University of BRISTOL

Systems Security

COMSM1500

bristol.ac.uk

University of BRISTOL

About the unit

bristol.ac.uk

Unit principles

- You are in 3rd/4th year
- You have good understanding of C, assembly, network stack, cryptography etc.

Unit principles

- You are in 3rd/4th year
- You have good understanding of C, assembly, network stack, cryptography etc.

- This unit is about **breadth** not depth
- Topics explored from a security perspective
- Your objective is to understand fundamental **concepts**
- And how they apply to **systems security**

WARNING

- You may learn how to break things
- This is necessary to understand how to secure things

- Do not do anything illegal
- Do not attack any university systems

Schedule

- Lectures:
  - Tuesdays 9-10 / Fridays 11-12
  - ~45 minutes (there is time for questions, you can interrupt me)
  - You can come talk to me at the end of the lecture
  - Office hours online

Schedule

- Lectures:
  - Tuesdays 9-10 / Fridays 11-12
  - ~45 minutes (there is time for questions, you can interrupt me)
  - You can come talk to me at the end of the lecture
  - Office hours online (http://tfjmp.org)

Schedule

- Lectures:
  - Tuesdays 9-10 / Fridays 11-12
  - ~45 minutes (there is time for questions, you can interrupt me)
  - You can come talk to me at the end of the lecture
  - Office hours online
- Labs:
  - Mondays 2-4
  - On week 2, 5, 6, 9, 10

Schedule

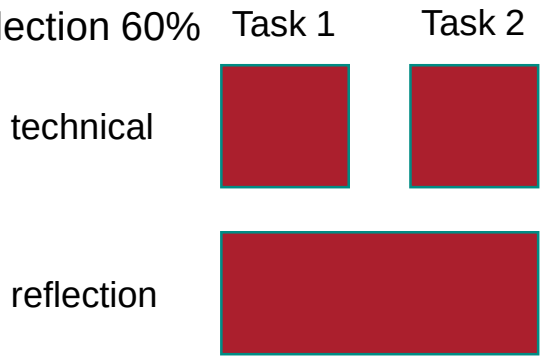
- Lectures:
  - Tuesdays 9-10 / Fridays 11-12
  - ~45 minutes (there is time for questions, you can interrupt me)
  - You can come talk to me at the end of the lecture
  - Office hours online
- Labs:
  - Mondays 2-4
  - On week 2, 5, 6, 9, 10
- Week 8 reading week

Schedule

- Lectures:
  - Tuesdays 9-10 / Fridays 11-12
  - ~45 minutes (there is time for questions, you can interrupt me)
  - You can come talk to me at the end of the lecture
  - Office hours online
- Labs:
  - Mondays 2-4
  - On week 2, 5, 6, 9, 10
- Week 8 reading week
- Week 12 revision week (there will be “revision” lectures)

Grading

- 40% exam
- 60% coursework
  - two coursework (30%)
    - technical report 40% (2x20%)
    - reflection 60%



Coursework (1/3)

- Check material online
  - https://github.com/bris-sys-sec
- No need to wait for the lab to start working
- Come to the lab (mandatory)
  - Labs week 5, 6, deadline week 7 Friday 7pm
  - Labs week 9, 10, deadline week 11 Friday 7pm
- Lab 0 to make sure you have the basis
- If you struggle during lab 0 consider dropping the unit

Coursework (2/3)

- You need to bring your laptops (again check instructions online)
- Lab 0: introduction (how to use Linux and VMs)
- Lab 1: format string
- Lab 2: buffer overflow
- Lab 3: SQL injection
- Lab 4: network

- TAs are here to help, not to give you the solution!
- Technical part is graded
  - That means YOU need to get it to work
  - In the past students who did not met the prerequisite struggled

Coursework (3/3)

- Coursework goals are:
  - Gaining a practical understanding of vulnerabilities (practicals);
  - Learning how to identify mitigation techniques.
- The goal is not to spend hours on the technical work;
- The goal is to develop critical though and research skills;
- TAs support technical work;
- The lecturer support reflective work.

Coursework (3/3)

- Coursework goals are:
  - Gaining a practical understanding of vulnerabilities (practicals);
  - Learning how to identify mitigation techniques.
- The goal is not to spend hours on the technical work;
- The goal is to develop critical though and research skills;
- TAs support technical work;
- The lecturer support reflective work.
  - Come talk to me!

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**

Exam

- 10 points Unit means 100h work
  - 20h lectures
  - 10h labs
  - the rest: individual work and research

- Questions 60%, Essay 40%
  - Choice between 3 essay topics
- Top grades requires to go beyond the lectures
- Giving (relevant) example from outside the lectures is good
- Read the news, check extra material on github, google …

Exam

- 10 points Unit means 100h work
  - 20h lectures
  - 10h labs
  - the rest: individual work and research

- Questions 60%, Essay 40%
  - Choice between 3 essay topics
- Top grades requires to go beyond the lectures
- Giving (relevant) example from outside the lectures is good
- Read the news, check extra material on github, google, academic articles …
  - … that is only necessary for top grade, i.e. **going beyond expectation**

Lecture notes

- Slides are presentation support
- I expect you to make your own lecture notes
- i.e. slides are unlikely to be sufficient revision support

Lecture notes

- Slides are presentation support
- I expect you to make your own lecture notes
- i.e. slides are unlikely to be sufficient revision support
- Lectures on Re/Play Blackboard
  - Please, let me know of technical issues
  - … and contact IT
  - i.e. I have no more control than you

Blackboard

- Be nice I am hopeless with it!
- I will put important material on github
  - Coursework material
  - Slides (it will pop up as we go through the unit)
  - Reading material (it will pop up as we go through the unit)
  - etc…
- If there is material that you would like that is not there let me know

Blackboard

- Be nice I am hopeless with it!
- I will put important material on github
  - Coursework material
  - Slides (it will pop up as we go through the unit)
  - Reading material (it will pop up as we go through the unit)
  - etc…
- If there is material that you would like that is not there let me know

University of BRISTOL

Systems

bristol.ac.uk

System what is it?

System what is it?

- A collection of component

System what is it?

- A collection of component
- With relationships and connections

System what is it?

- A collection of component
- With relationships and connections
- A purpose/goal

System what is it?

- A collection of component
- With relationships and connections
- A purpose/goal
- Within an environment

System what is it?

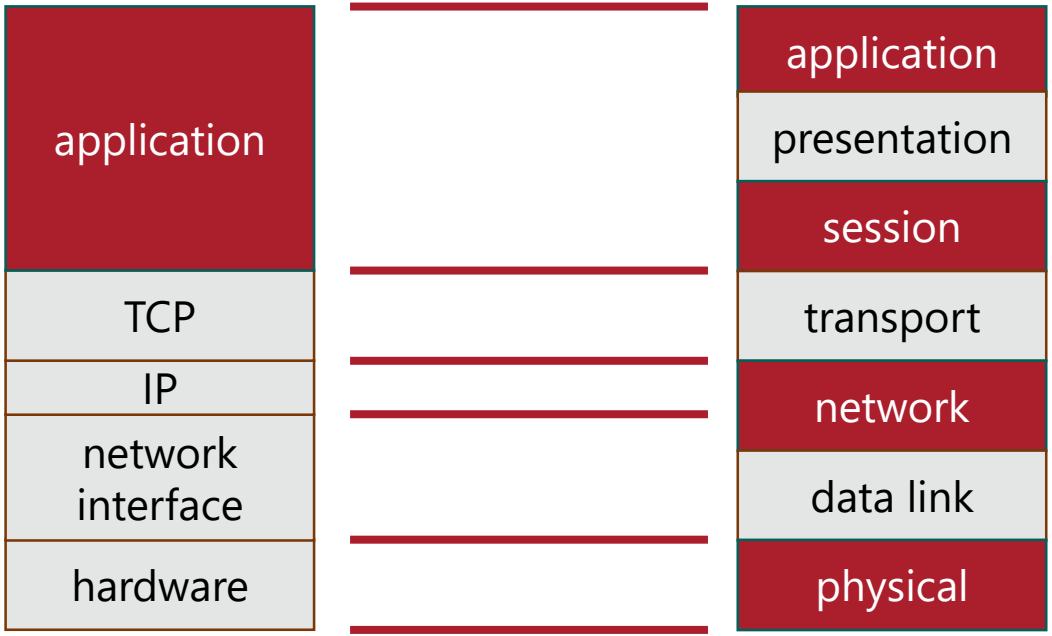
- A collection of component
- With relationships and connections
- A purpose/goal
- Within an environment
- With artificial boundaries

University of BRISTOL

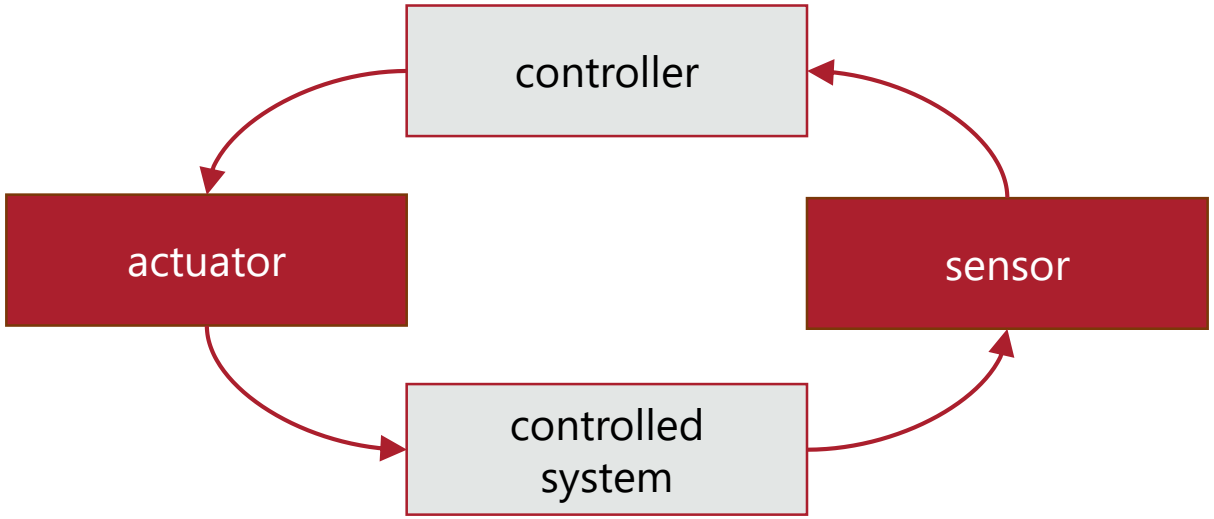
Discuss

How do I make sure my server remain available?

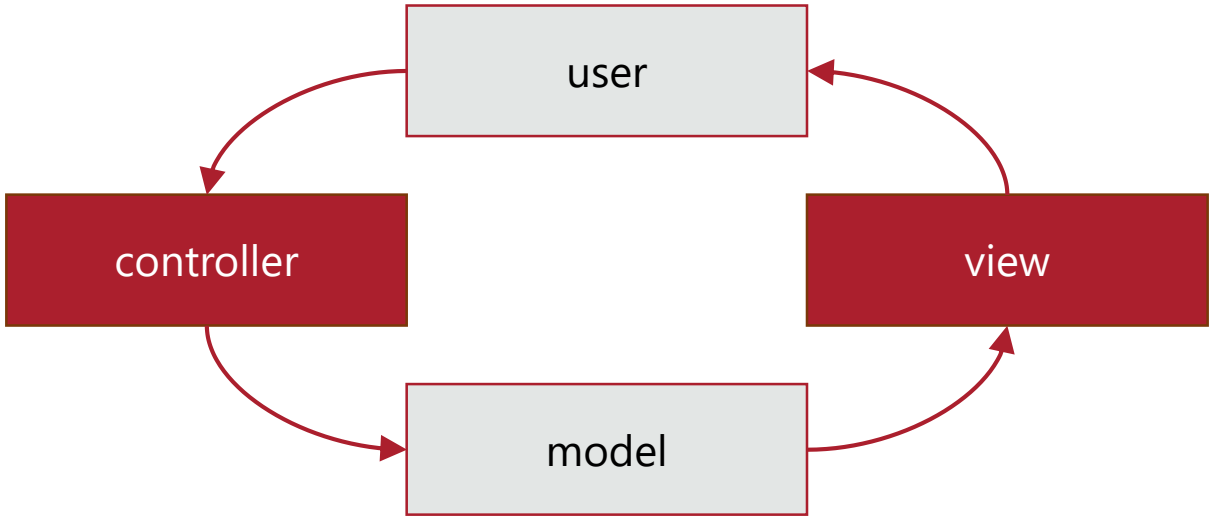
subsystems and levels



control and feedback



control and feedback



Emerging behaviour

- A system is more than the sum of its parts
- Think about integration testing
  - There is similar concern for security
- Components are not secure on their own
  - Security is a property of the system

University of BRISTOL

Questions?

University of BRISTOL

Example

e-mail recovery

E-mail recovery

- Policy: you need to know the password to access an account

E-mail recovery

- Policy: you need to know the password to access an account
- … or you need to know the answer to the recovery questions?

E-mail recovery

- Policy: you need to know the password to access an account
- … or you need to know the answer to the recovery questions?

KIM ZETTER SECURITY 09.19.08 10:05 AM

PALIN E-MAIL HACKER SAYS IT WAS EASY

E-mail recovery

- Policy: you need to know the password to access an account
- … or you need to know the answer to the recovery questions?
- DoB, ZIP, where did you meet your partner?
- Just Google it!

KIM ZETTER SECURITY 09.18.08 10:05 AM

PALIN E-MAIL HACKER SAYS IT WAS EASY

E-mail recovery

- Policy: you need to know the password to access an account
- … people started to get more creative

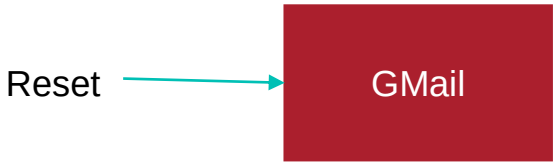
E-mail recovery

- Policy: you need to know the password to access an account
- … people started to get more creative

- Took over twitter account deleted google account etc.
- Mat Honan (Journalist)
- A real story!

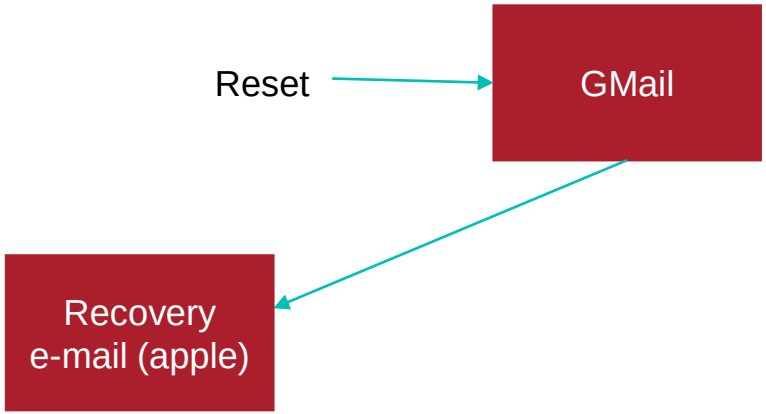
What happened?

- Took over twitter account, deleted google account etc.



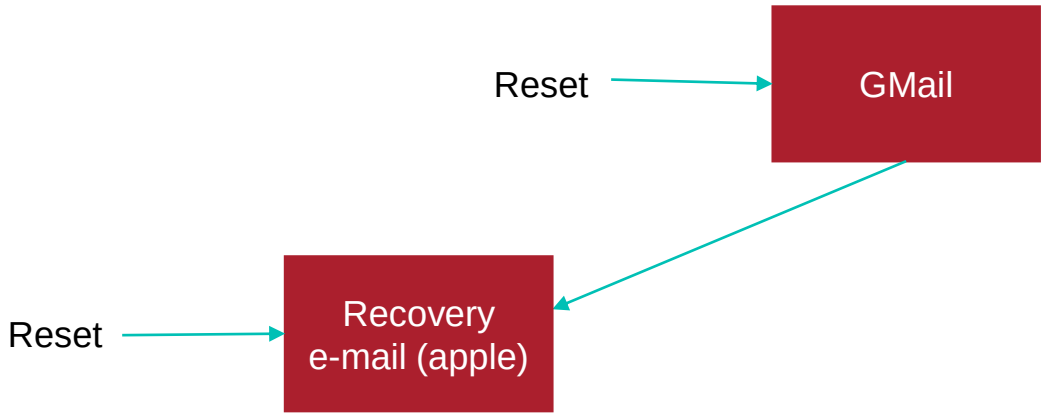
What happened?

- Took over twitter account, deleted google account etc.



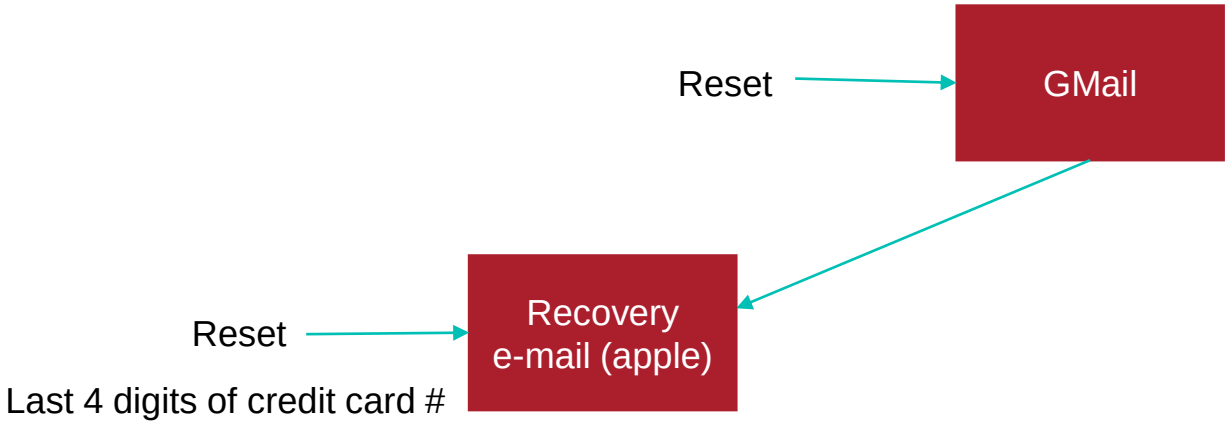
What happened?

- Took over twitter account, deleted google account etc.



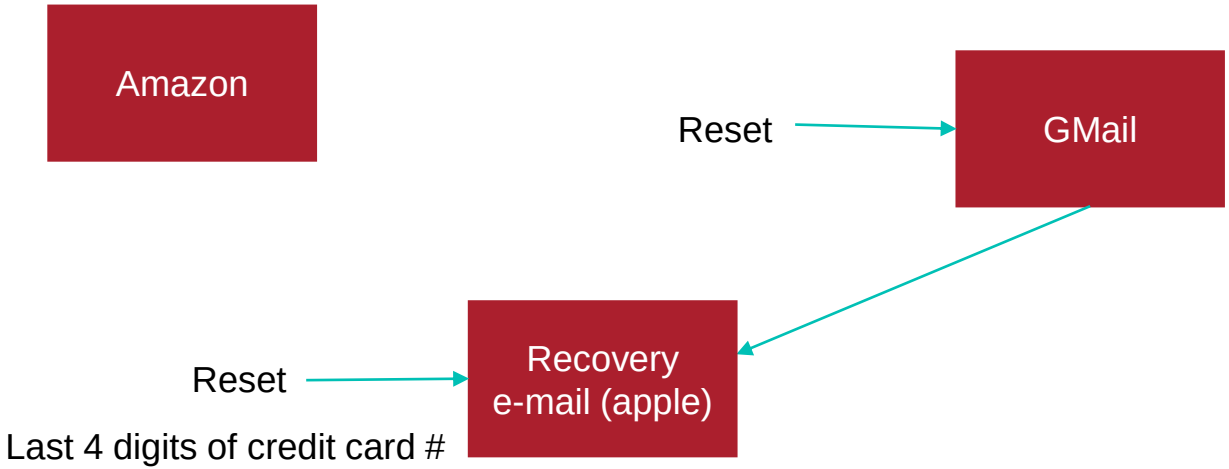
What happened?

- Took over twitter account, deleted google account etc.



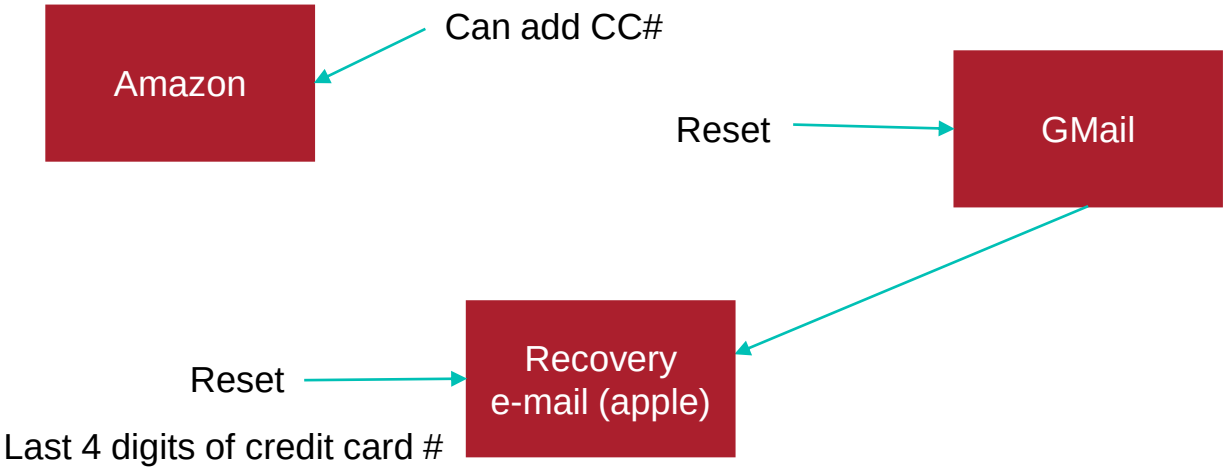
What happened?

- Took over twitter account, deleted google account etc.



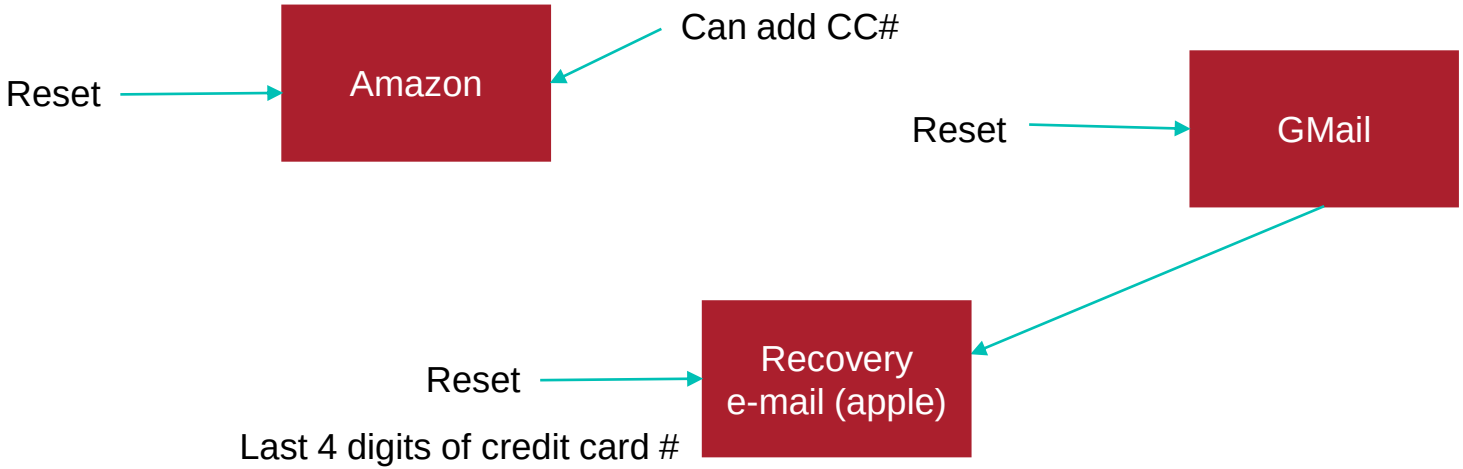
What happened?

- Took over twitter account, deleted google account etc.



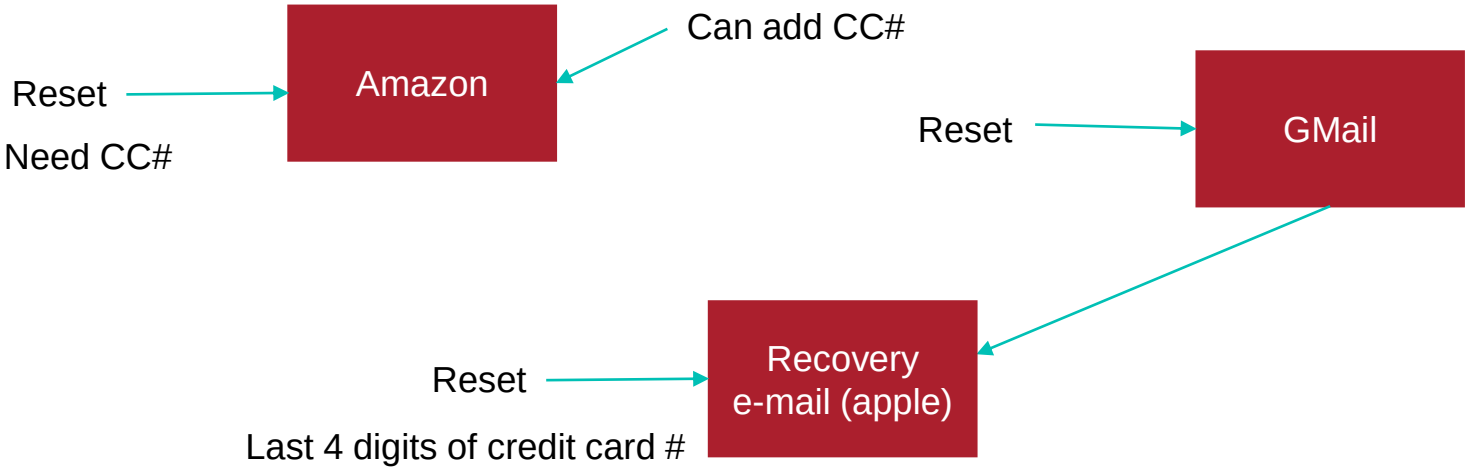
What happened?

- Took over twitter account, deleted google account etc.



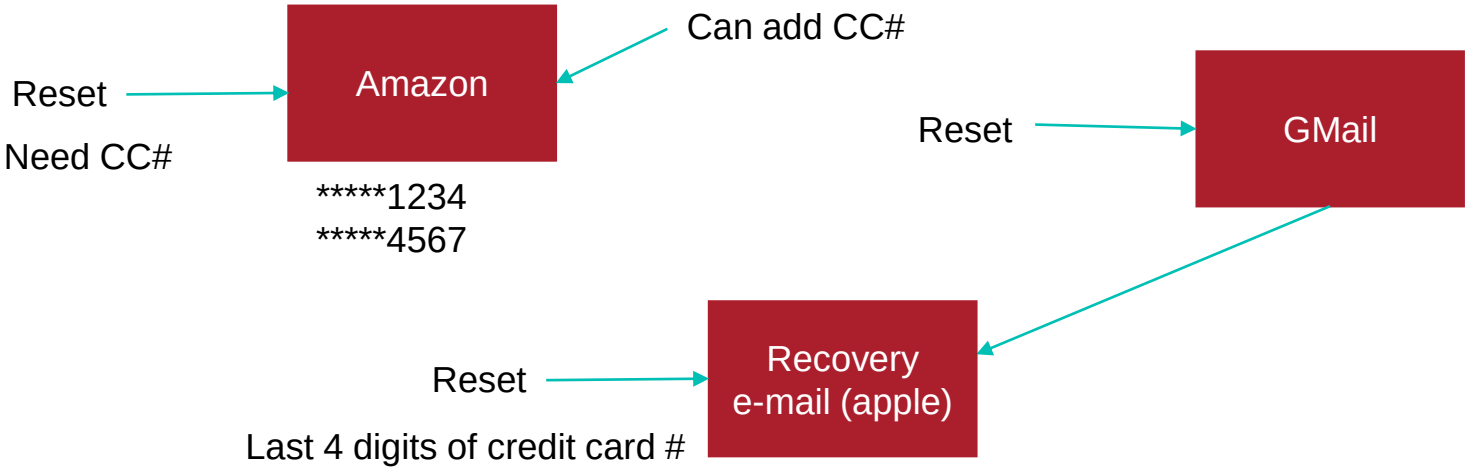
What happened?

- Took over twitter account, deleted google account etc.



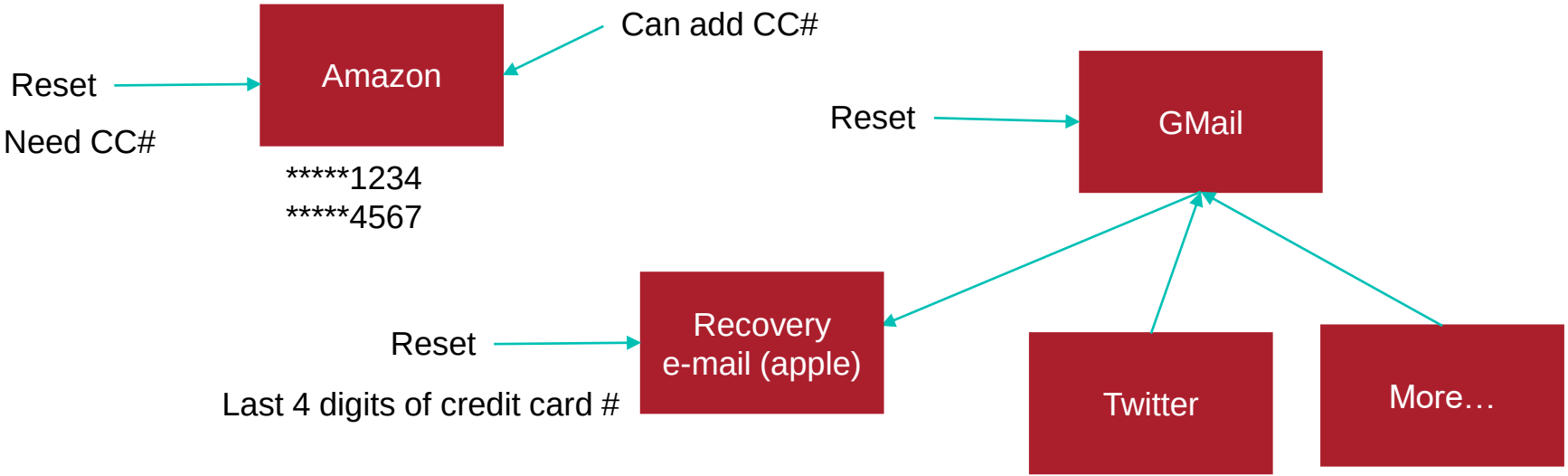
What happened?

- Took over twitter account, deleted google account etc.



What happened?

- Took over twitter account, deleted google account etc.



E-mail recovery

- Individual policies made sense
- Did not take in consideration the larger environment

- Now?
  - Two factor authentication etc…
  - Until someone find a vulnerability?

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