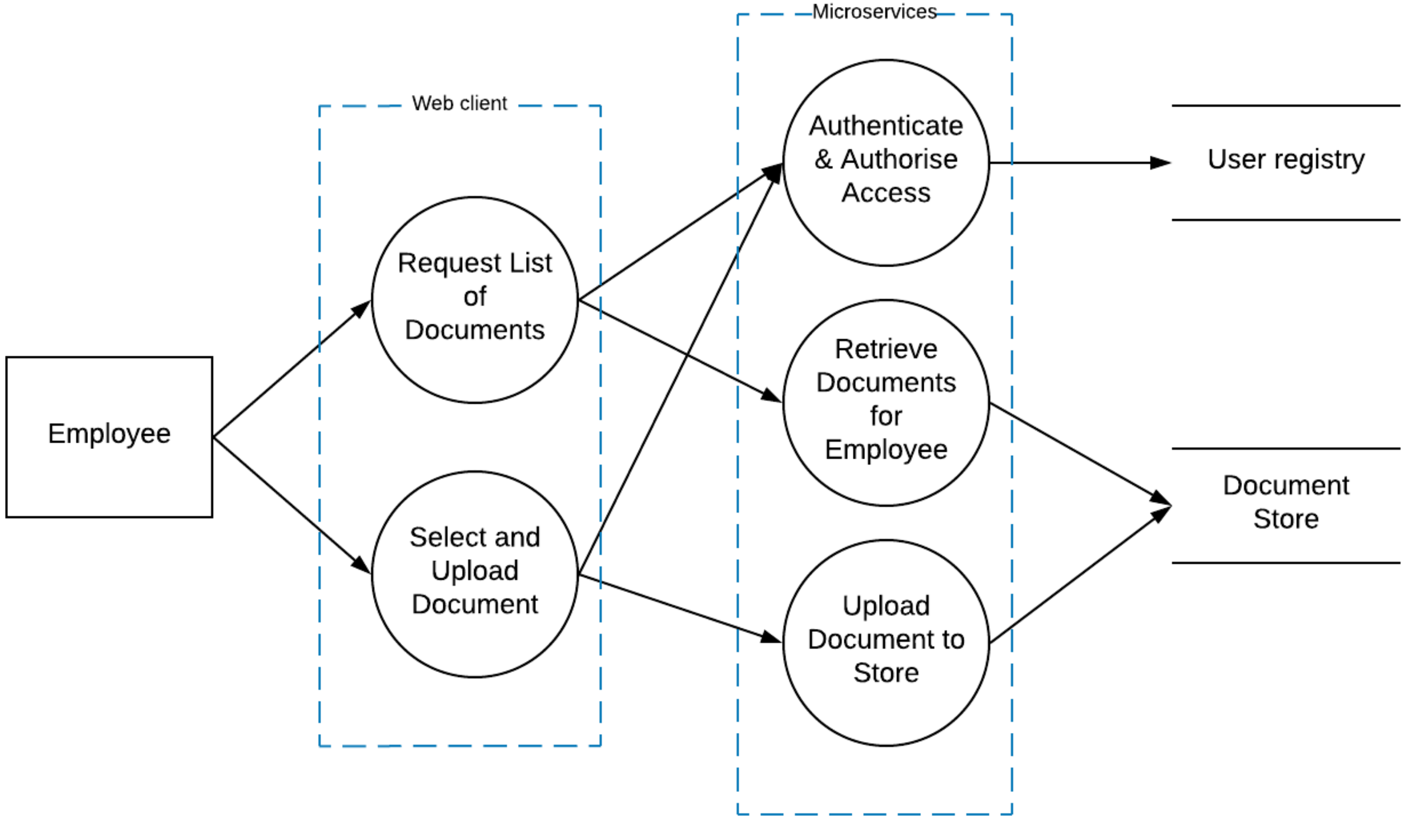
o Explain the scope (resources and the permissions) the user is about to grant in an understandable way (Section 5.2.4.2).

o Narrow the scope, based on the client. When obtaining end-user authorization and where the client requests scope, the authorization server may want to consider whether to honor that scope based on the client identifier. That decision is between the client and authorization server and is outside the scope of this spec. The authorization server may also want to consider what scope to grant based on the client type, e.g., providing lower scope to public clients (Section 5.1.5.1).

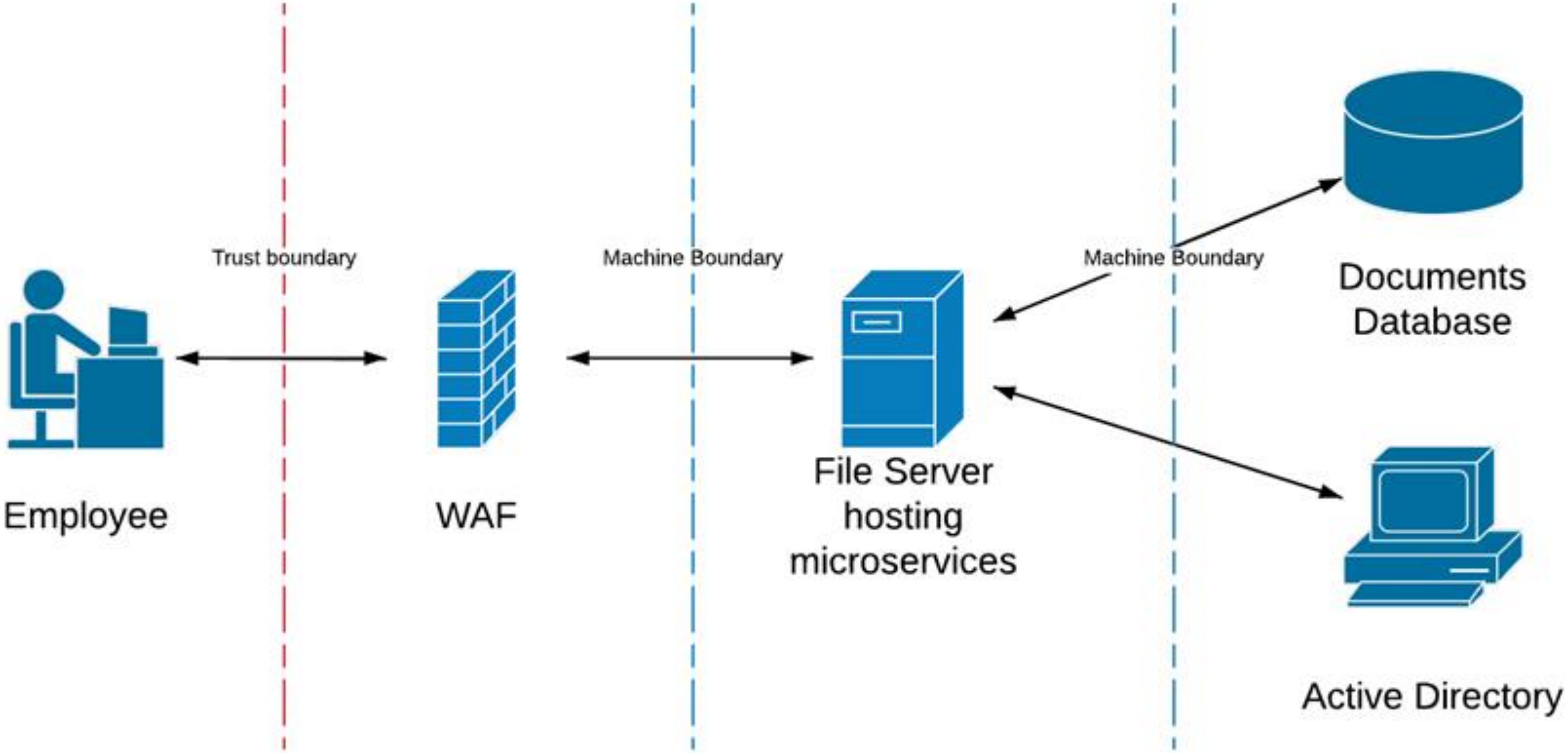
Component-based Data Flow Diagrams



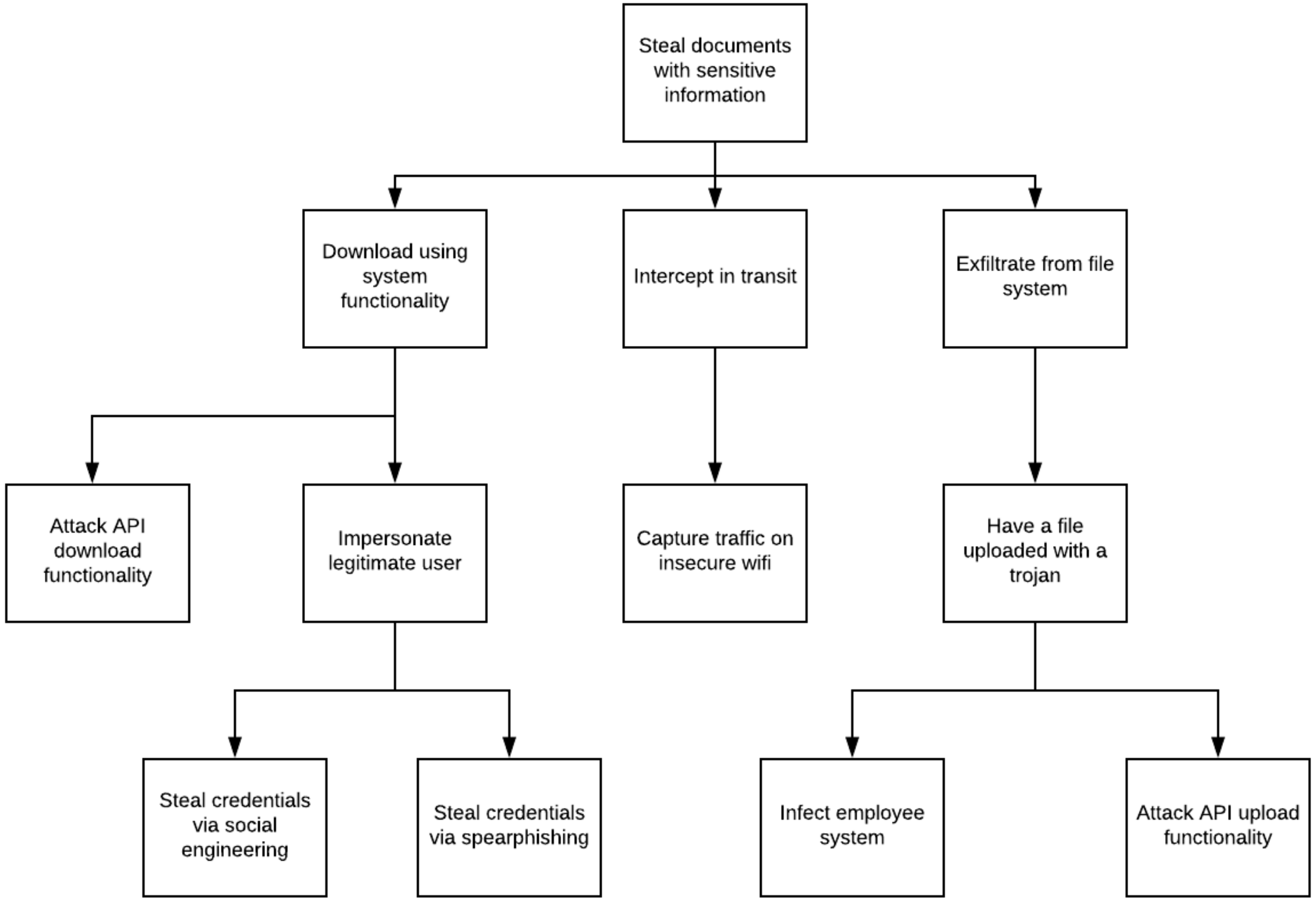
Process-based Data Flow Diagrams


Microservices
Web client
Employee
Request List of Documents
Select and Upload Document
Authenticate & Authorise Access
Retrieve Documents for Employee
Upload Document to Store
User registry
Document Store

Architecture Diagrams with Trust Boundaries



Attack Trees



Steal documents with sensitive information

Download using system functionality

Intercept in transit

Exfiltrate from file system

Attack API download functionality

Impersonate legitimate user

Capture traffic on insecure wifi

Have a file uploaded with a trojan

Steal credentials via social engineering

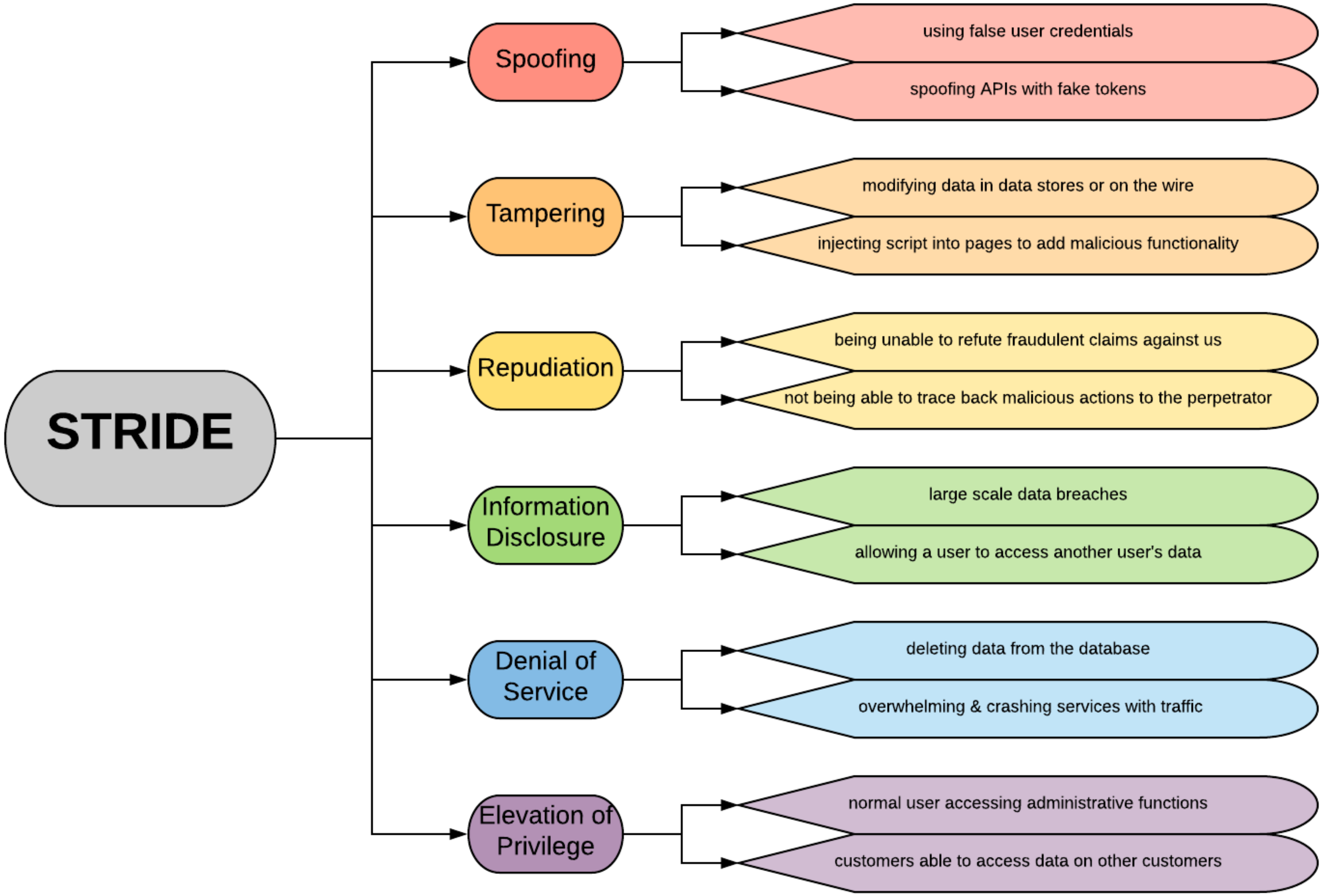
Steal credentials via spearphishing

Infect employee system

Attack API upload functionality

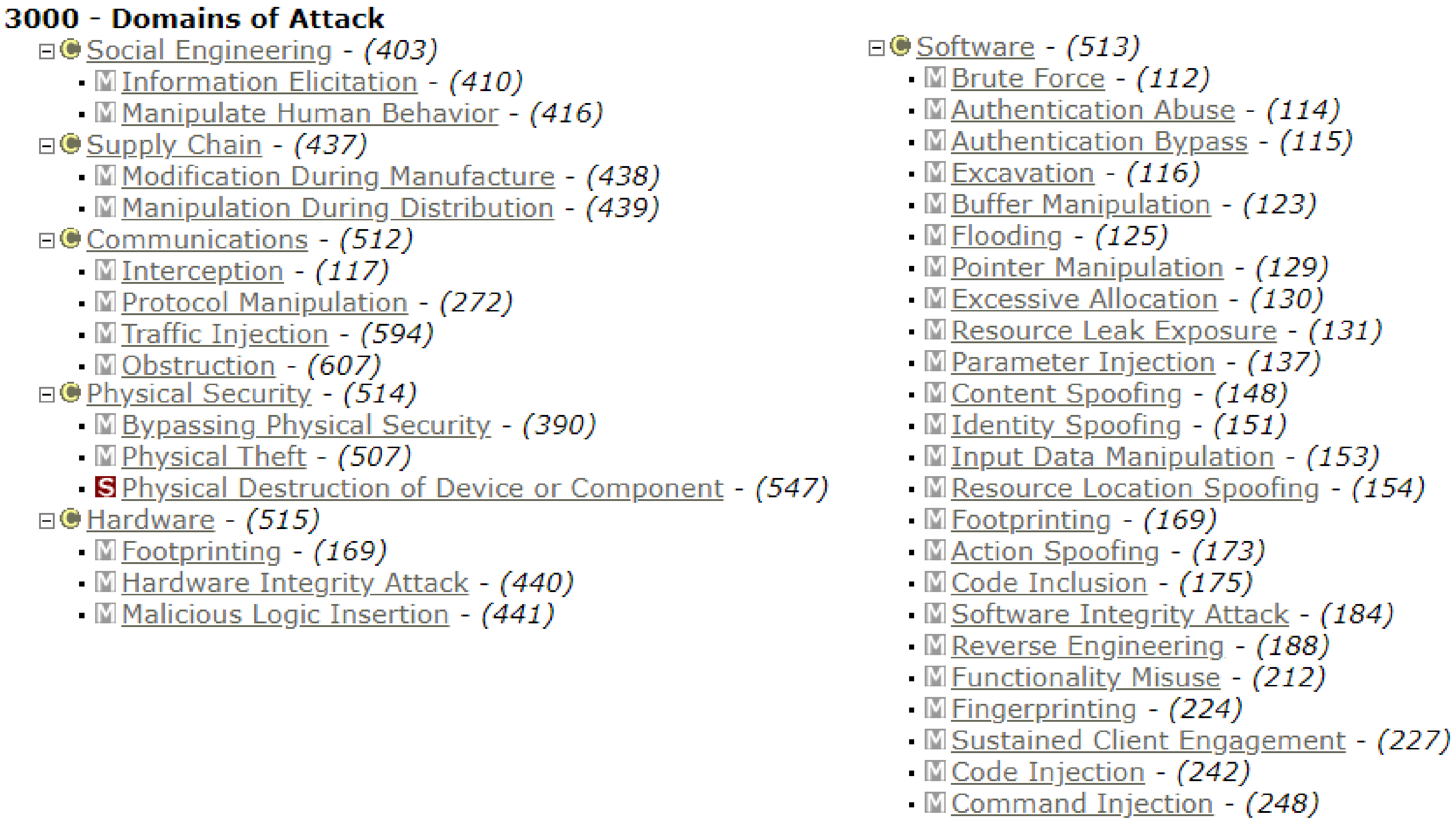
Deconstructing Threat

Ciaran Conliffe



STRIDE
Spoofing
using false user credentials
spoofing APIs with fake tokens
Tampering
modifying data in data stores or on the wire
injecting script into pages to add malicious functionality
Repudiation
being unable to refute fraudulent claims against us
not being able to trace back malicious actions to the perpetrator
Information Disclosure
large scale data breaches
allowing a user to access another user's data
Denial of Service
deleting data from the database
overwhelming & crashing services with traffic
Elevation of Privilege
normal user accessing administrative functions
customers able to access data on other customers

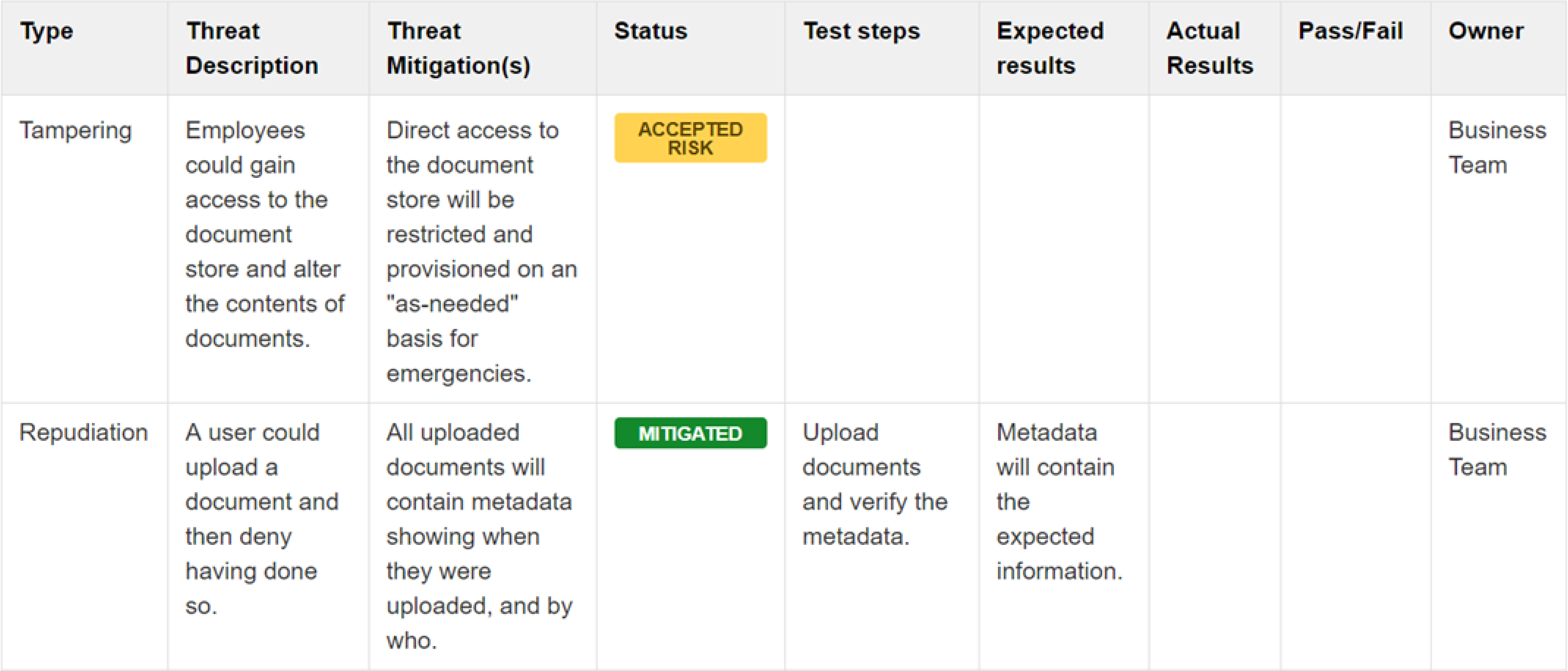
CAPEC



3000 - Domains of Attack

- ⊟ Social Engineering - *(403)*
  - M Information Elicitation - *(410)*
  - M Manipulate Human Behavior - *(416)*
- ⊟ Supply Chain - *(437)*
  - M Modification During Manufacture - *(438)*
  - M Manipulation During Distribution - *(439)*
- ⊟ Communications - *(512)*
  - M Interception - *(117)*
  - M Protocol Manipulation - *(272)*
  - M Traffic Injection - *(594)*
  - M Obstruction - *(607)*
- ⊟ Physical Security - *(514)*
  - M Bypassing Physical Security - *(390)*
  - M Physical Theft - *(507)*
  - S Physical Destruction of Device or Component - *(547)*
- ⊟ Hardware - *(515)*
  - M Footprinting - *(169)*
  - M Hardware Integrity Attack - *(440)*
  - M Malicious Logic Insertion - *(441)*
- ⊟ Software - *(513)*
  - M Brute Force - *(112)*
  - M Authentication Abuse - *(114)*
  - M Authentication Bypass - *(115)*
  - M Excavation - *(116)*
  - M Buffer Manipulation - *(123)*
  - M Flooding - *(125)*
  - M Pointer Manipulation - *(129)*
  - M Excessive Allocation - *(130)*
  - M Resource Leak Exposure - *(131)*
  - M Parameter Injection - *(137)*
  - M Content Spoofing - *(148)*
  - M Identity Spoofing - *(151)*
  - M Input Data Manipulation - *(153)*
  - M Resource Location Spoofing - *(154)*
  - M Footprinting - *(169)*
  - M Action Spoofing - *(173)*
  - M Code Inclusion - *(175)*
  - M Software Integrity Attack - *(184)*
  - M Reverse Engineering - *(188)*
  - M Functionality Misuse - *(212)*
  - M Fingerprinting - *(224)*
  - M Sustained Client Engagement - *(227)*
  - M Code Injection - *(242)*
  - M Command Injection - *(248)*

Organizing Threats



Type	Threat Description	Threat Mitigation(s)	Status	Test steps	Expected results	Actual Results	Pass/Fail	Owner
Tampering	Employees could gain access to the document store and alter the contents of documents.	Direct access to the document store will be restricted and provisioned on an "as-needed" basis for emergencies.	ACCEPTED RISK					Business Team
Repudiation	A user could upload a document and then deny having done so.	All uploaded documents will contain metadata showing when they were uploaded, and by who.	MITIGATED	Upload documents and verify the metadata.	Metadata will contain the expected information.			Business Team

Prioritizing Threats

Damage

Reproducibility

Exploitability

Affected users

Discoverability

Prioritizing Threats

Damage
Reproducibility
Exploitability
Affected users
Discoverability

Factor
Analysis of
Information
Risk

Prioritizing Threats

Common

Vulnerability

Scoring

System

Deconstructing Threat

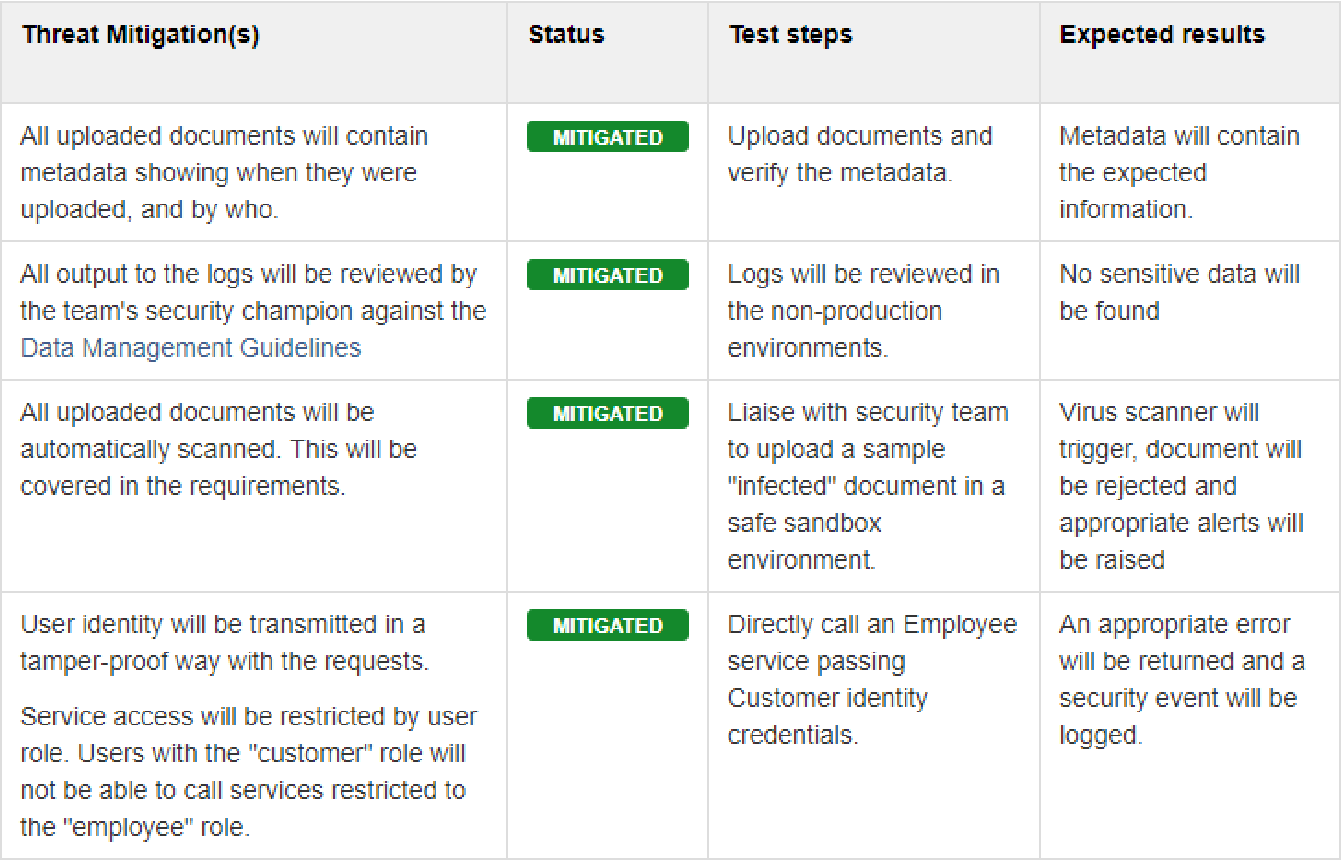
Ciaran Conliffe

Deconstructing Threat

Ciaran Conliffe

EPIC	TO DO	IN PROGRESS	DONE
The Odyssey	Kill Cyclops Return to Ithaca	Persuade Circe to turn pigs back into sailors	Fail to placate Poseidon
Táin Bó Cúailnge	Defeat Cuchullain	Lull Ulstermen into magical slumber	Steal cow

Testing Your Mitigations

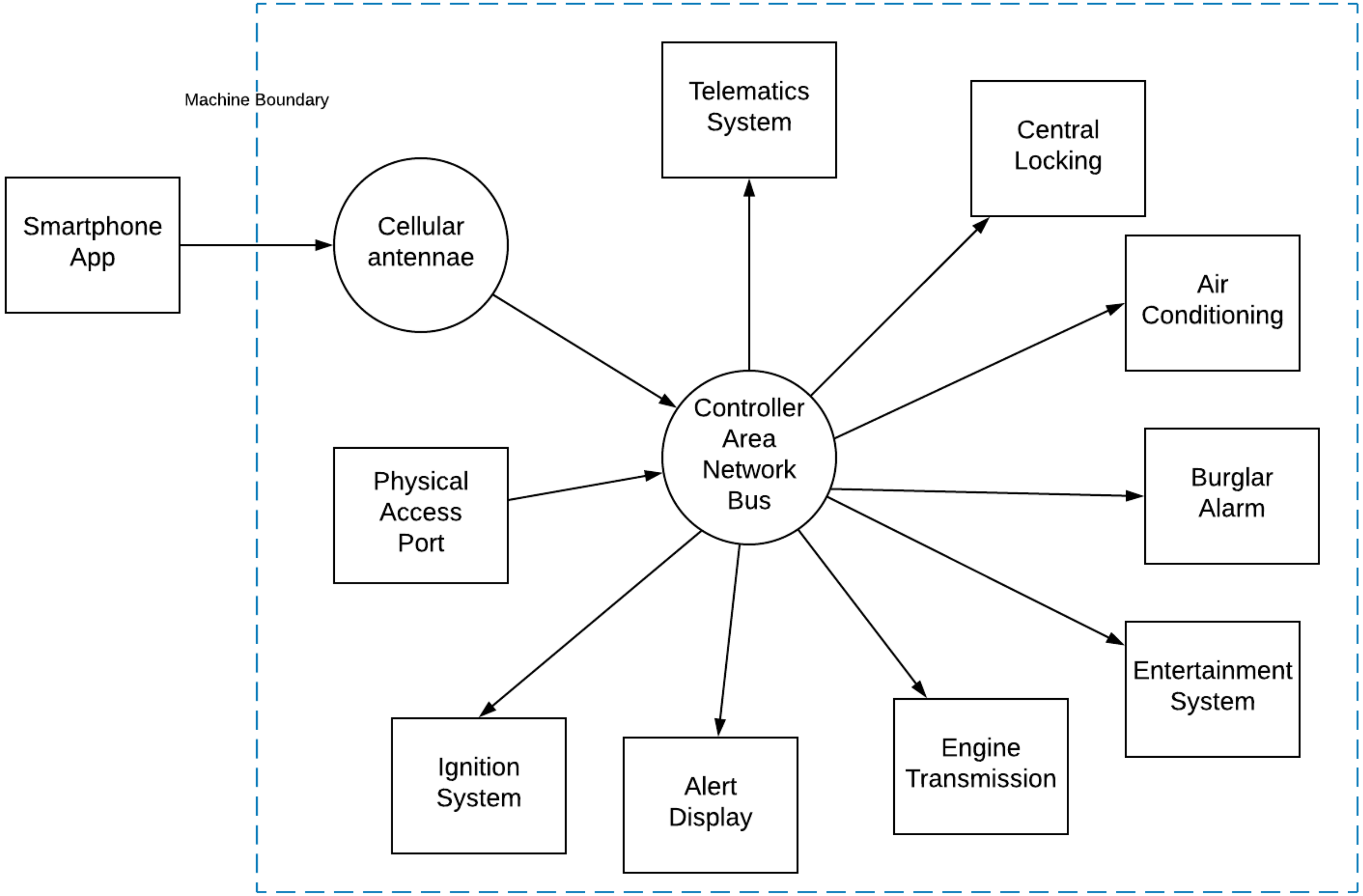


Threat Mitigation(s)	Status	Test steps	Expected results
All uploaded documents will contain metadata showing when they were uploaded, and by who.	MITIGATED	Upload documents and verify the metadata.	Metadata will contain the expected information.
All output to the logs will be reviewed by the team's security champion against the Data Management Guidelines	MITIGATED	Logs will be reviewed in the non-production environments.	No sensitive data will be found
All uploaded documents will be automatically scanned. This will be covered in the requirements.	MITIGATED	Liaise with security team to upload a sample "infected" document in a safe sandbox environment.	Virus scanner will trigger, document will be rejected and appropriate alerts will be raised
User identity will be transmitted in a tamper-proof way with the requests. Service access will be restricted by user role. Users with the "customer" role will not be able to call services restricted to the "employee" role.	MITIGATED	Directly call an Employee service passing Customer identity credentials.	An appropriate error will be returned and a security event will be logged.

Example Time!

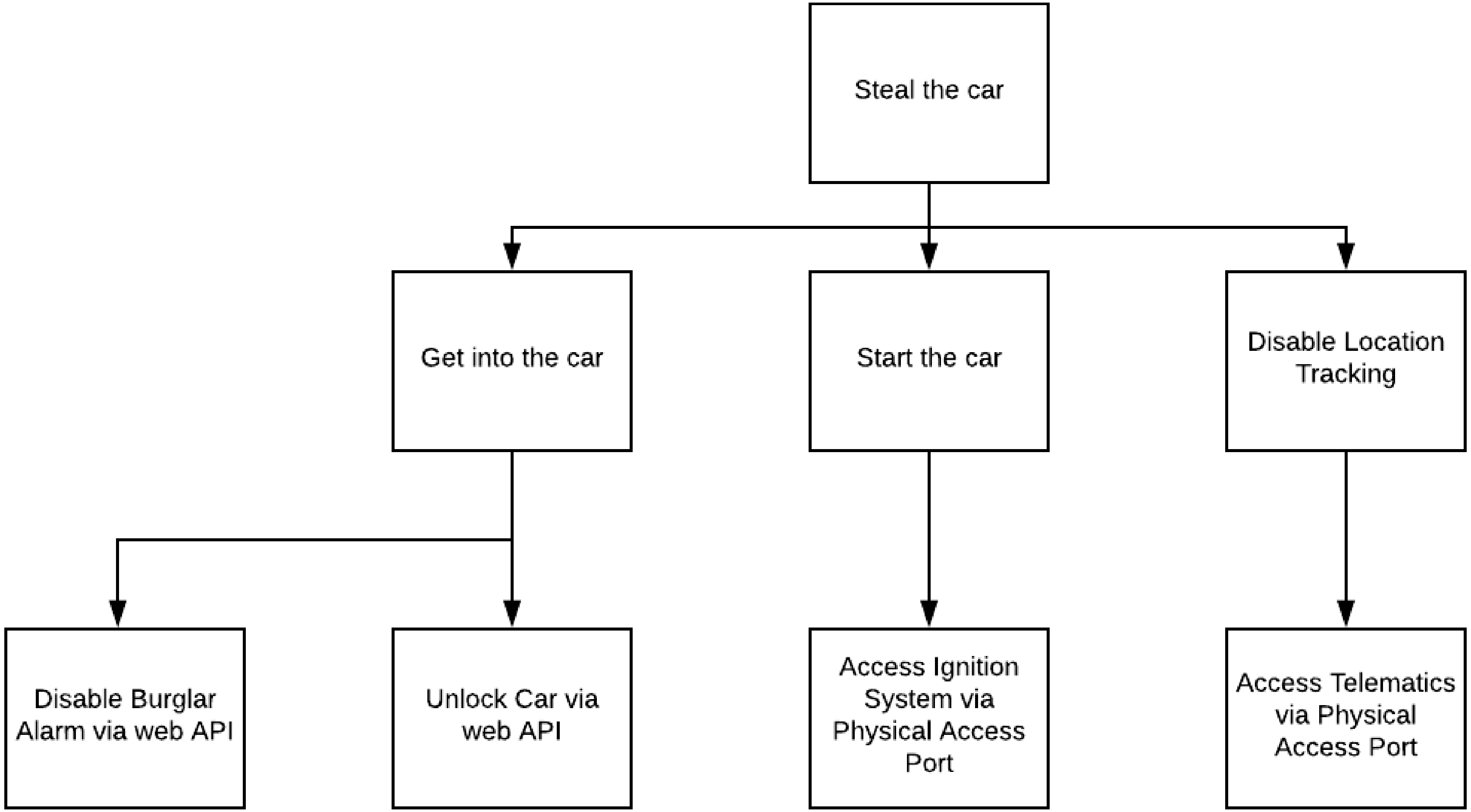
Deconstructing Threat

Ciaran Conliffe



Deconstructing Threat

Ciaran Conliffe



Steal the car

Get into the car

Start the car

Disable Location Tracking

Disable Burglar Alarm via web API

Unlock Car via web API

Access Ignition System via Physical Access Port

Access Telematics via Physical Access Port

List & Prioritize Threats

The physical access port is used to disable the central lo
and start the car without a valid key

- **Exploitability:** Requires physical access
- **Damage:** Theft of car
- **Rating:** Medium

Remote Access is used to turn off the burglar ala
and unlock the car

- **Exploitability:** Exploitable remotely
- **Damage:** Theft of car, theft of contents
- **Rating:** High

Remote Access is used to extract the telematics
information and determine the location of the ca

- **Exploitability:** Exploitable remotely
- **Damage:** Information loss
- **Rating:** Low

Remote Access is used to disable the transmiss
and cut engine power to the wheels during trans

- **Exploitability:** Exploitable remotely
- **Damage:** Loss of life
- **Rating:** Critical

Mitigate & Test Threats

The physical access port is used by an unauthorised person to access core car systems

- **Mitigation:** Individual PIN for each car, only available to authorized repair professionals
- **Test:** Access car port using PIN from another car

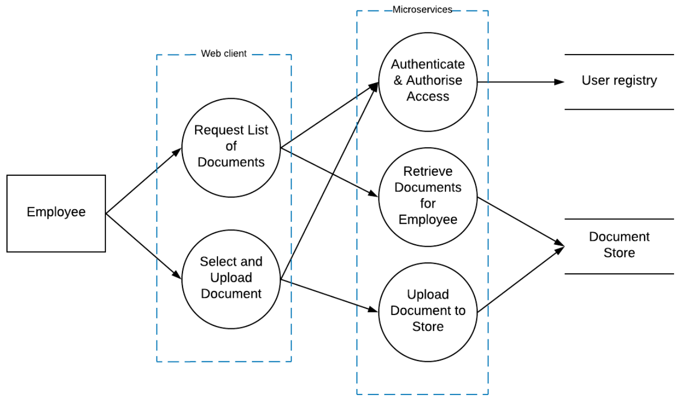
Remote access is used to access critical car systems such as the transmission

- **Mitigation:** Remove ability for remote access to be used on those systems by removing unnecessary functionality from the API & segregating control to physical access only
- **Test:** Audit the API for unnecessary functions

Air conditioning is activated remotely and run overnight in order to drain car batte

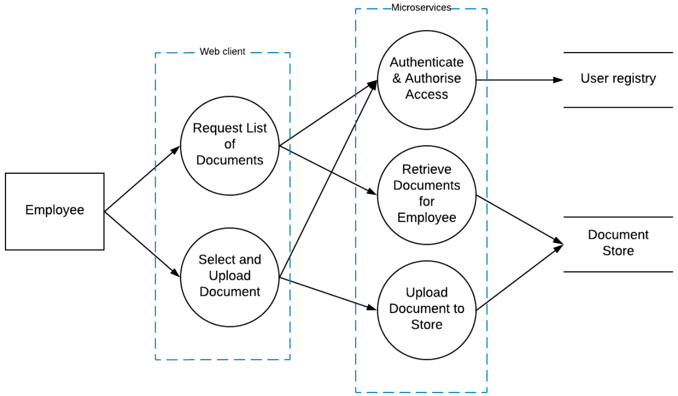
- **Mitigation:** Time-limit aircon activation remotely & disable it when car battery is below 25% charge
- **Test:** Activate aircon remotely and run through scenarios that would drain the battery

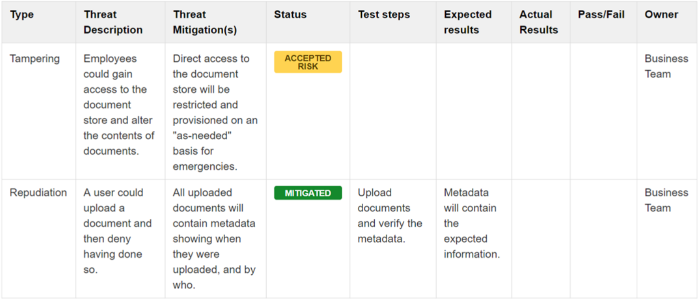
The Deconstructed Threat Model


Web client
Microservices
Employee
Request List of Documents
Select and Upload Document
Authenticate & Authorise Access
Retrieve Documents for Employee
Upload Document to Store
User registry
Document Store

Find Threats

The Deconstructed Threat Model


Web client
Microservices
Employee
Request List of Documents
Select and Upload Document
Authenticate & Authorise Access
Retrieve Documents for Employee
Upload Document to Store
User registry
Document Store

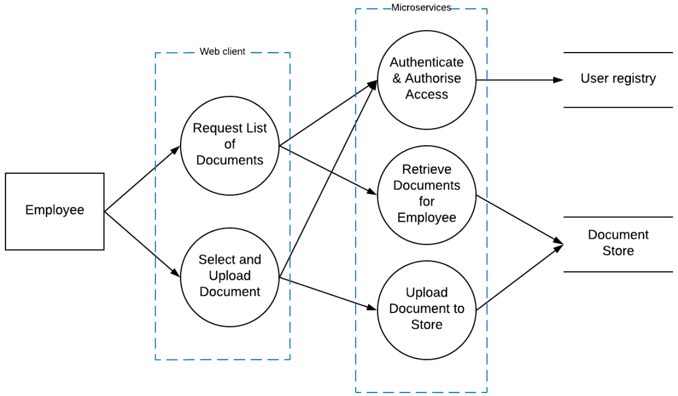


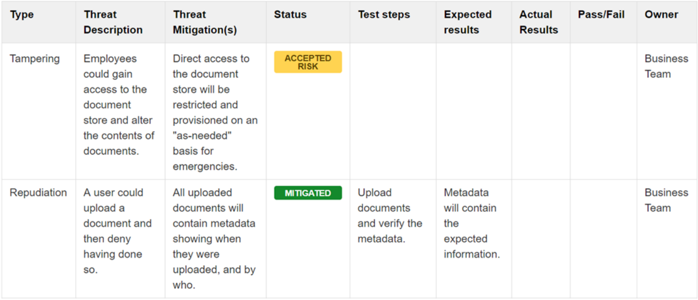
Type	Threat Description	Threat Mitigation(s)	Status	Test steps	Expected results	Actual Results	Pass/Fail	Owner
Tampering	Employees could gain access to the document store and alter the contents of documents.	Direct access to the document store will be restricted and provisioned on an "as-needed" basis for emergencies.	ACCEPTED RISK					Business Team
Repudiation	A user could upload a document and then deny having done so.	All uploaded documents will contain metadata showing when they were uploaded, and by who.	MITIGATED	Upload documents and verify the metadata.	Metadata will contain the expected information.			Business Team

Find Threats

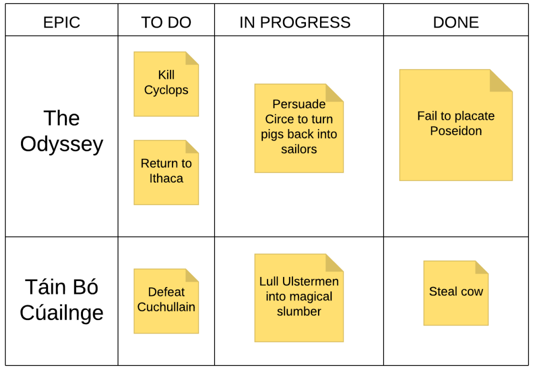
Organize

The Deconstructed Threat Model


Employee
Web client
Request List of Documents
Select and Upload Document
Microservices
Authenticate & Authorise Access
Retrieve Documents for Employee
Upload Document to Store
User registry
Document Store



Type	Threat Description	Threat Mitigation(s)	Status	Test steps	Expected results	Actual Results	Pass/Fail	Owner
Tampering	Employees could gain access to the document store and alter the contents of documents.	Direct access to the document store will be restricted and provisioned on an "as-needed" basis for emergencies.	ACCEPTED RISK					Business Team
Repudiation	A user could upload a document and then deny having done so.	All uploaded documents will contain metadata showing when they were uploaded, and by who.	MITIGATED	Upload documents and verify the metadata.	Metadata will contain the expected information.			Business Team



EPIC	TO DO	IN PROGRESS	DONE
The Odyssey	Kill Cyclops Return to Ithaca	Persuade Circe to turn pigs back into sailors	Fail to placate Poseidon
Táin Bó Cúailnge	Defeat Cuchullain	Lull Ulstermen into magical slumber	Steal cow

Find Threats

Organize

Take Action

Questions?

@shinyemptyhead

liberty-it.co.uk