University of BRISTOL

Computer Systems B

COMS20012

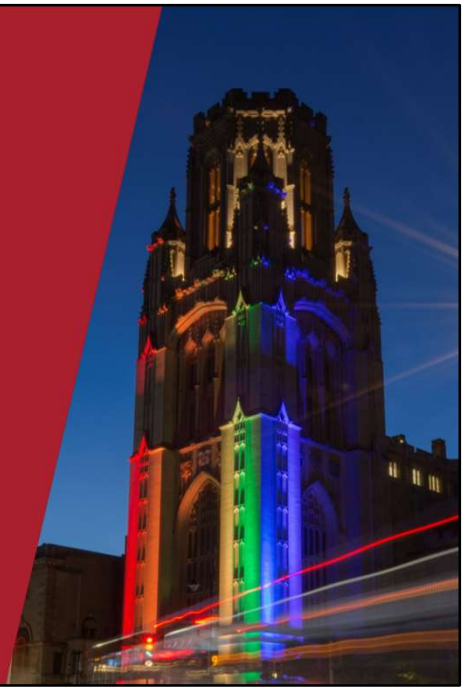
Introduction to Operating Systems and Security

bristol.ac.uk

University of BRISTOL

Threat 3

Man in the middle



bristol.ac.uk

Transmit password

- In the clear?

bristol.ac.uk

Transmit password

- In the clear?
  - Just need to listen on network packet…

bristol.ac.uk

Transmit password

- In the clear?
- Over encrypted connection?

bristol.ac.uk

Transmit password

- In the clear?
- Over encrypted connection?
  - Man in the middle attack
  - Need to authenticate the server (e.g. Am I really talking to google?)

bristol.ac.uk

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?

bristol.ac.uk

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
  - Does not make a difference!

bristol.ac.uk

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
- Challenge response protocol?

bristol.ac.uk

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
- Challenge response protocol?
  - Bob can verify Alice know the secret
  - If someone pretend to be Bob he cannot know the password

bristol.ac.uk

Transmit password

- In the clear?
- Over encrypted connection?
- Send the hash?
- Challenge response protocol?
  - Bob can verify Alice know the secret
  - If someone pretend to be Bob he cannot know the password
  - Naïve (more in a future video)

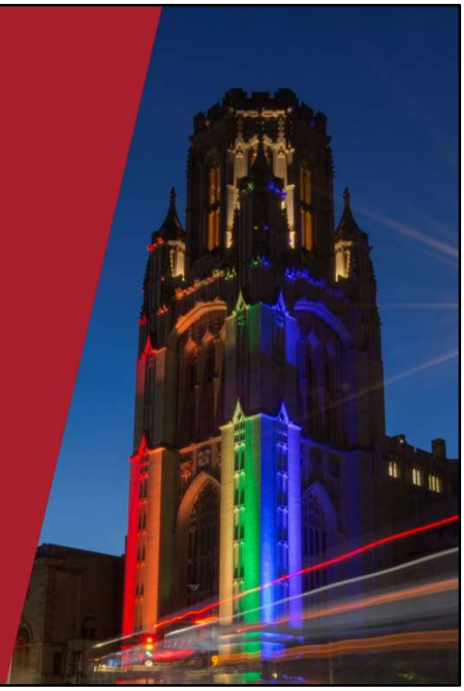
Discussed further in future video

bristol.ac.uk

University of BRISTOL

Threat 4

"Hammering" the login page



bristol.ac.uk

Anti-hammering defences

- Rate-limit
  - Number of guess, then password revoked
- Time-outs
  - e.g. prevent to login within the next hours
- Why is it important?

bristol.ac.uk

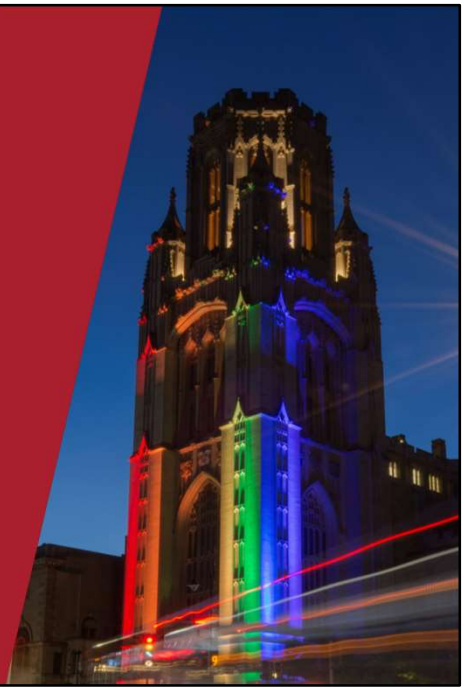
Anti-hammering defenses

- Rate-limit
  - Number of guess, then password revoked
- Time-outs
  - e.g. prevent to login within the next hours
- Why is it important?
  - Password have very low entropy!
  - Need to prevent brute forcing

bristol.ac.uk

University of BRISTOL

Thank you



bristol.ac.uk