

Systems Security

COMSM1500

About the unit

bristol.ac.uk



Unit principles

- You are in 3rd/4th year
- You have good knowledge 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**

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:
 - Tuesday 11-12 / Friday 12-13
 - ~45 minutes (there is time for questions, you can interrupt me)
 - You can come at the end of the lecture
 - Office hours Tuesday 12-13, Friday 13-14 (in MVB 3.26)
- Labs:
 - Monday 2-4
 - On week 2, 5, 6, 9, 10
- Week 8 reading week

Grading

- 40% exam
- 60% coursework
 - two coursework (30%)
 - 4 part per coursework (7.5%) each

	Task 1	Task 2
technical		
reflection		

Coursework (1/2)

- Join the unit slack channel
 - <https://bris-sys-sec.slack.com>
- Check material online
 - <https://github.com/bris-sys-sec>
- No need to wait for the lab to start working
- Come to the lab to ask questions
 - 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 (2/2)

- You need to bring your laptops (again check instructions online)
- Lab 0: introduction
- 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 meet the prerequisite struggled

Exam

- 10 points Unit means 100h work
 - 22h 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 worth more
- Read the news, check extra material on github, google ...

Systems



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

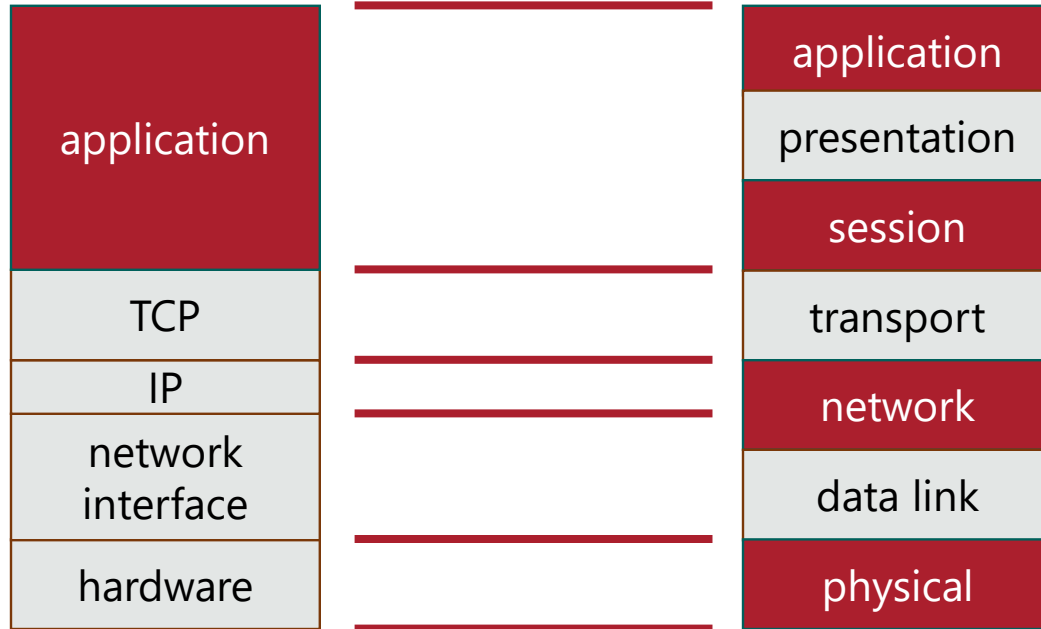
System what is it?

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

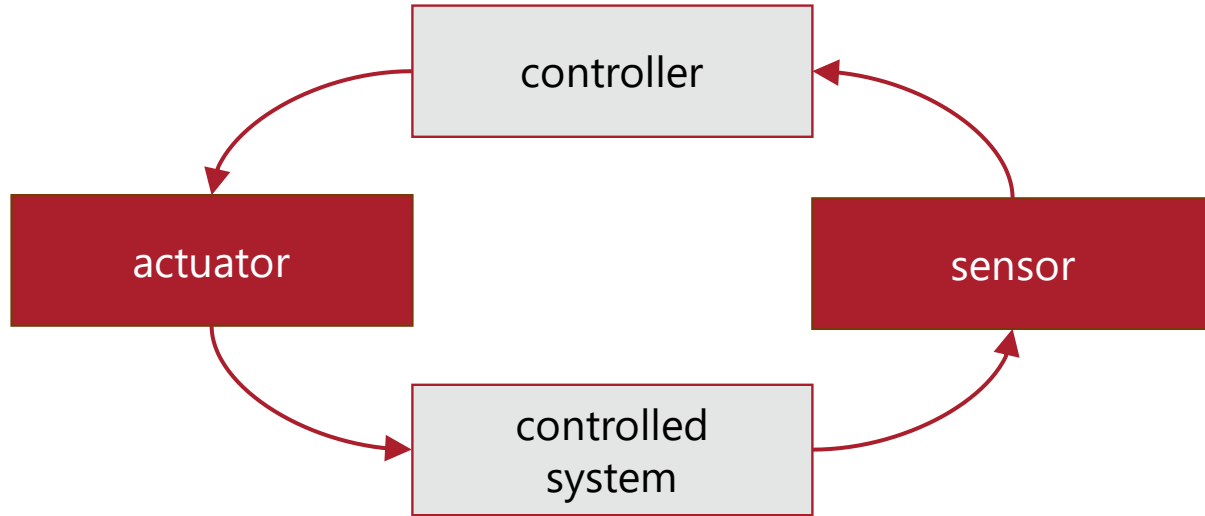
Discuss

How do I make sure my server remain available?

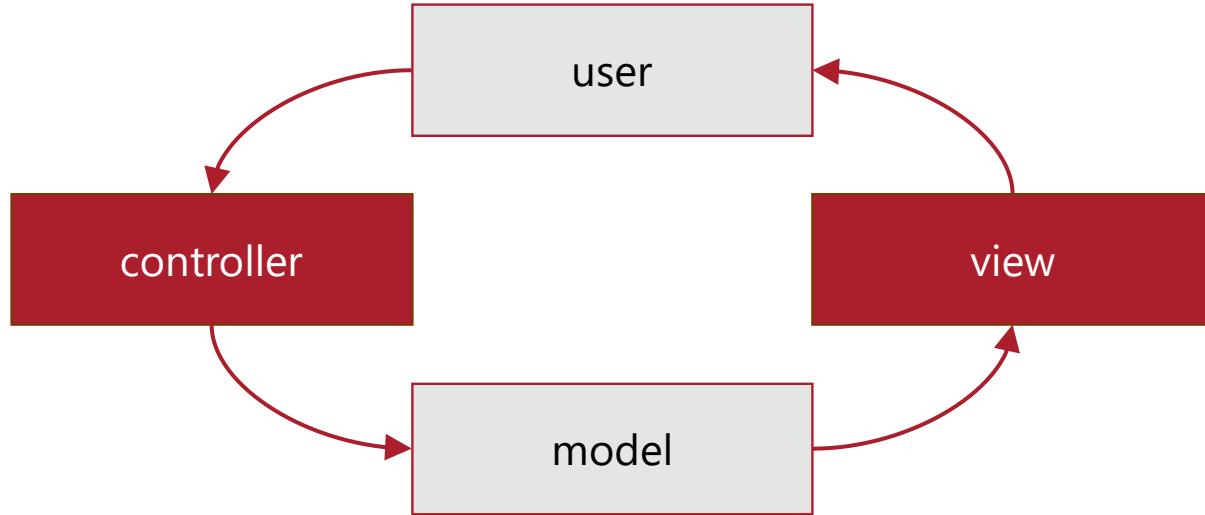
subsystems and levels



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

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 02.10.06 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 02.10.06 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

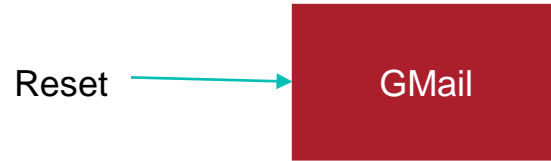
- Policy: you need to know the password to access an account
- ... people started to get more creative
- Took over twitter account
deleted google account etc.

MAC HENRY BEAR 00.06.13 00:01 PM
**HOW APPLE AND AMAZON
SECURITY FLAWS LED TO MY
EPIC HACKING**



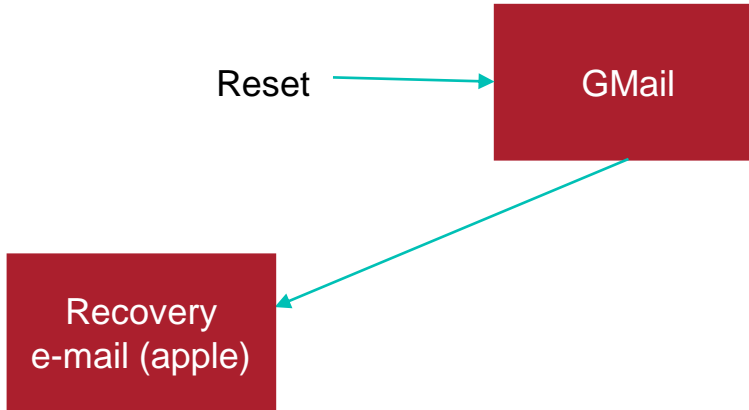
What happened?

- Took over twitter account, deleted google account etc.



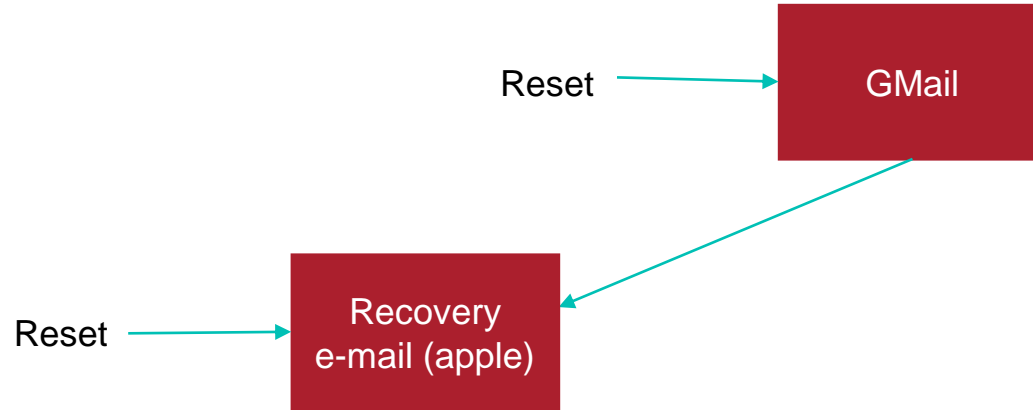
What happened?

- Took over twitter account, deleted google account etc.



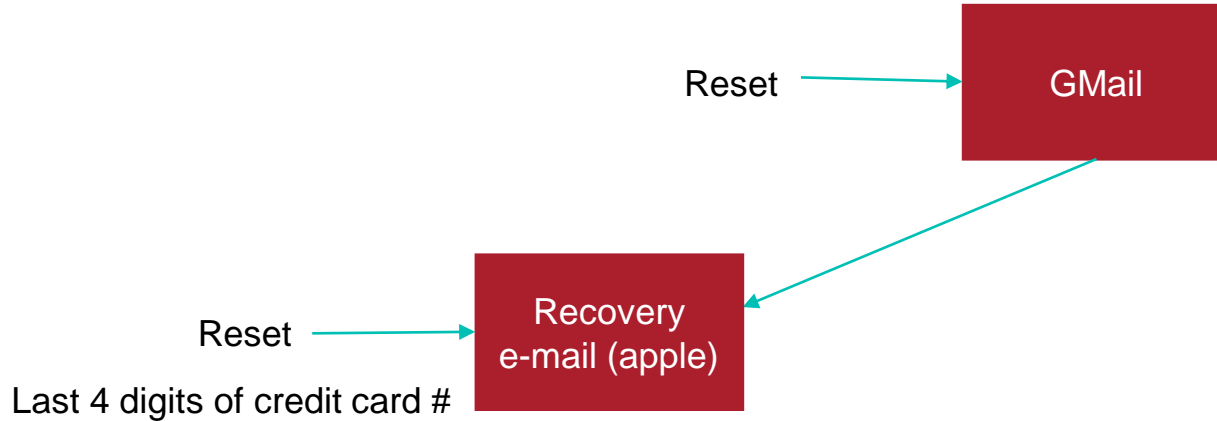
What happened?

- Took over twitter account, deleted google account etc.



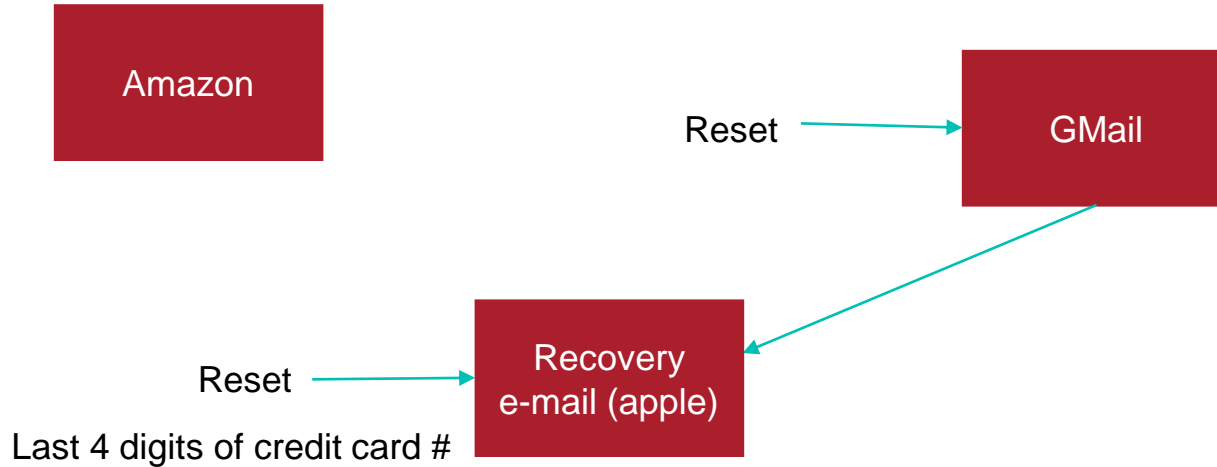
What happened?

- Took over twitter account, deleted google account etc.



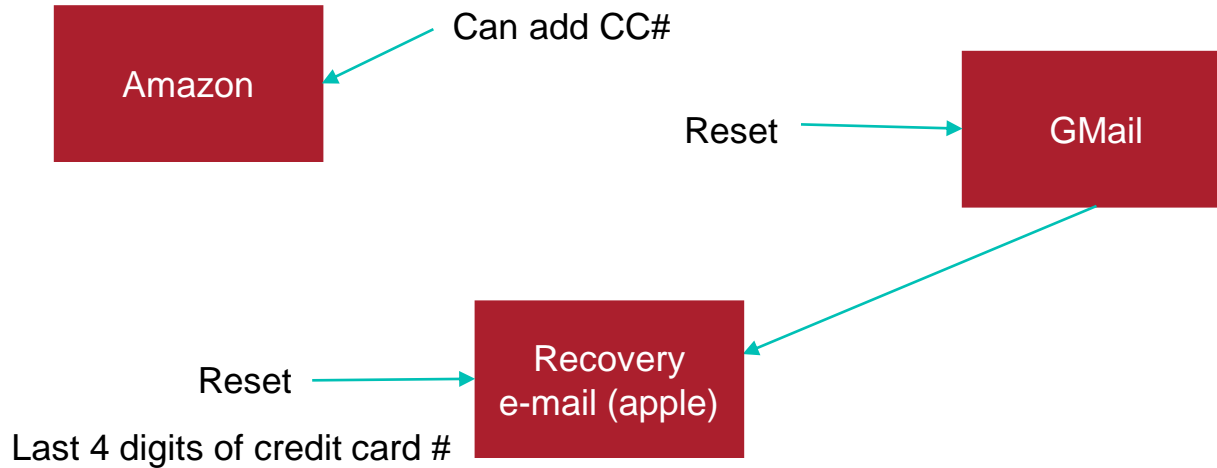
What happened?

- Took over twitter account, deleted google account etc.



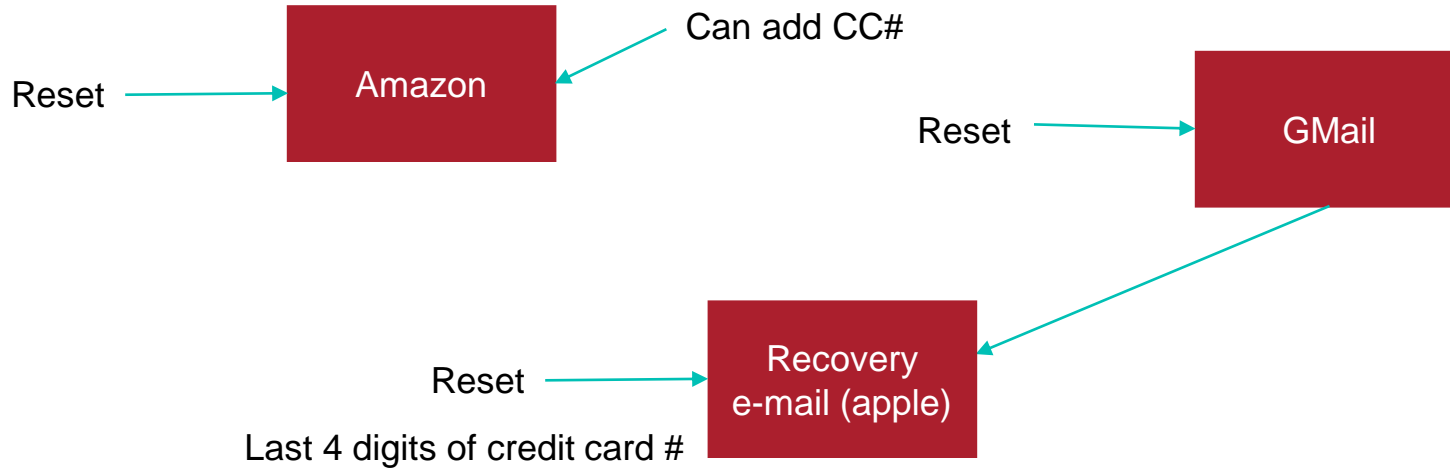
What happened?

- Took over twitter account, deleted google account etc.



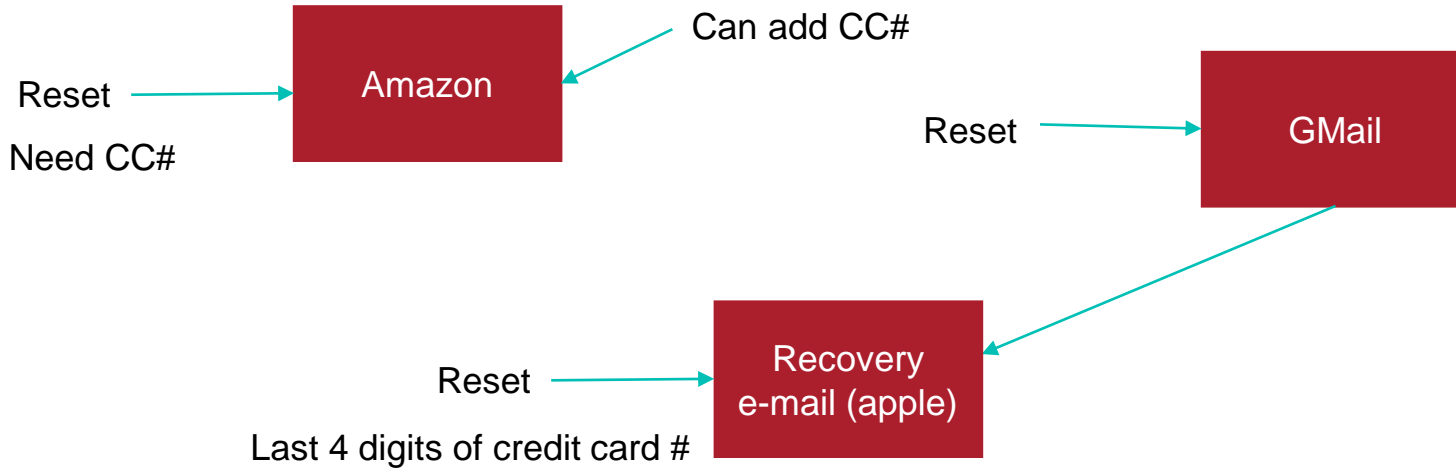
What happened?

- Took over twitter account, deleted google account etc.



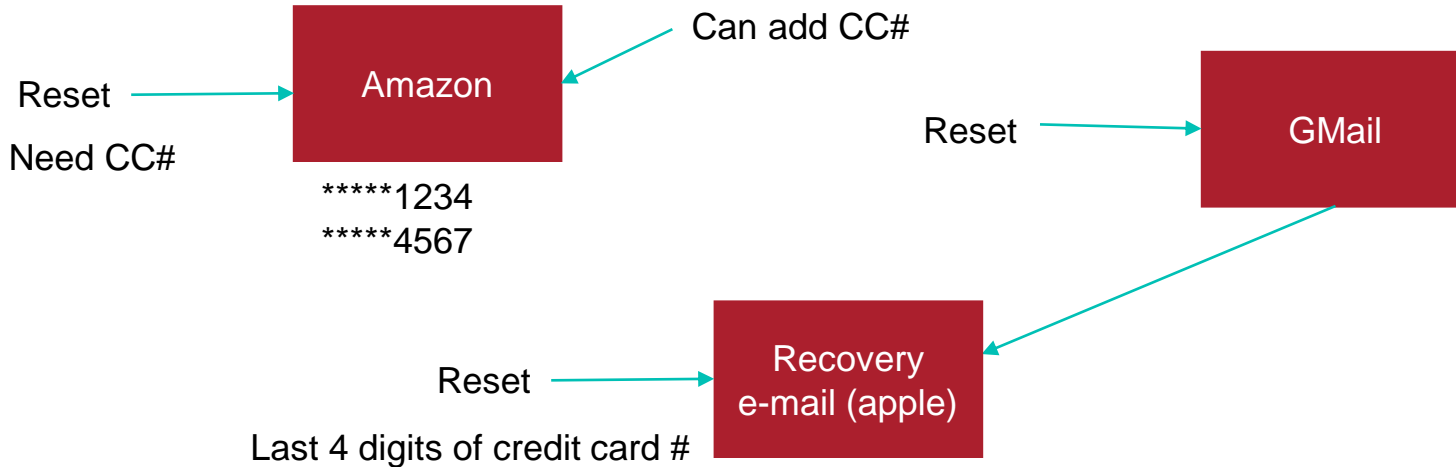
What happened?

- Took over twitter account, deleted google account etc.



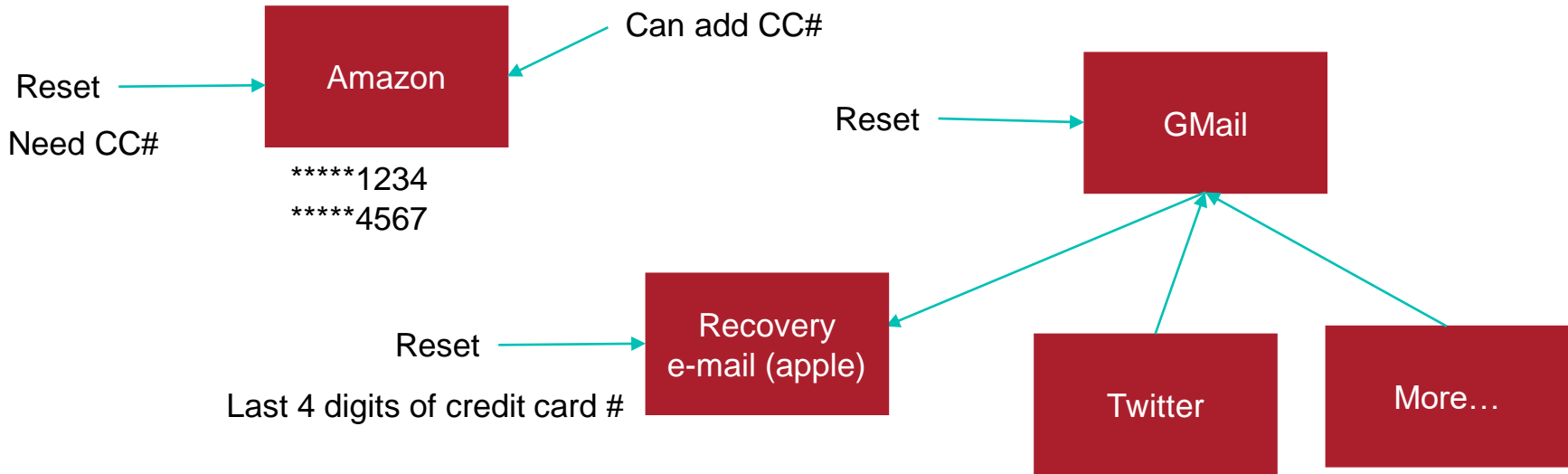
What happened?

- 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

Thank you

Office MVB 3.26

bristol.ac.uk

