University of BRISTOL

Computer Systems B

COMS20012

Introduction to Operating Systems and Security

bristol.ac.uk

University of BRISTOL

Threat 2

The recovery problem

bristol.ac.uk

Password recovery

- External knowledge
  - Social Media
  - Famous people
  - Environment vulnerability
  - etc…
- Social engineering
  - Fake e-mail
  - Fake website
  - Ask over the phone
  - etc…
- Entropy of recovery is very bad! Entropy = Min(Ent(password), Ent(Recovery))
  - e.g. what's your favorite color? (likely red or blue)
  - User selected questions are terrible (e.g. 2+3)

bristol.ac.uk

University of BRISTOL

Examples

bristol.ac.uk

E-mail recovery

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

bristol.ac.uk

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?

bristol.ac.uk

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 09.10.08 10:05 AM

PALIN E-MAIL HACKER SAYS IT WAS EASY

bristol.ac.uk

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!

bristol.ac.uk

E-mail recovery

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

bristol.ac.uk

E-mail recovery

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

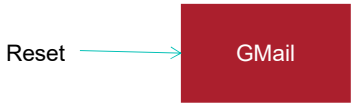
- Took over twitter account deleted google account etc.
- A real story!

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING

bristol.ac.uk

What happened?

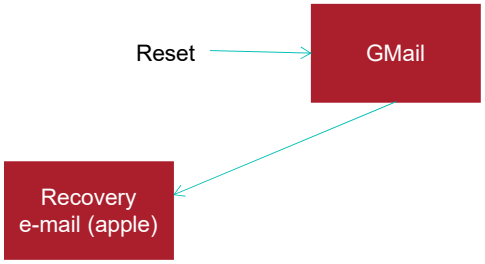
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

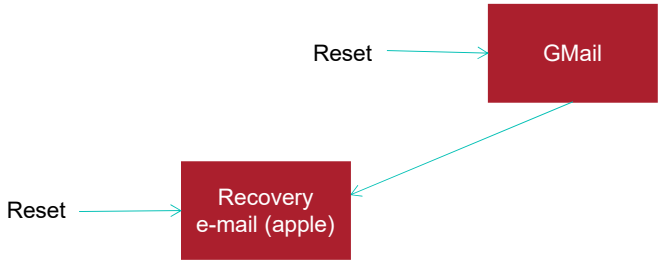
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

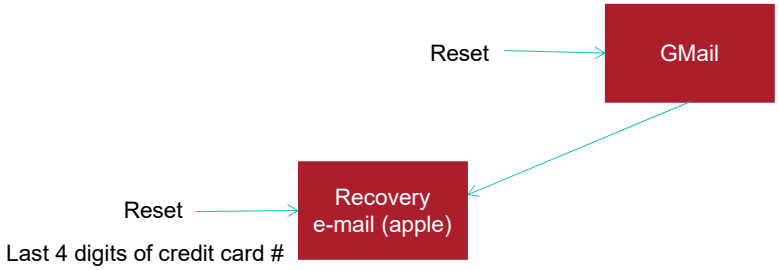
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

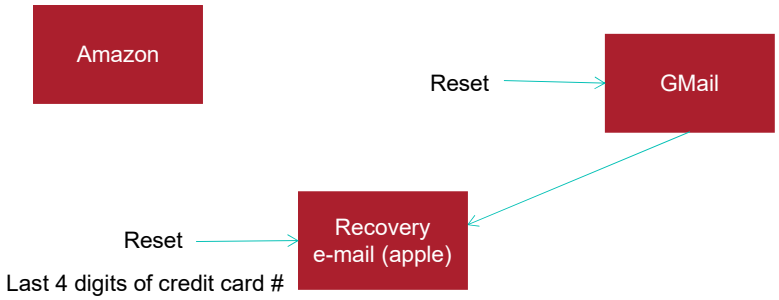
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

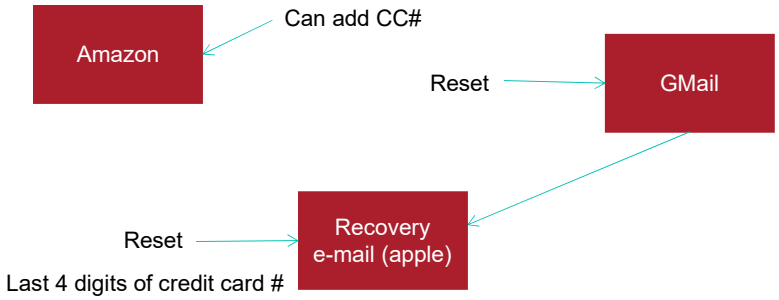
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

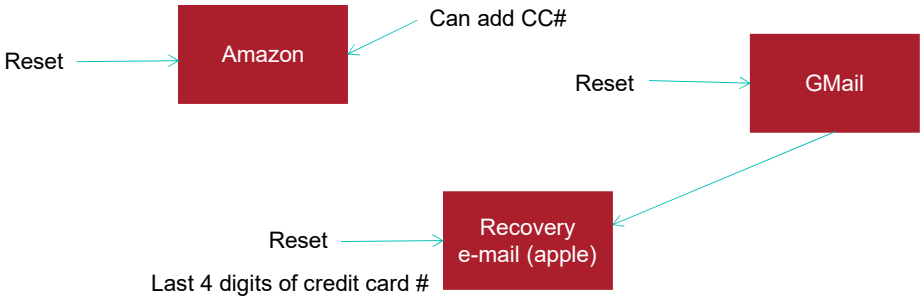
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

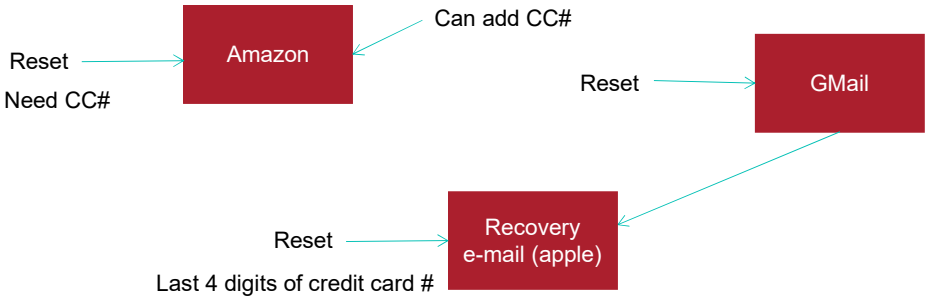
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

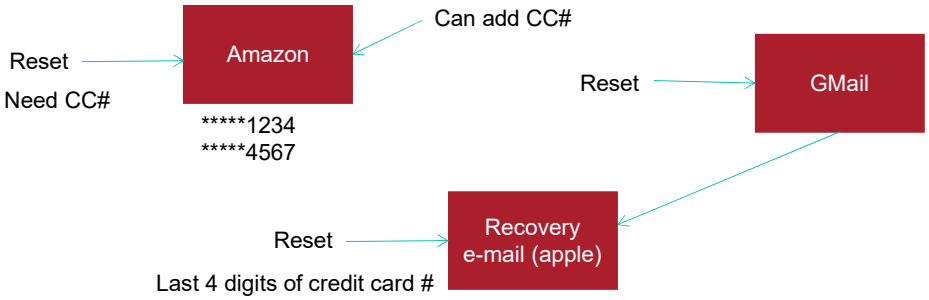
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

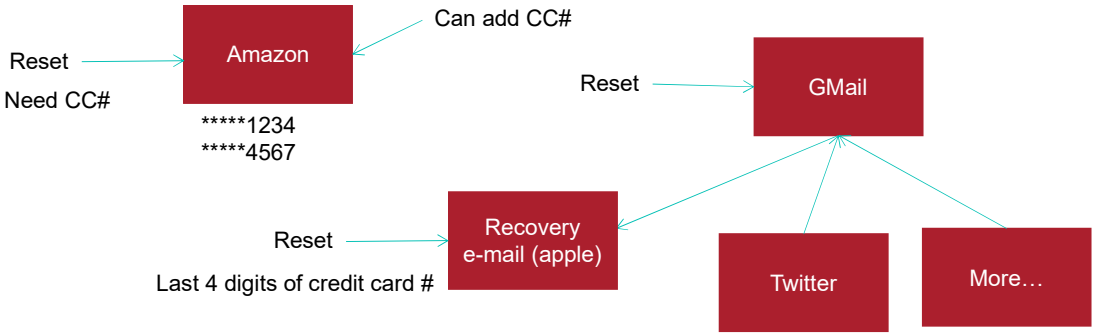
- Took over twitter account, deleted google account etc.



bristol.ac.uk

What happened?

- Took over twitter account, deleted google account etc.



bristol.ac.uk

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?

bristol.ac.uk

University of BRISTOL

Thank you

bristol.ac.uk