As a freshly appointed head of security…

Source: https://d12edgf4lwbh8j.cloudfront.net/photo/image/Knighting.gif

What would you do?

Source: https://i.imgflip.com/2cmmww.jpg

Scaling threat models... by playing cards!?

A case study

$ whoami

- Mateusz Niezabitowski (Poland)
- 11 years as Software Developer (mostly Java & Web)
- Started moving towards Application Security 5 years ago
- Application Security Engineer @ Ocado Technology
- Mostly web technologies

In theory, there is no difference between theory and practice.

In practice, there is…

Agenda

1. Why doing Threat Models is a good idea?
2. How did we approached Threat Modeling?
3. What lessons were learnt during the process?

So, what would you do?

So, what would you do?

Source: https://i.giphy.com/media/d2ZjBlsQa5dWO45a/giphy.gif

①

Why doing Threat Models is a good idea?

Don’t be a headless chicken!

Learn the answer to these 3 questions:

1. Why do you want to be “Secure”?

Beware of zealots

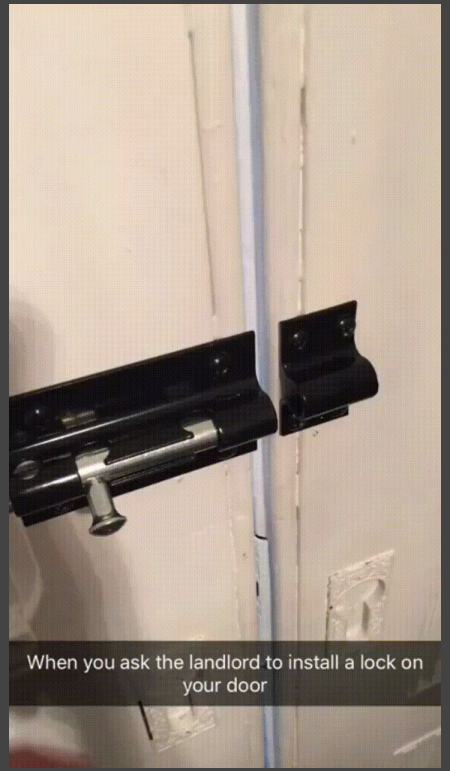
Source: https://pre00.deviantart.net/8eba/th/pre/f/2015/282/5/8/starcraft_ii__legacy_of_the_void_opening_cinematic_by_dimensionaldrift-d9cgntn.jpg

2. What does “Secure” mean in your context?

“Secure” System

Source: https://i.gifer.com/Bl4g.gif

“Secure” System



Source: https://i.imgur.com/oSUaHS7.gif

Security doesn’t have one simple definition.

3. How do you prioritise your work?

Have you talked to Product Owners?

Source: http://jolanamalkston.com/wp-content/uploads/2017/05/Office-Clutter-1.jpg

Have you talked to Developers?

Source: http://www.cutecatgifs.com/wp-content/uploads/2014/02/ctn.gif

You can’t make everything secure overnight!

②

How did we approached Threat Modeling effort?

Fun and engaging

As simple as possible

Adds value

(and you feel it)

“Elevation of Privilege”,

“**Cornucopia**”

approach

Step 0: Draw

Step 1: Collect threats

Step 2: Assess threats

Step 2.1: Quantify risk

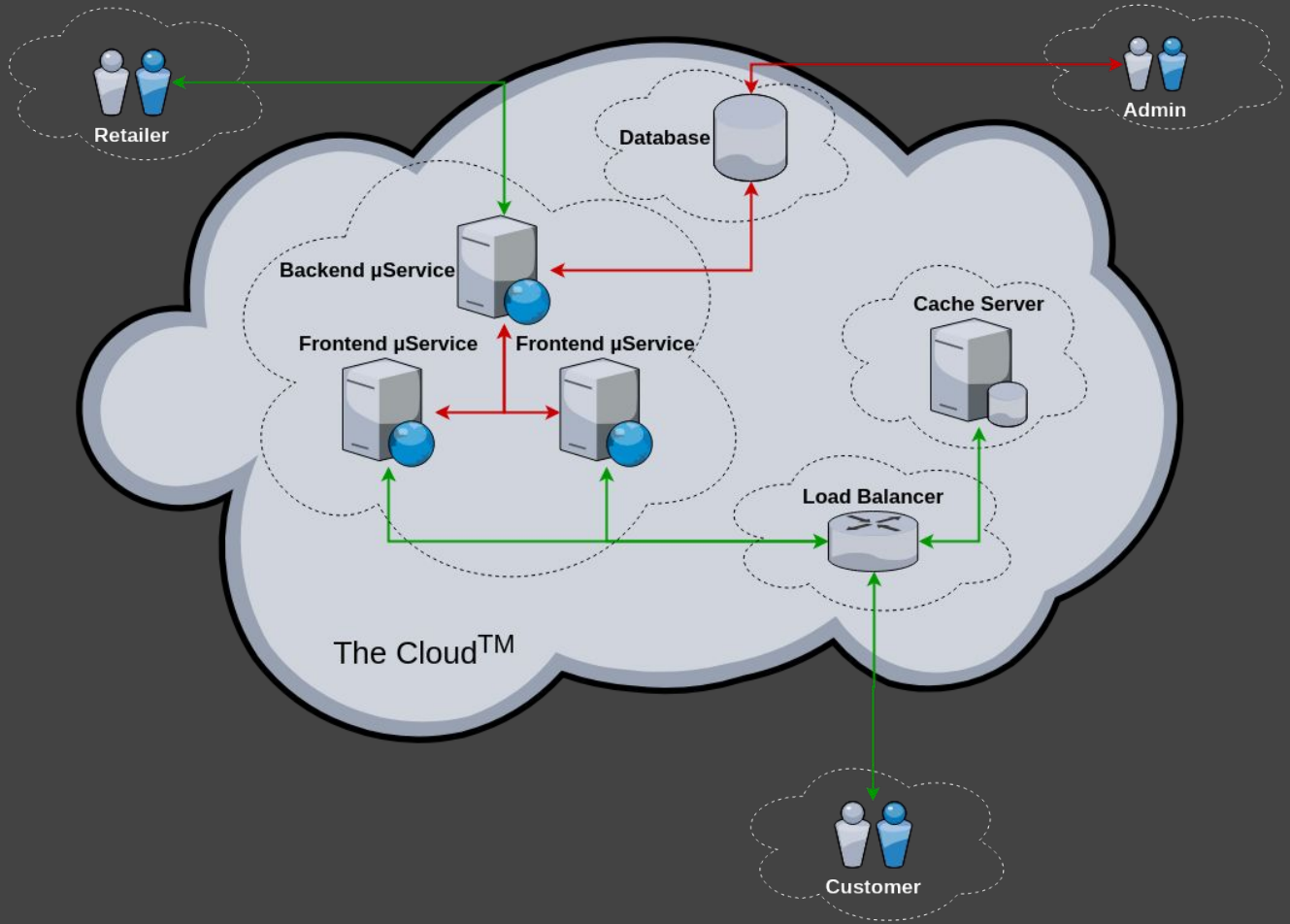
Step 2.2: Assess your situation

Step 2.3: Agree on action(s)

Step (+1): ACT!

General overview

1. Pick a card
2. Quick brainstorming - is this a threat?
3. *Calculate the risk (out of scope)*
4. Propose mitigation(s)
5. … repeat


Retailer
Admin
Database
Backend µService
Frontend µService
Frontend µService
Cache Server
Load Balancer
The Cloud™
Customer

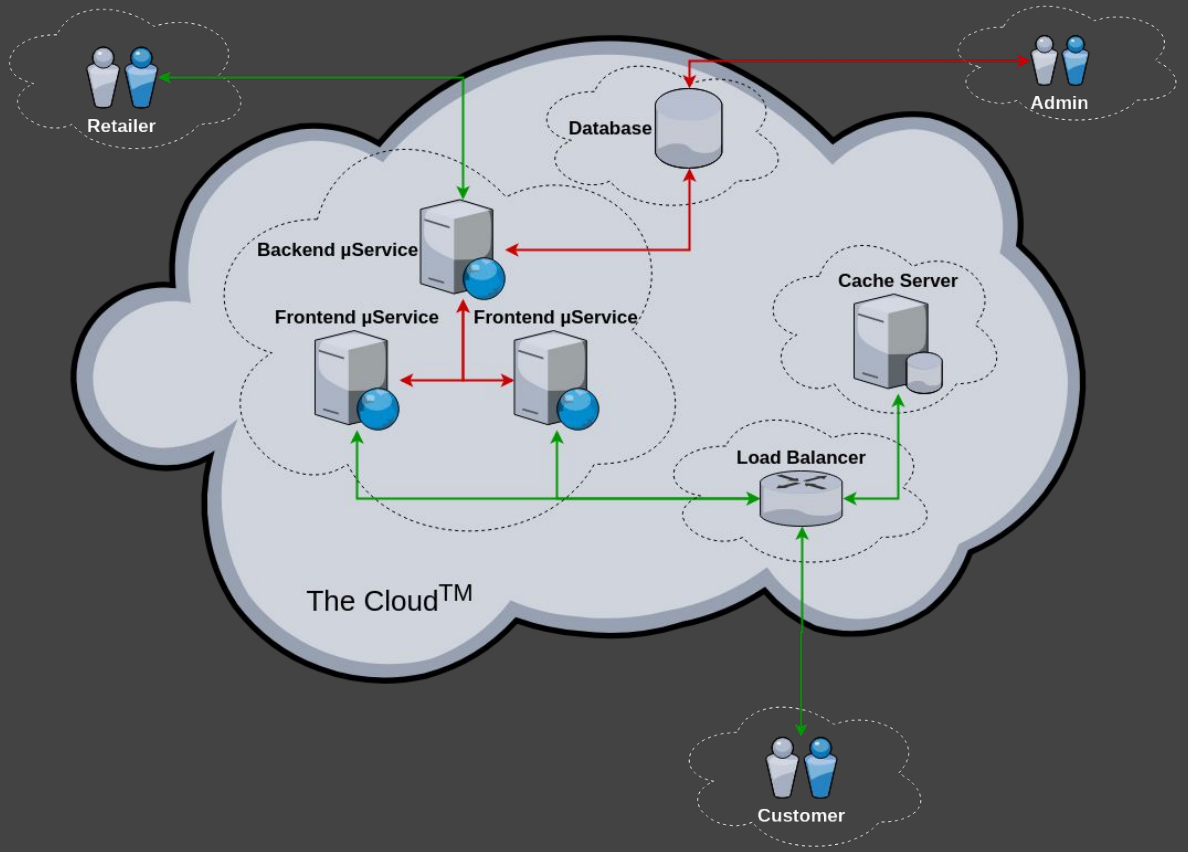
AUTHENTICATION

4

Sebastien can easily identify user names or can enumerate them

OWASP SCP	33, 53
OWASP ASVS	2.18, 2.28
OWASP AppSensor	AE1
CAPEC	383
SAFECODE	28

OWASP Cornucopia Ecommerce Website Edition v1.20-EN



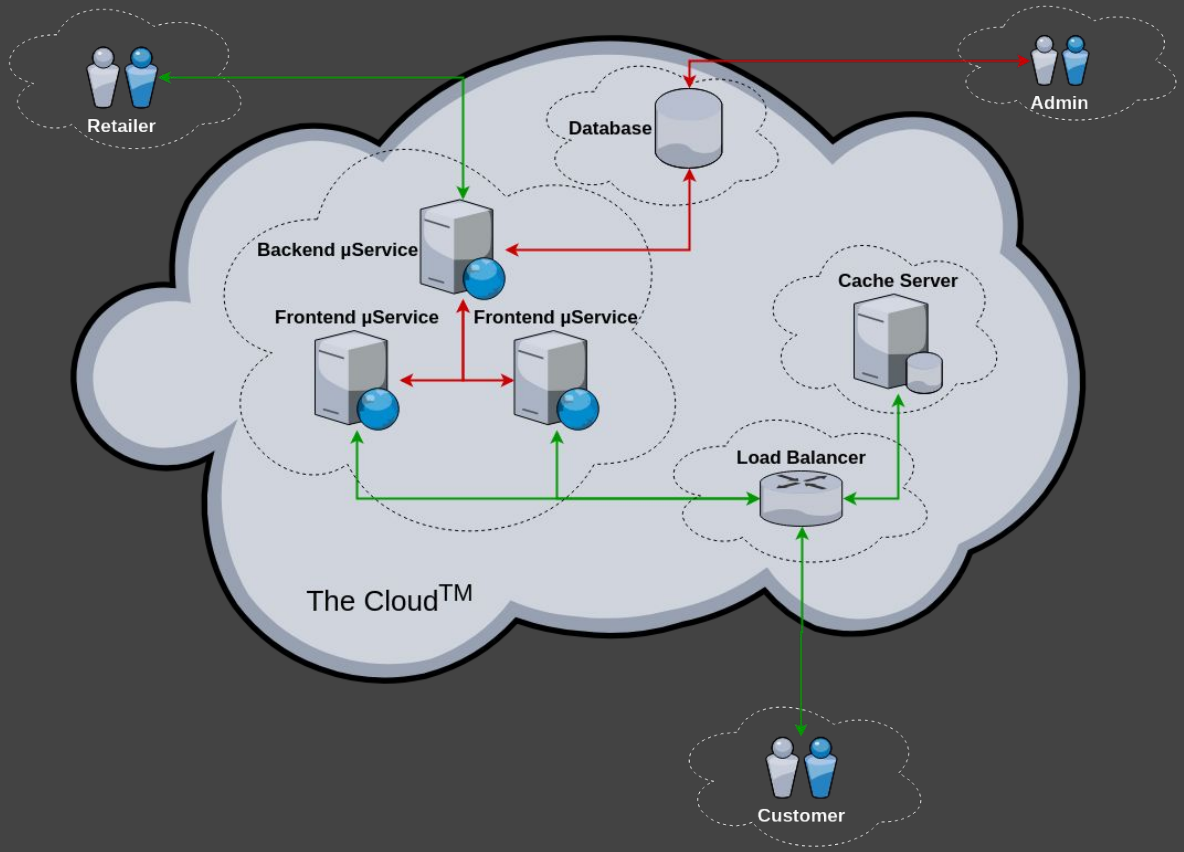
SESSION MANAGEMENT

J

Jeff can resend an identical repeat interaction (e.g. HTTP request, signal, button press) and it is accepted, not rejected

OWASP SCP
-
OWASP ASVS
15.1, 15.2
OWASP AppSensor
IE5
CAPEC
60
SAFECODE
12, 14

OWASP Cornucopia Ecommerce Website Edition v1.20-EN



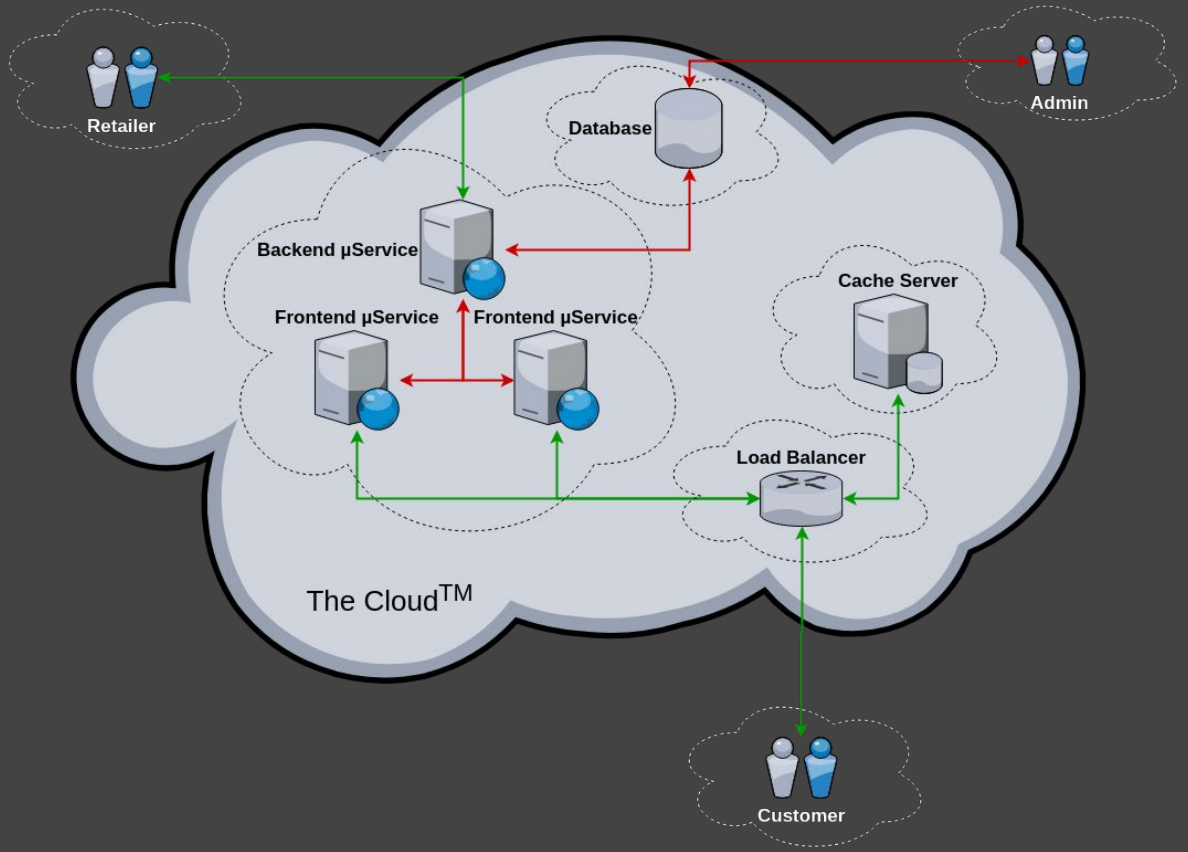
CRYPTOGRAPHY

8

Eoin can access stored business data (e.g. passwords, session identifiers, PII, cardholder data) because it is not securely encrypted or securely hashed

OWASP SCP	30, 31, 70, 133, 135
OWASP ASVS	2.13, 7.7, 7.8, 9.2
OWASP AppSensor	-
CAPEC	31, 37, 55
SAFECODE	21, 29, 31

OWASP Cornucopia Ecommerce Website Edition v1.20-EN



CORNUCOPIA

10

Xavier can circumvent the application's controls because code frameworks, libraries and components contain malicious code or vulnerabilities (e.g. in-house, commercial off the shelf, outsourced, open source, externally-located)

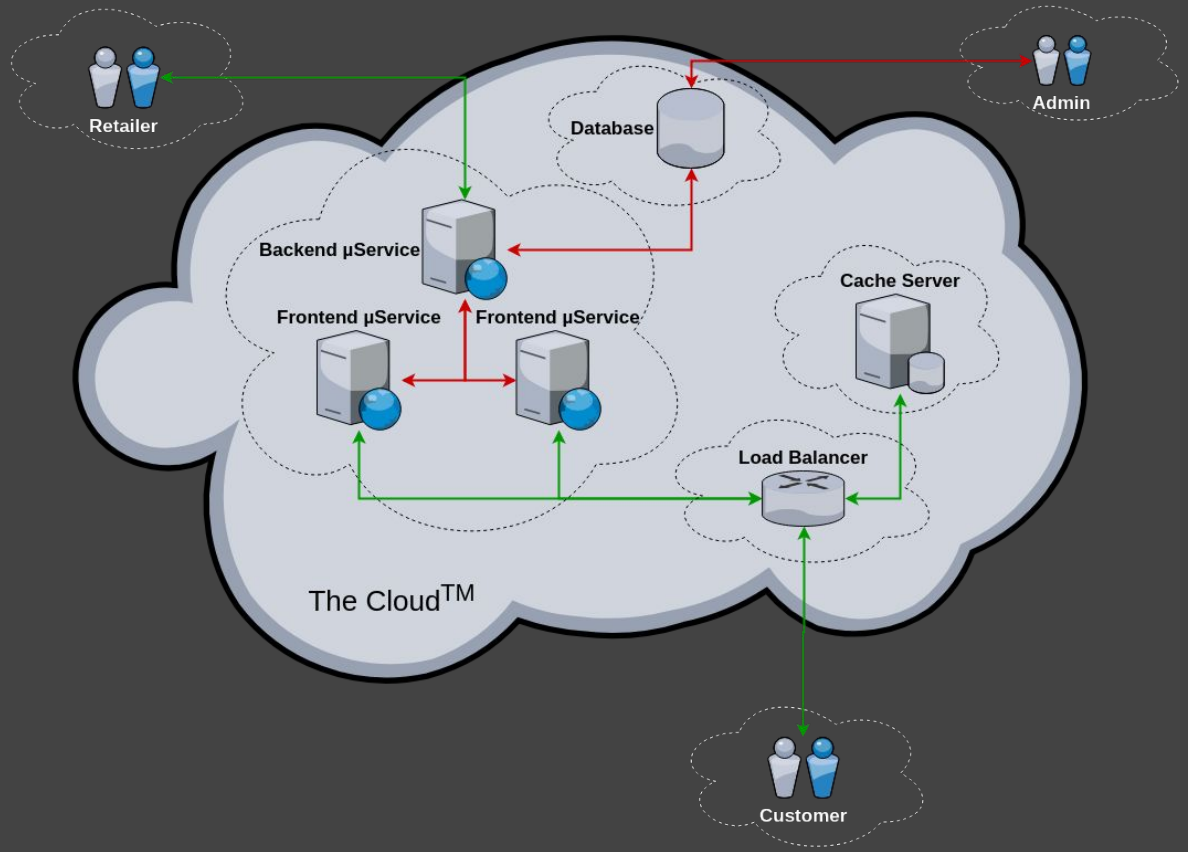
OWASP SCP
57, 151, 152, 204, 205, 213, 214

OWASP ASVS
1.11

OWASP AppSensor
-

CAPEC
68, 438, 439, 442, 524, 538

SAFECODE
15



③

What lessons were learned in the process?

It’s the best. It’s great. It’s true.

Documentation

Education

Visibility

Bug Hunting

Agility

Source: http://www.quickmeme.com/img/bb/bbc16868746f9549cca9b682ec15183b606fe304a258fb77c972a1652dd99317.jpg

Time

Effort

Immature process

10/10 would do this again

Source: https://www.computing.co.uk/w-images/e0dfb134-a128-4123-9ee3-7f421a32c293/3/StrictlyComeDancingScores10-580x358.jpg

Questions?

LinkedIN | Twitter | Email