University of BRISTOL

Systems Security

COMSM1500

bristol.ac.uk

RE/PLAY issue

- No sound
- I checked with IT
  - Microphone not properly connected to the computer
  - Should be fixed
- Next lectures should be properly recorded
- Please do check for issue
- Thanks to Rajat who spotted the problem

University of BRISTOL

Safety

bristol.ac.uk

Safety terminology

- Accident: unplanned and undesired event that leads to a loss
- Hazard: condition that can lead to an accident in a particular environment
- Incident: sometimes, a hazard that does not lead to an accident

- In security only “security incident”, it does not “happen by accident”

Safety and Security

- Safety: freedom from accident (caused without intent)
- Security: freedom from incident (caused maliciously)

Safety measure

1. eliminate hazard
2. reduce likelihood of occurrence
3. control
4. mitigate (reduce damage in case of accident)

Active/Passive

- Passive safety measure: presence alone contributes to safety
  - e.g. fences
- Fail-safe: fail in such a way that the system end-up in a safer state
  - e.g. fuse
- Active safety measure: monitor the system and intervene
  - e.g. fire tower (forest fire)

Risk

- risk = loss * probability of occurrence
  - Favored: reduce probability of accident (to zero if possible)
  - Reduce loss
- In most case it should not be acceptable to not reduce occurrence of hazard if possible
- Safety industry ALARP (as low as reasonably practical)
  - Must demonstrate further reduction is either impractical…
  - … or unreasonably costly

University of BRISTOL

Security

bristol.ac.uk

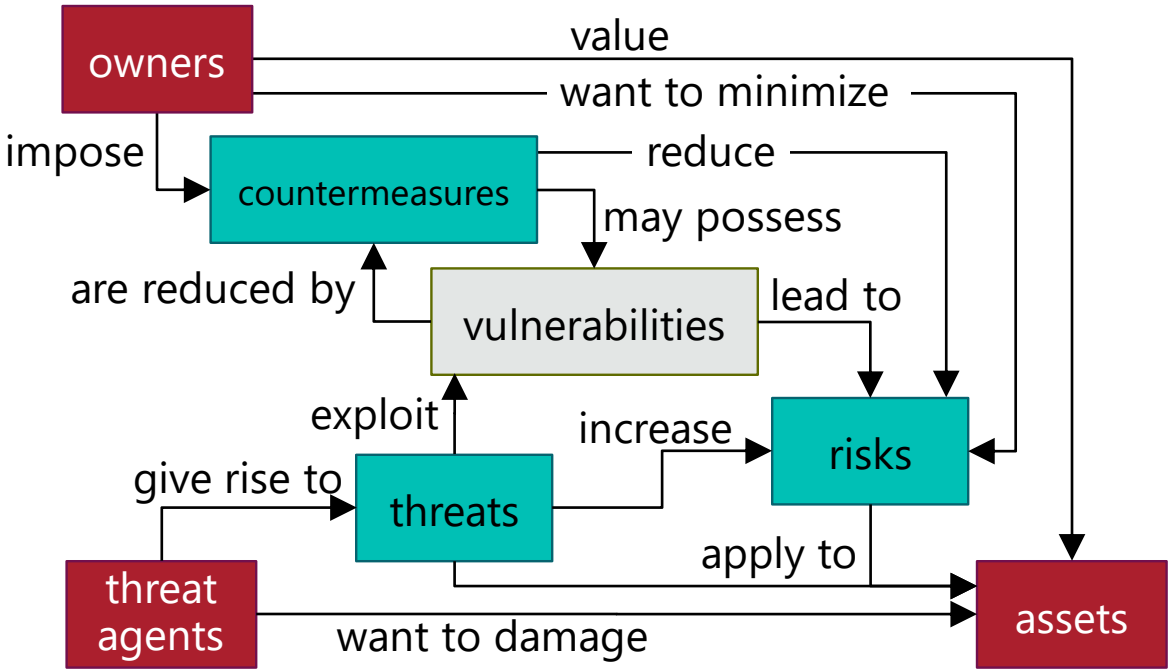
Computer Security

- *Protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data and telecommunications).*
  - US National Institute of Standards and Technology 1995

terminology

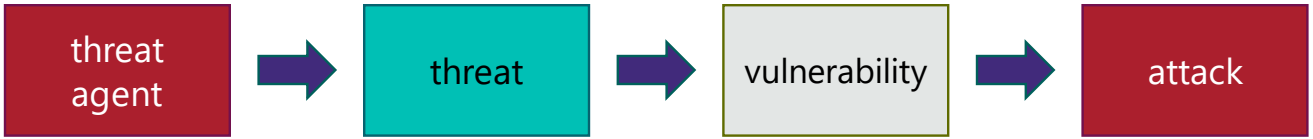
safety	security
hazard	vulnerability
(no equivalent)	threat
safety measure	countermeasure
risk	risk
accident / incident	incident

Terminology (IETF RFC 2828)



attack

- realisation of a threat
- sequence of actions that results in a loss



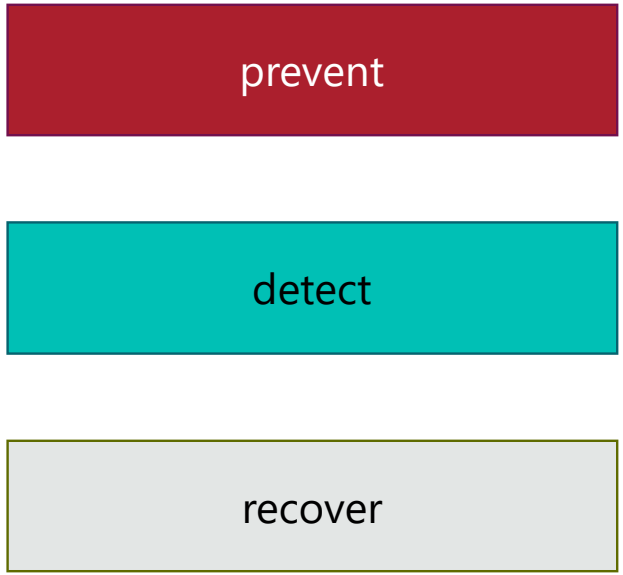
hackers

SQL injection

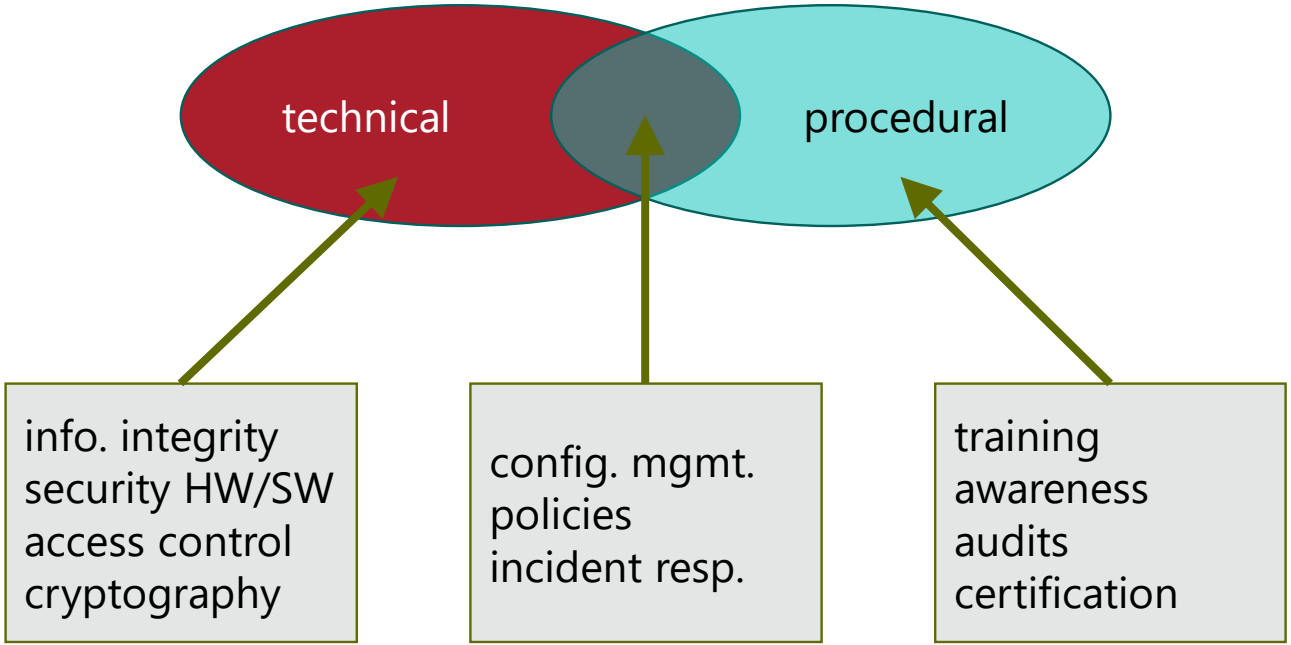
login form's code

deface the website

countermeasures



countermeasures



Risk (security economics side notes)

- risk = loss * probability of occurrence
- Think about CC fraud
  - Cost of preventive measure (i.e. reduce probably)
    VS
    Paying for damage
  - Bank prefer to pay for damage (simple cost calculation)
    - Simple risk calculation
    - Risk < cost of preventive measure
- In other industry:
  - Data leaks, maybe some damage to your image
  - GDPR fines for personal data leak (up to 4% of annual global turnover)
  - Loss sky rocket
  - Incentive to bring down probability of occurrence

Computer Security

- Policy -> Confidentiality, Integrity, Availability

Computer Security

- Policy -> Confidentiality, Integrity, Availability
  - C: only faculties can see your coursework

Computer Security

- Policy -> Confidentiality, Integrity, Availability
  - C: only faculties can see your coursework
  - I: only faculties can change grades

Computer Security

- Policy -> Confidentiality, Integrity, Availability
  - C: only faculties can see your coursework
  - I: only faculties can change grades
  - A: faculties must be able to enter grades/students to submit their work

Computer Security

- Policy -> Confidentiality, Integrity, Availability
  - C: only faculties can see your coursework
  - I: only faculties can change grades
  - A: faculties must be able to enter grades/students to submit their work
- Threat Model -> assumptions about the adversary, the system, the environment

Computer Security

- Policy -> Confidentiality, Integrity, Availability
  - C: only faculties can see your coursework
  - I: only faculties can change grades
  - A: faculties must be able to enter grades/students to submit their work
- Threat Model -> assumptions about the adversary, the system, the environment
- Mechanism -> Software/Hardware

Why is it hard?

- A faculty can access coursework
  - Easy just need to test!
- Negative goal
  - This is much harder
- Only a faculty can access coursework
  - It is hard need to think about what the adversary may do
  - Guess password?
  - Steal a laptop?
- It is an iterative process (we saw it during the last lecture)

What can go wrong?

- Policy
  - Last lecture
    - e-mail access
    - Amazon example

What can go wrong?

- Threat models
  - Human factor! (making assumption about what people would do)
  - Wrong assumptions about attacker knowledge (last lecture Apple)
  - Change over time (DES)
  - DARPA secure OS / similar issue more recently in China

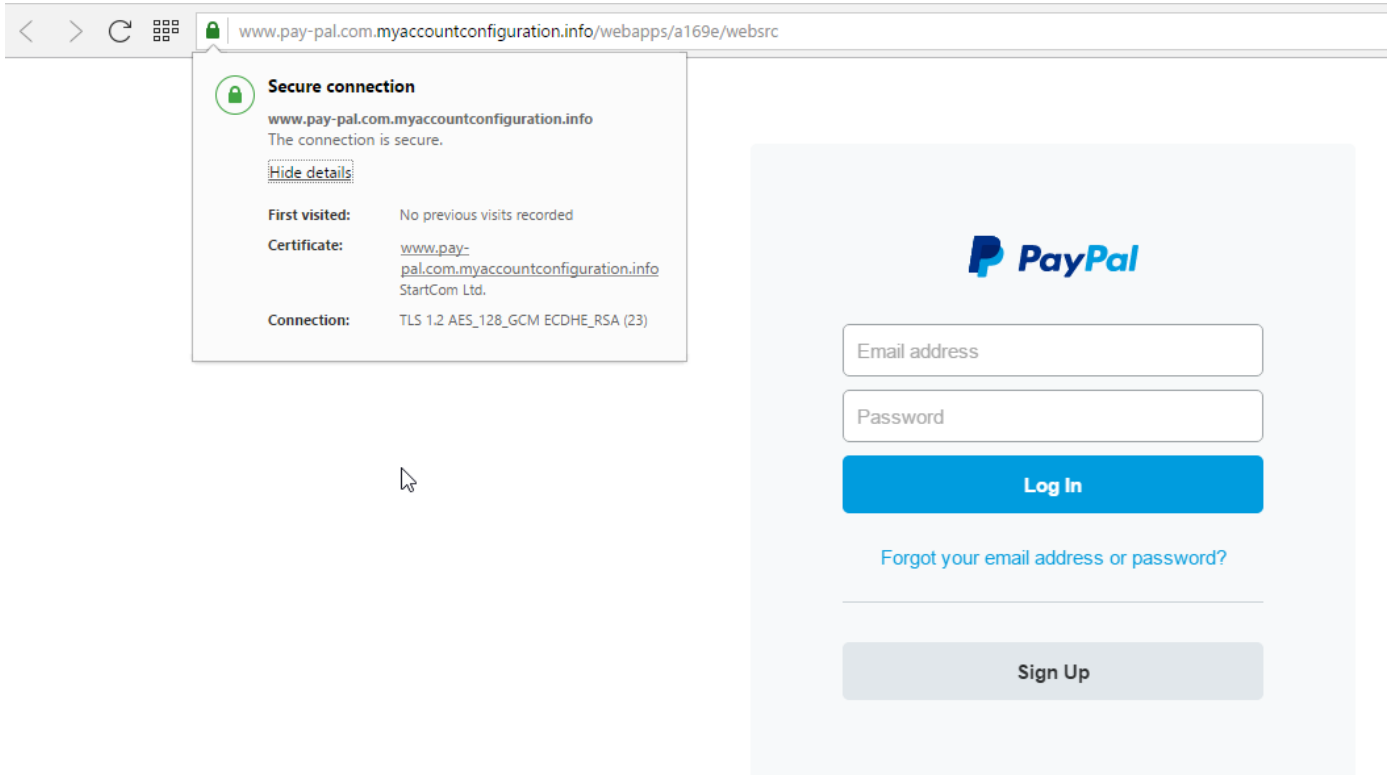
Jennifer Lawrence Phishing

- Simple and easy
- Send e-mail that appears to come from a legitimate party
- Ask for information
- Or link to a fake website looking like the real thing (i.e. please reset your password)


Man behind Jennifer Lawrence nude photo hack sentenced to prison

Edward Majerczyk, 29, of Chicago receives nine-month prison term in plea deal after illegally accessing celebrity accounts and stealing nude images

A legitimate fake site (untrustworthy CA)



What can go wrong?

- Mechanisms
  - That is the source of most vulnerabilities

Spectre/Meltdown (made simple)

- Late 2017/ Early 2018
- Lots of chatter online
- Fixes to the Linux Kernel being pushed
- Family of exploit to the same underlying vulnerability

Spectre/Meltdown (made simple)

- Problem is much larger
- Every OS is affected
- Modern CPU architecture is the problem
- Intel, AMD, ARM are affected

Spectre/Meltdown (made simple)

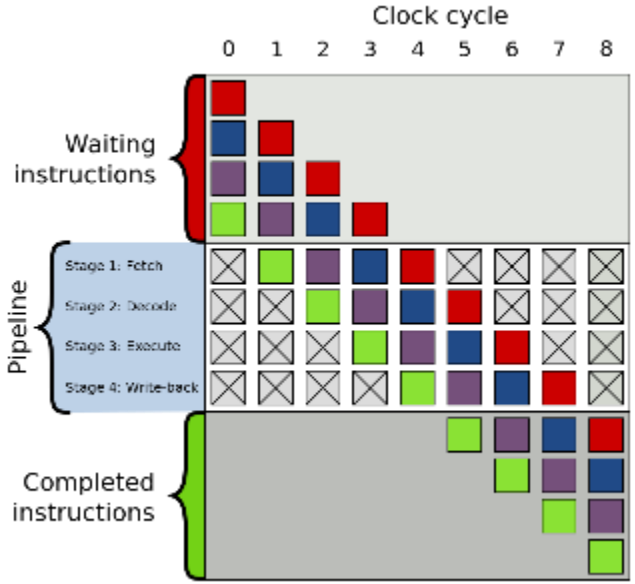
- Problem is much larger
- Every OS is affected
- Modern CPU architecture is the problem
- Intel, AMD, ARM are affected
- Can be exploited by a simple piece of javascript

University of BRISTOL

High risk!

bristol.ac.uk

Instructions pipeline



Branch and bubble

- Problem when branching
- Evaluate conditions
- Need to wait to get the instructions to put in the pipeline
- This create a “bubble”

Branch and bubble

- Problem when branching
- Evaluate conditions
- Need to wait to get the instructions to put in the pipeline
- This create a “bubble”
- Solution branch predictor
  - Make an educated guest of what should be executed
  - If wrong?

Branch and bubble

- Problem when branching
- Evaluate conditions
- Need to wait to get the instructions to put in the pipeline
- This create a “bubble”
- Solution branch predictor
  - Make an educated guest of what should be executed
  - If wrong
    - CPU state is reverted (that is good)
    - … but CPU cache is not (that is bad)

Branch and bubble

- Problem when branching
- Evaluate conditions
- Need to wait to get the instructions to put in the pipeline
- This create a “bubble”
- Solution branch predictor
  - Make an educated guest of what should be executed
  - If wrong
    - CPU state is reverted (that is good)
    - … but CPU cache is not (that is bad)
  - If guessed wrong we may have (half) executed instructions in the pipeline

Spectre/Meltdown (made simple)

- Exploit branch prediction

Spectre/Meltdown (made simple)

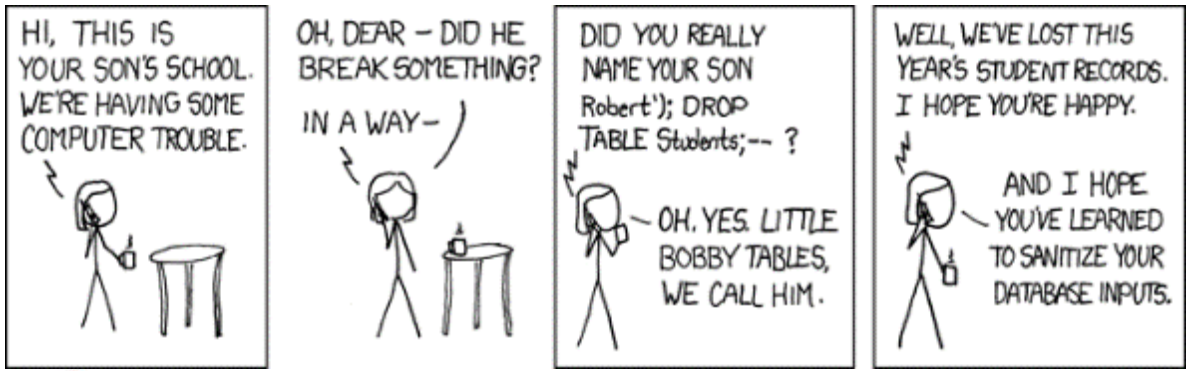
- Exploit branch prediction
- You can get access to data in the cache
- Access check is done when instructions are “executed”
- You can read kernel memory, leak password, keys etc…
  - if (x < array1.size)
  - y = array2[array1[x]]

- https://github.com/bris-sys-sec/docs/tree/master/specter-meltdown

SQL injection

- Attacker can pass any command to the database
  - SELECT, INSERT, UPDATE, DELETE

```php
global $wpdb;
$title = $wpdb->get_var("select post_title from " . $wpdb->posts . " where ID="
. $_GET['id']);
echo $title;
```



Relatively easy fix

```php
global $wpdb;
$title = $wpdb->get_var($wpdb->prepare("select post_title from " . $wpdb->posts
. " where ID=%d", $_GET['id']));
echo $title;
```

COURSEWORK GROUPS!

- Groups of 4 students
- (only) 1 e-mail per group
  - thomas.pasquier@bristol.ac.uk
    - Header: [Systems Security] Group
    - Body: id1, id2, id3, id4
- If you cannot form a group you will get one, no need to e-mail me (>80)
- I will circulate the list
- FRIDAY 7PM
- IF NOT IN A GROUP RANDOM ALLOCATION

University of BRISTOL

Thank you

Office MVB 3.26

bristol.ac.uk