University of BRISTOL

Computer System B

bristol.ac.uk

bristol.ac.uk

The Plan for CSB

Syllabus CSB

- Intro to general security
- Intro to Network Security
- Network Security
- Web Security + Firewalls
- Private networks
- Intro to Software Security
- Intro to OS + File System
- Memory management
- Large org in real world*

The Exam

- **Final exam is 100% of the grade!**
- **Everything we cover (lectures, labs, exercises) is a part of the exam!**

Today!

- Motivation for Cybersecurity
- CIA
- Authentication
- Authorization
- Accountability

bristol.ac.uk

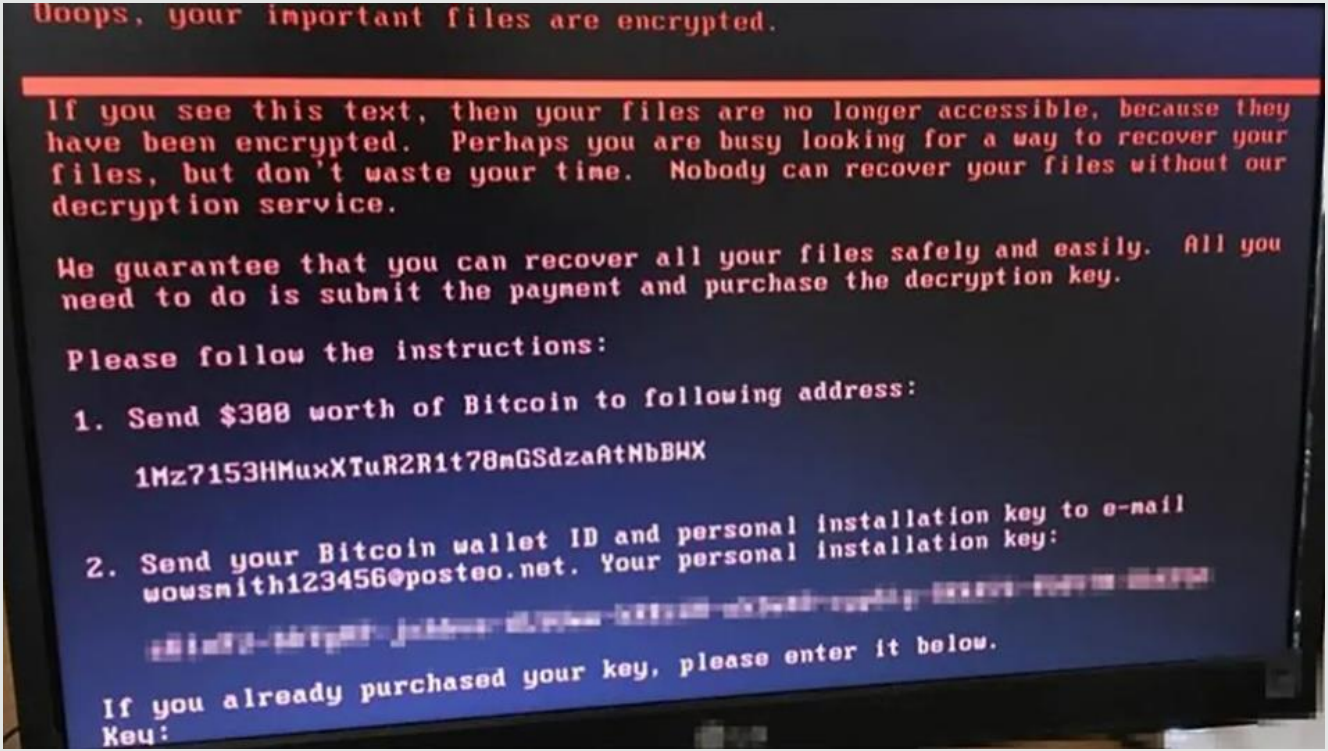
What is cybersecurity?

Computer Security

- The NIST *Computer Security Handbook* defines the term computer security as:

  "the 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)

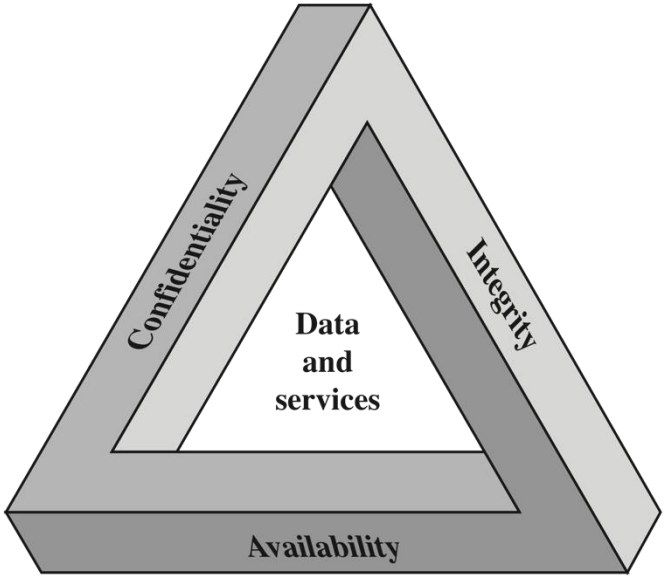

Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
If you already purchased your key, please enter it below.
Key:

NotPetya

Why do we need cybersecurity?


CYBER SECURITY
Application
Information
Network
Operational
Encryption
Access control
End-user education
Disaster recovery

CIA Triad


Confidentiality
Integrity
Data
and
services
Availability

Computer Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

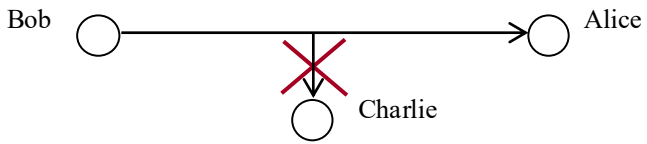
Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

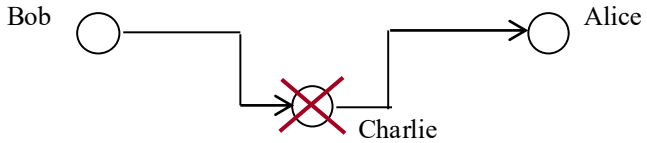
Availability

- Assures that systems work promptly and service is not denied to authorized users

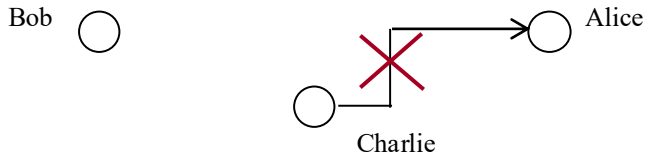
1. Confidentiality



2. Message integrity



3. Message authentication



Possible additional concepts:

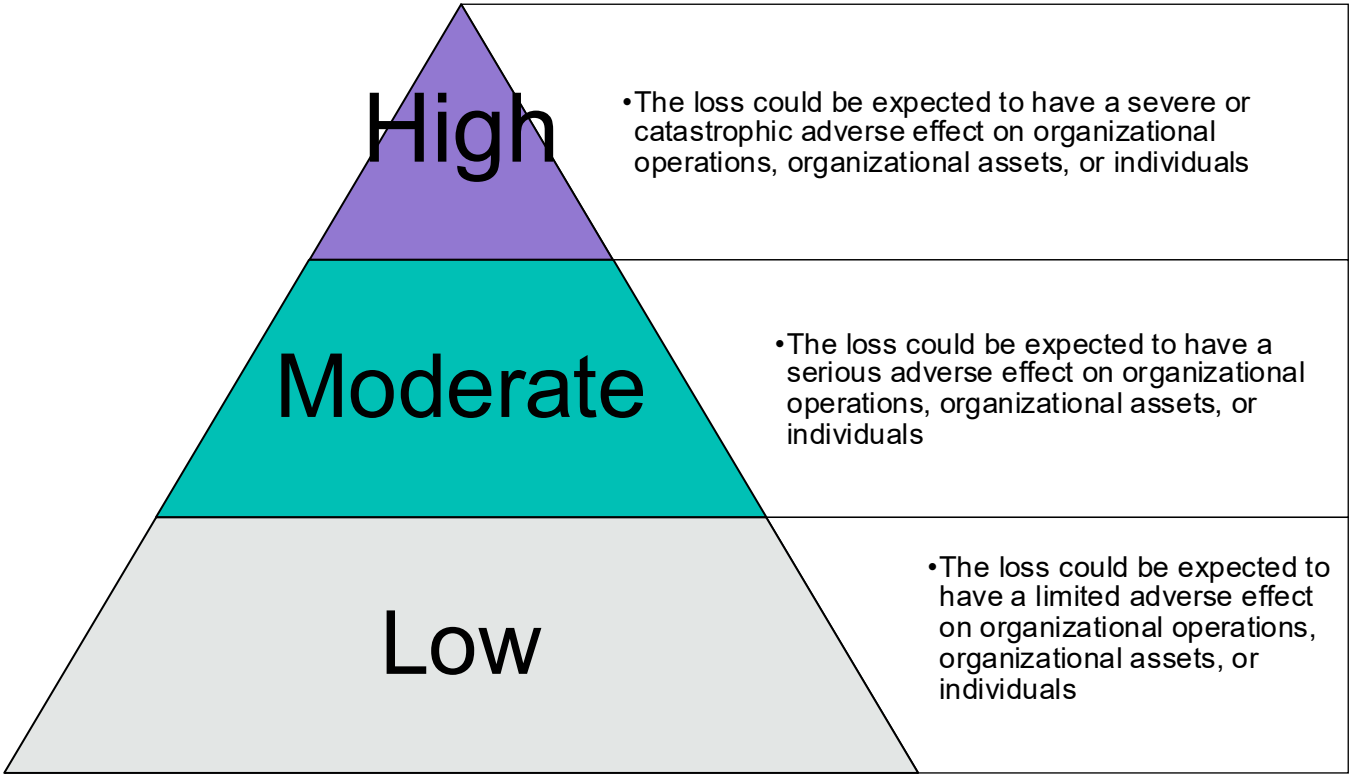
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Breach of Security Levels of Impact

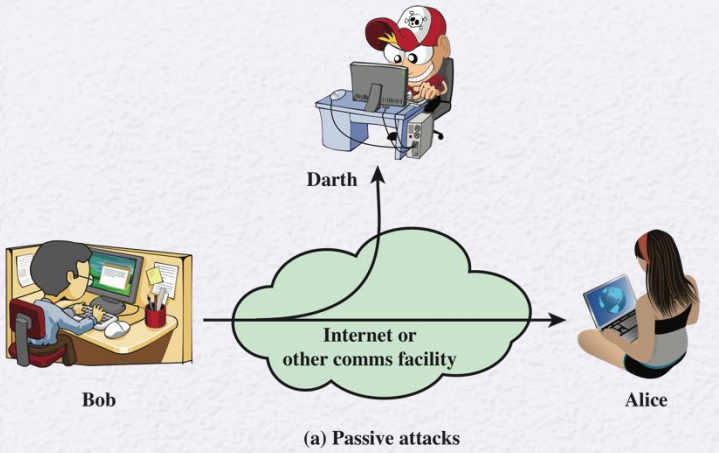


OSI Security Architecture

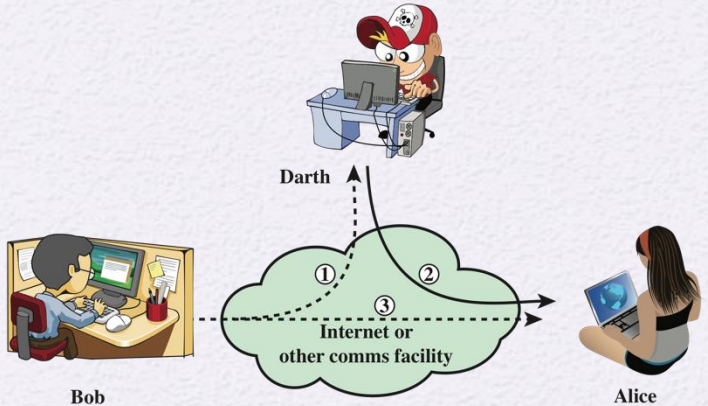
- Security attack
  - Any action that compromises the security of information owned by an organization
- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- Security service
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
  - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation



(a) Passive attacks



(b) Active attacks

Figure 1.1 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

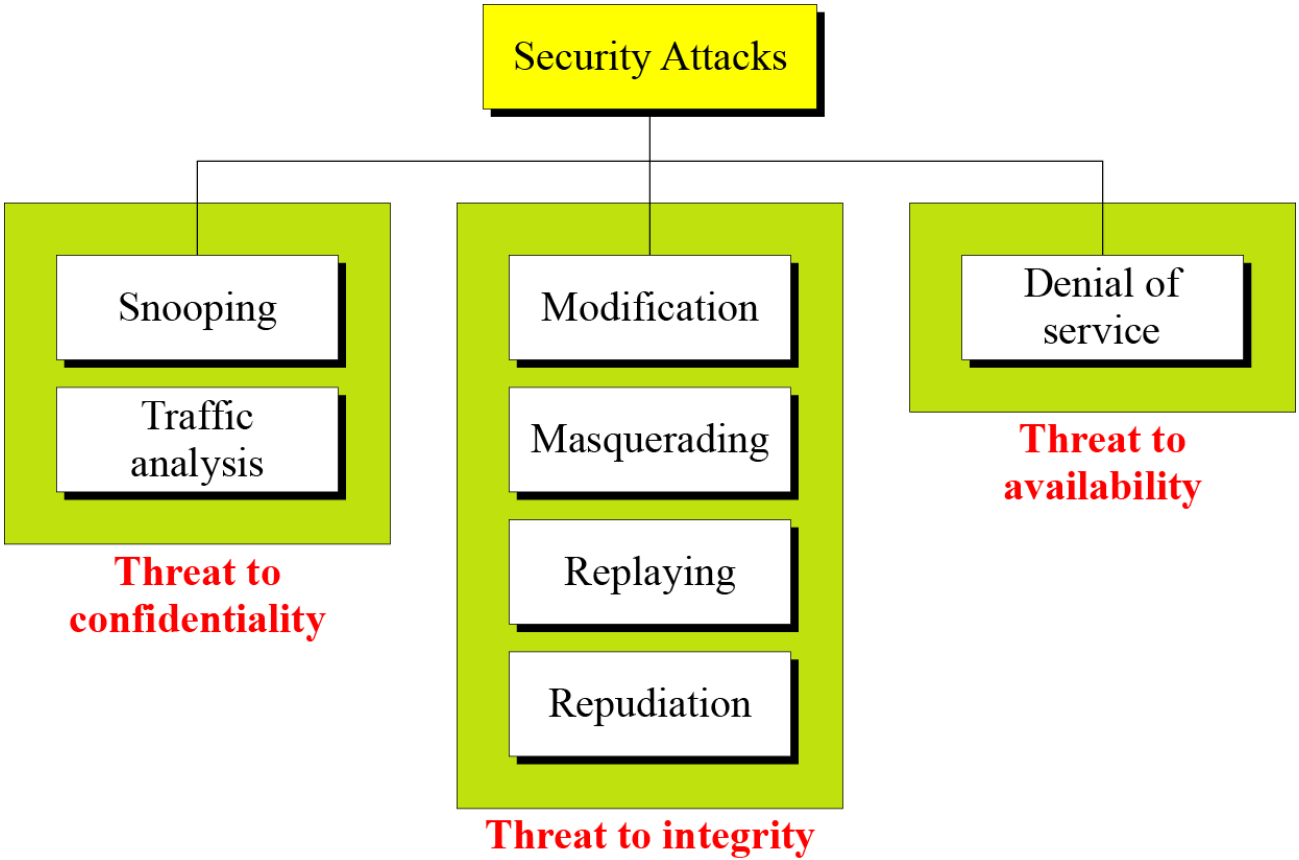
- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis

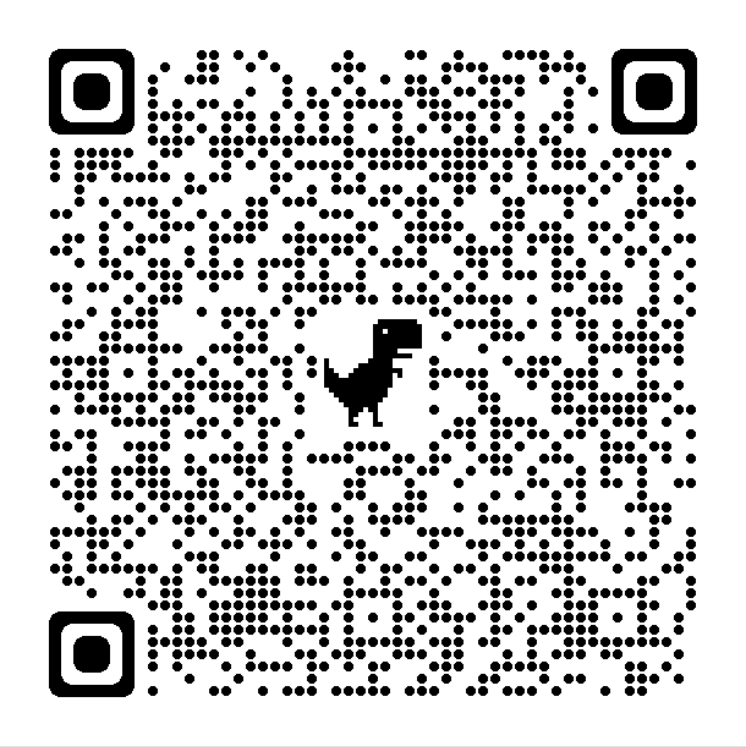
Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

bristol.ac.uk

Masquerade	• Takes place when one entity pretends to be a different entity • Usually includes one of the other forms of active attack
Replay	• Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
Modification of messages	• Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect
Denial of service	• Prevents or inhibits the normal use or management of communications facilities


Security Attacks
Snooping
Traffic analysis
Threat to confidentiality
Modification
Masquerading
Replaying
Repudiation
Threat to integrity
Denial of service
Threat to availability



bristol.ac.uk

Authentication:

***Or* who are you?**

Authorization:

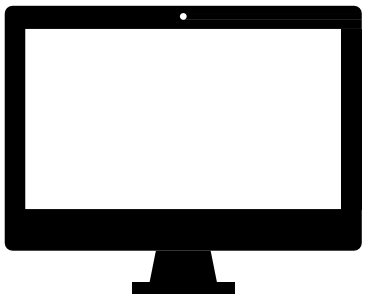
***Or* what can you do?**

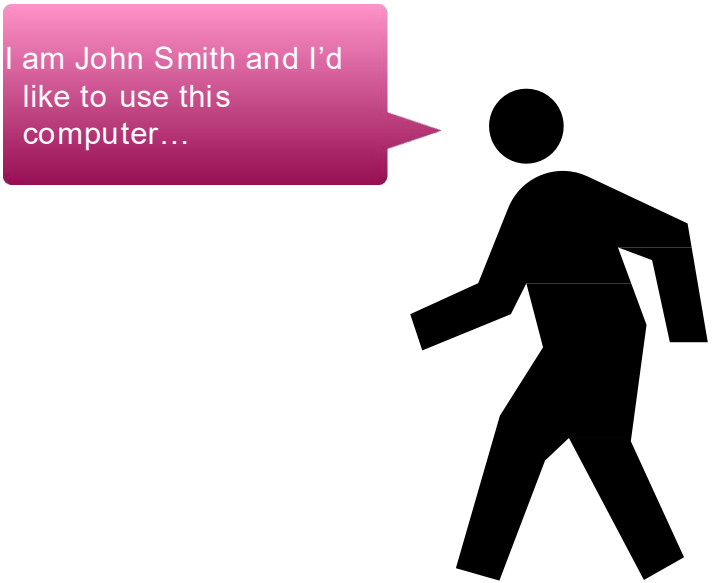
Accountability:

***Or* who did what?**

Authentication

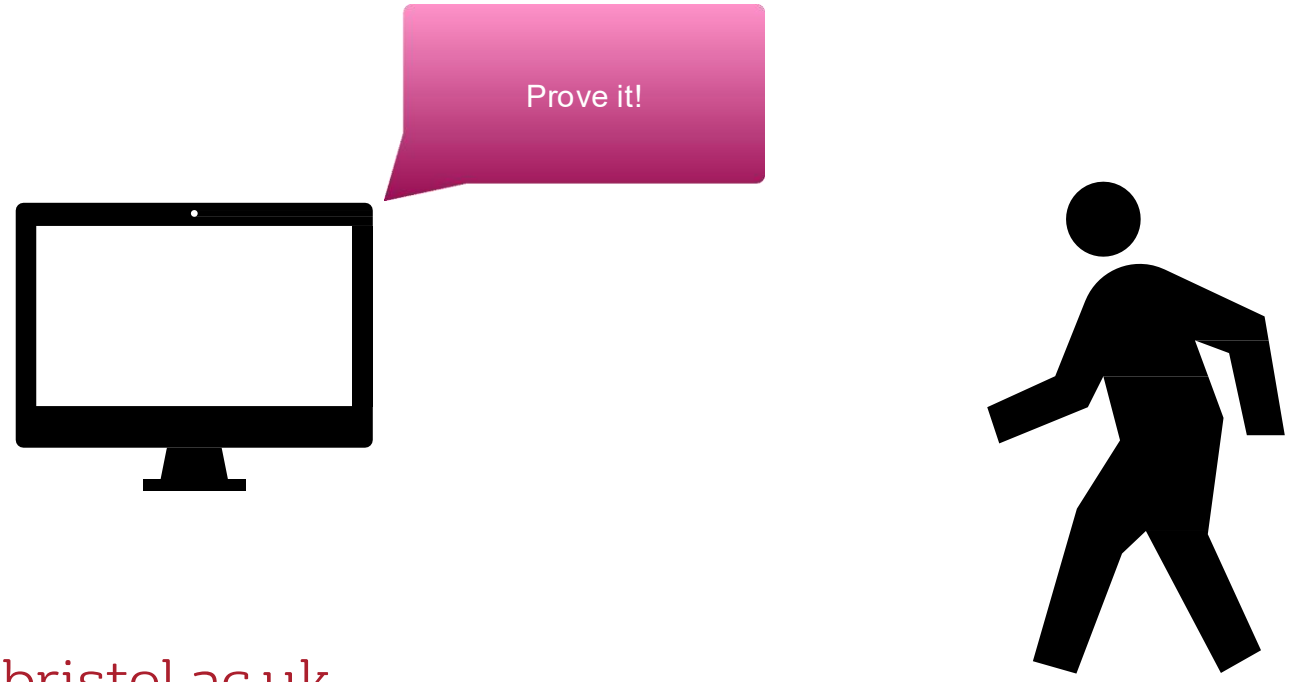
Who are you?





Authentication

Who are you?



Authentication

3 Basic Mechanisms

Something you know

- Passwords

Something you have

- Keys

Something you are

- Biometrics and behaviours

Authentication

3 Basic Mechanisms

Something you know

- Passwords

Something you have

- Keys

Multi-factor authentication

Something you are

- Biometrics and behaviours

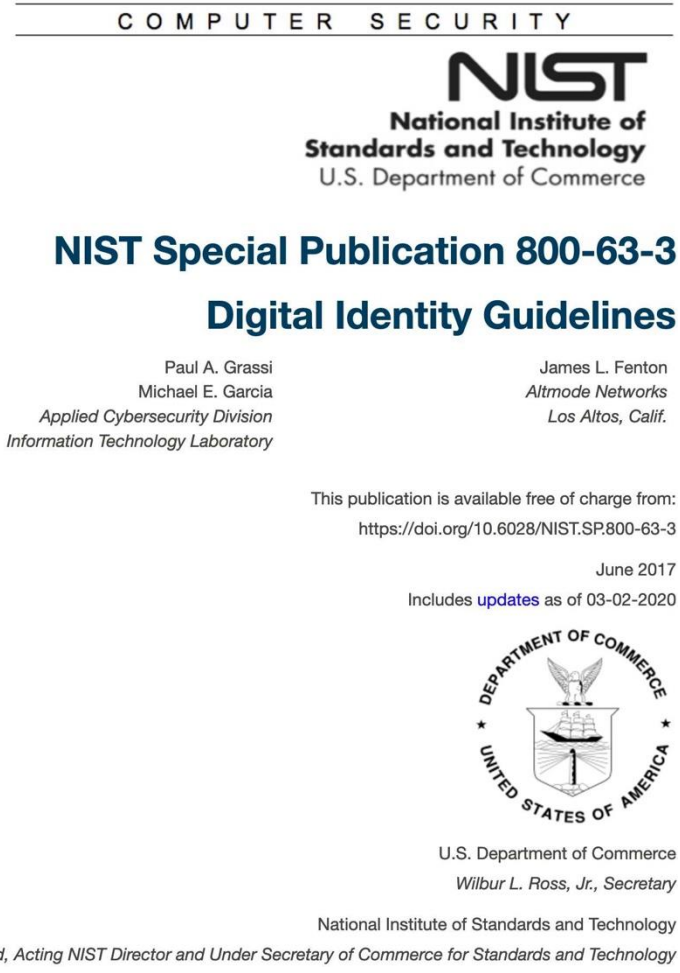
Authentication

Passwords and gotchas

Storing passwords isn't hard
…but everyone gets it wrong.

Just go look up what current best practice is.

(Randomize the salt, 1024 rounds of bcrypt…)



COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017

Includes updates as of 03-02-2020

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authentication

Keys

Something you have!

Typically a digital signature of some kind…

- PGP is hard (-ish)

What happens if you lose it?

Authentication

Biometrics

Something you are!

Track something about a person…

- Gait… mouse movements… usage patterns
- Build a machine learning model about it

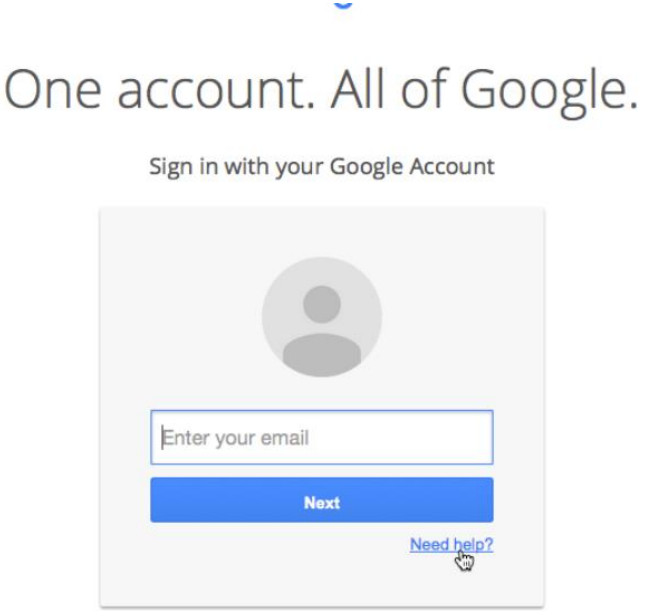
- How do you repudiate your fingerprints?
- How do you handle accessibility?

Authentication
Federated Identity Management

Delegate to someone else for your identity management!

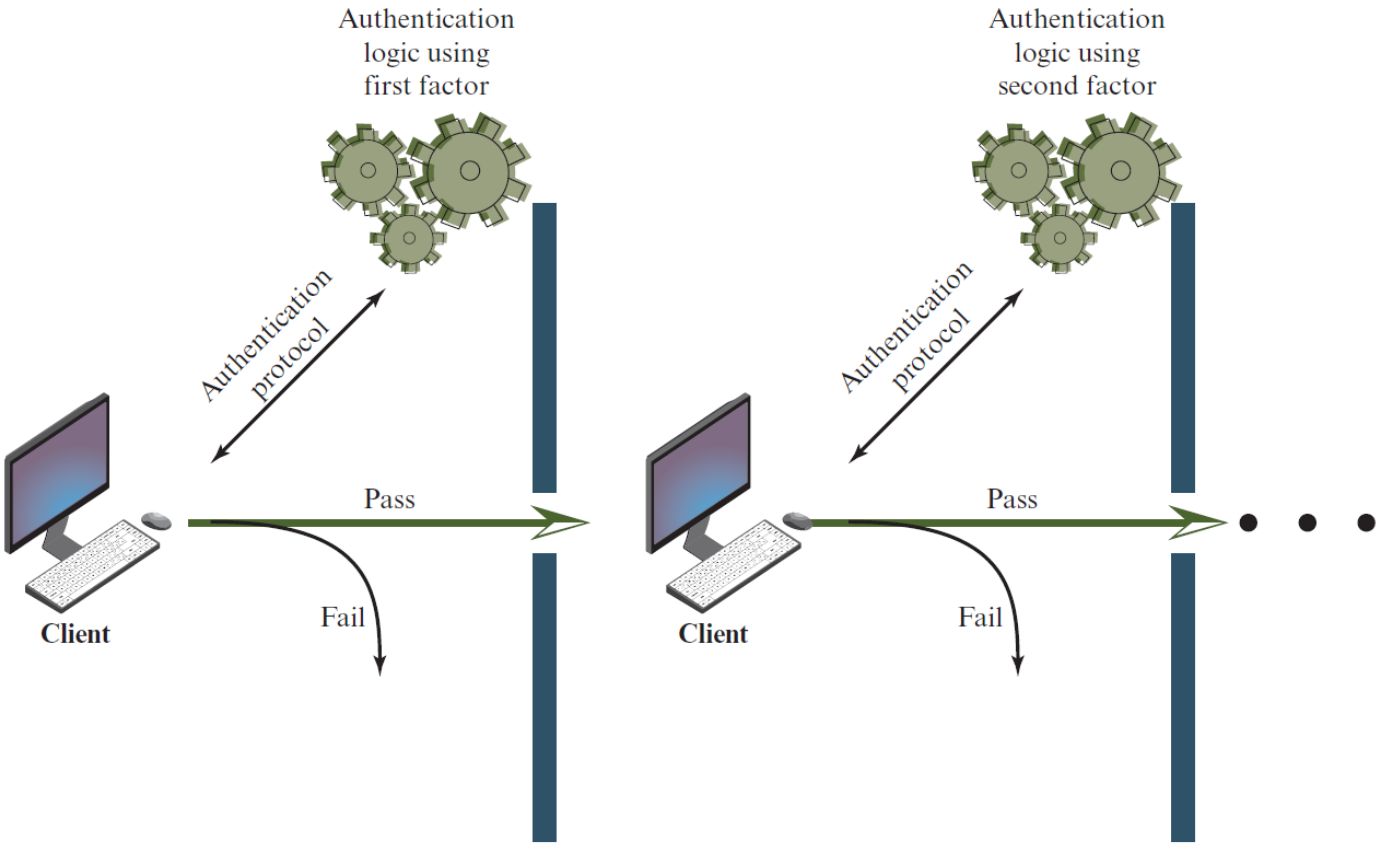
- Great for organisations
  - …centralised employee management!
- Great for amateur developers
  - …less to get wrong/GDPR compliance!
- Bad for privacy
  - …if you lose access to your Google account you lose access to EVERY connected service.

Kerberos, LDAP, OAuth2…

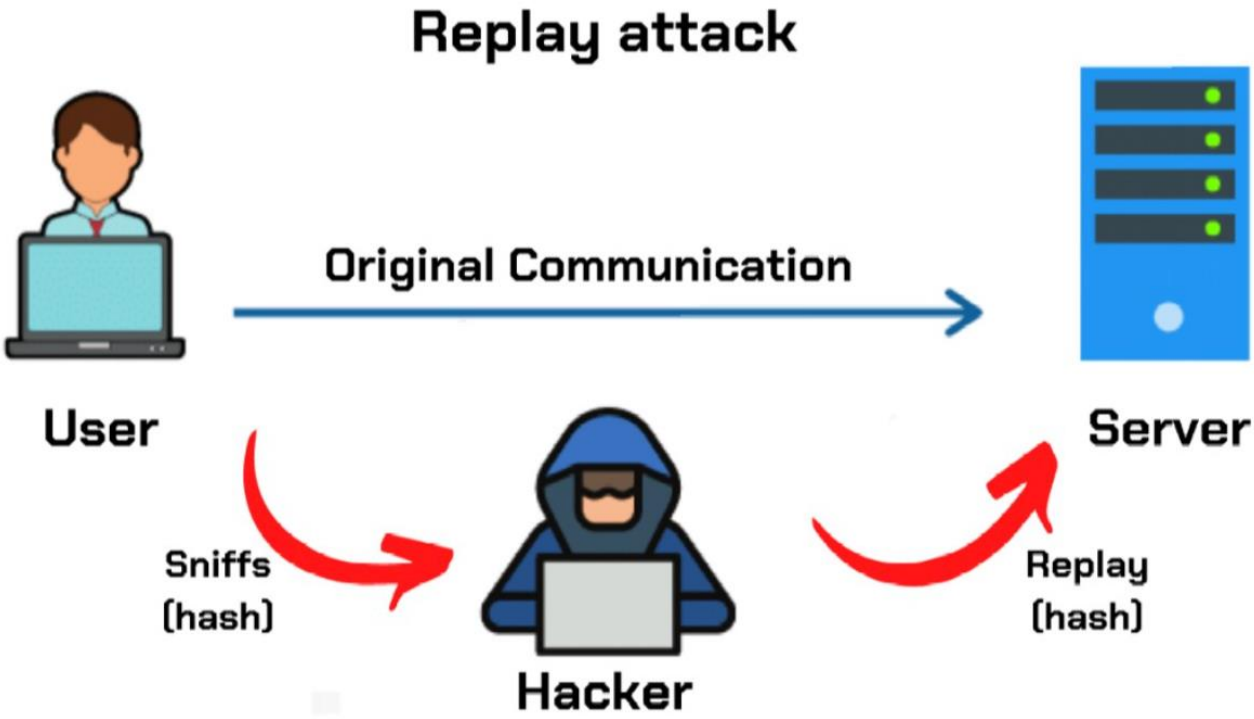


Authentication factors

Factor	Examples	Properties
Knowledge	User ID Password PIN	Can be shared Many passwords easy to guess Can be forgotten
Possession	Smart Card Electronic Badge Electronic Key	Can be shared Can be duplicated (cloned) Can be lost or stolen
Inherence	Fingerprint Face Iris Voice print	Not possible to share False positives and false Negatives possible Forging difficult


Authentication logic using first factor
Authentication protocol
Pass
Fail
Client
Authentication logic using second factor
Authentication protocol
Pass
Fail
Client

What can go wrong?


Replay attack
Original Communication
User
Server
Sniffs
(hash)
Hacker
Replay
(hash)

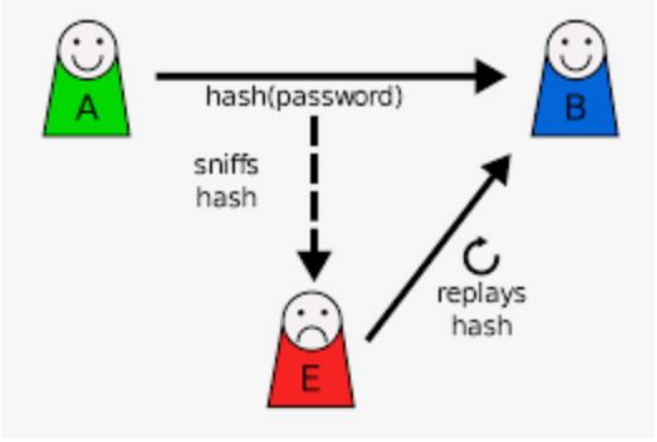
Replay attack

The simplest replay attack is one in which the opponent simply copies a message and replays it later.

An opponent can replay a timestamped message within the valid time window.

An opponent can replay a timestamped message within the valid time window, but in addition, the opponent suppresses the original message; thus, the repetition cannot be detected.

Another attack involves a backward replay without modification and is possible if symmetric encryption is used and the sender cannot easily recognize the difference between messages sent and messages received on the basis of content.

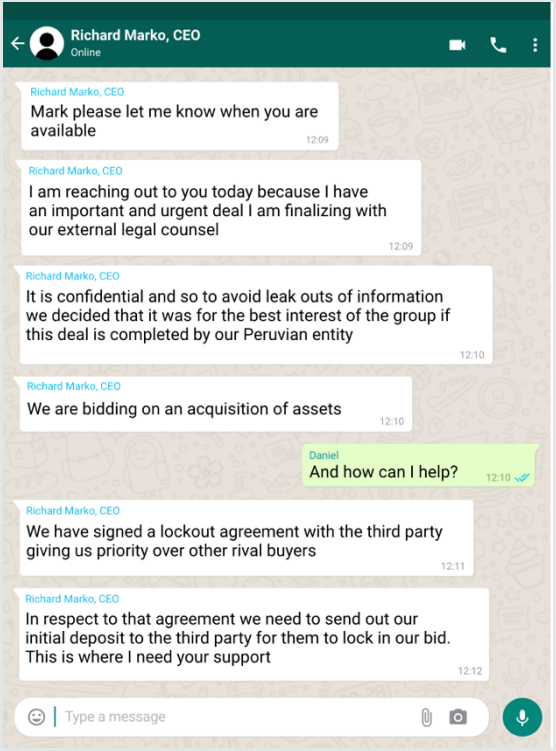


Impersonation attack

Cybercriminals usually **replay authentication sessions**, which give attackers full control of your accounts and all the privileges you enjoy on specific websites or apps.

They can **impersonate you** online, **send and receive messages on your behalf**, and **access confidential data** or documents.

Impersonation



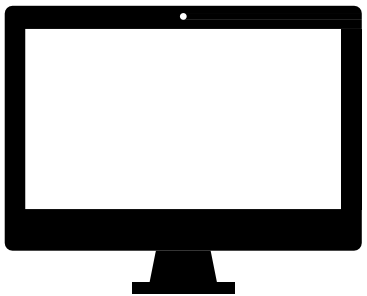
Impersonation

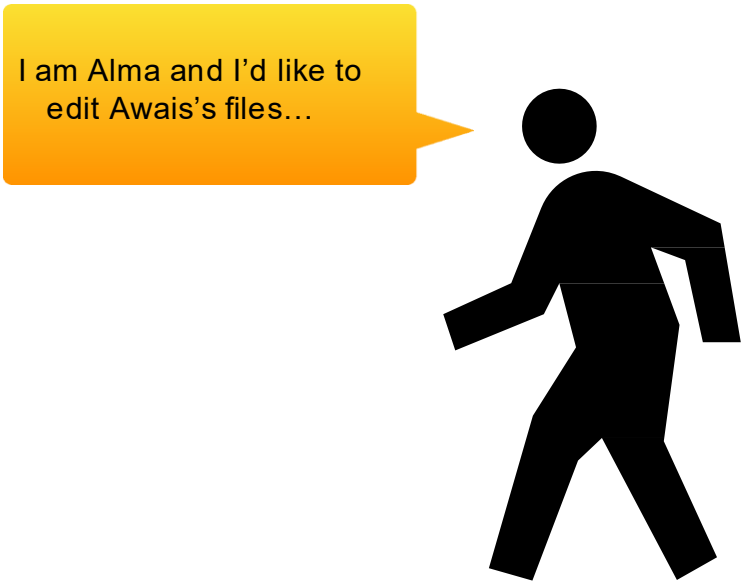
Authorization:

***Or* what can you do?**

Authorization

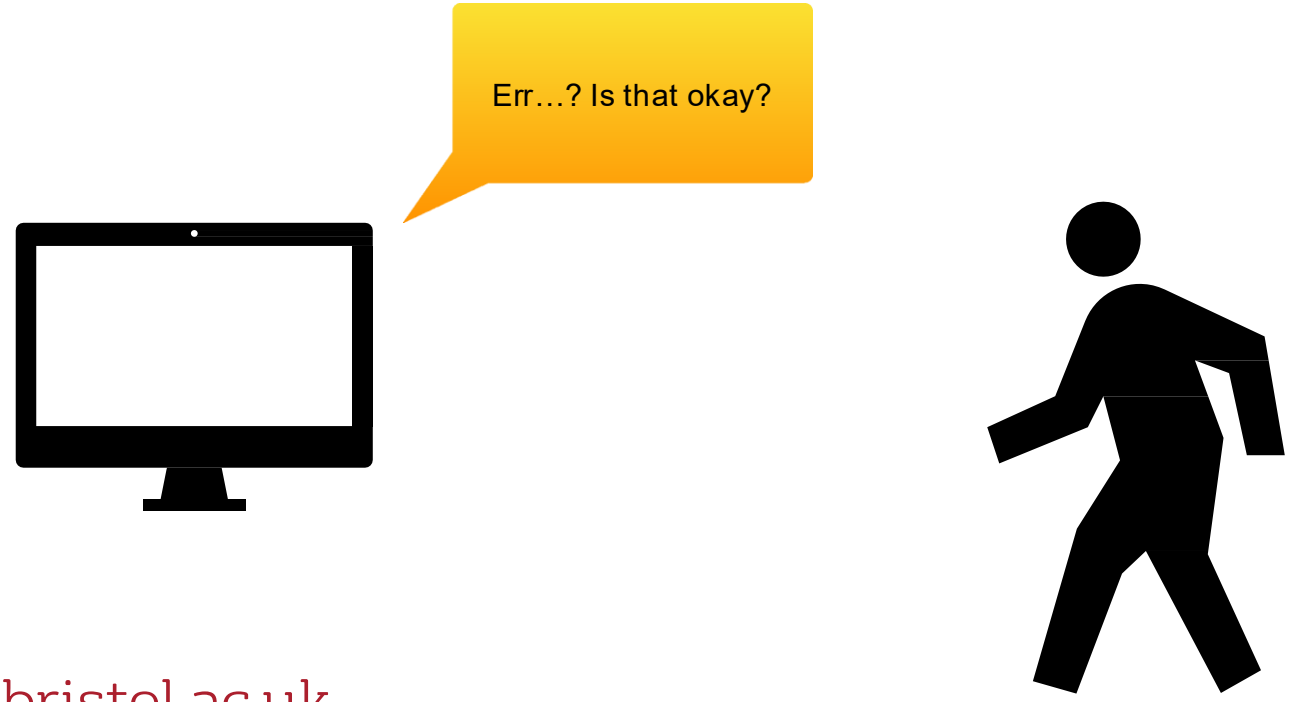
What can you do?





Authorization

What can you do?



Authorization

Distributed Access Control

Sometimes it'd be really nice to get information dynamically from third-parties instead of keeping it locally.

- All *MSc students* can access *MSc Room*
- *MSc manager* can say who's a *MSc Student*
- *Awais* can say whose the *MSc manager*

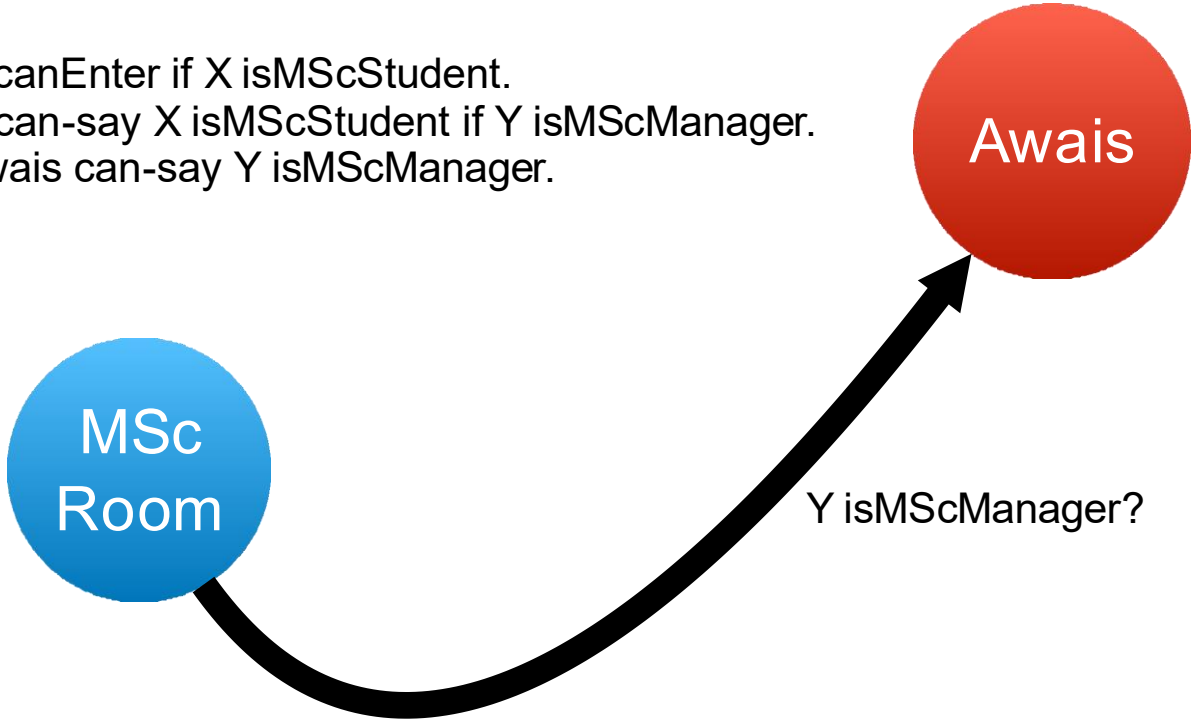
Bob wants to access the MSc room…

?- bob canEnter.

X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.

?- bob canEnter.

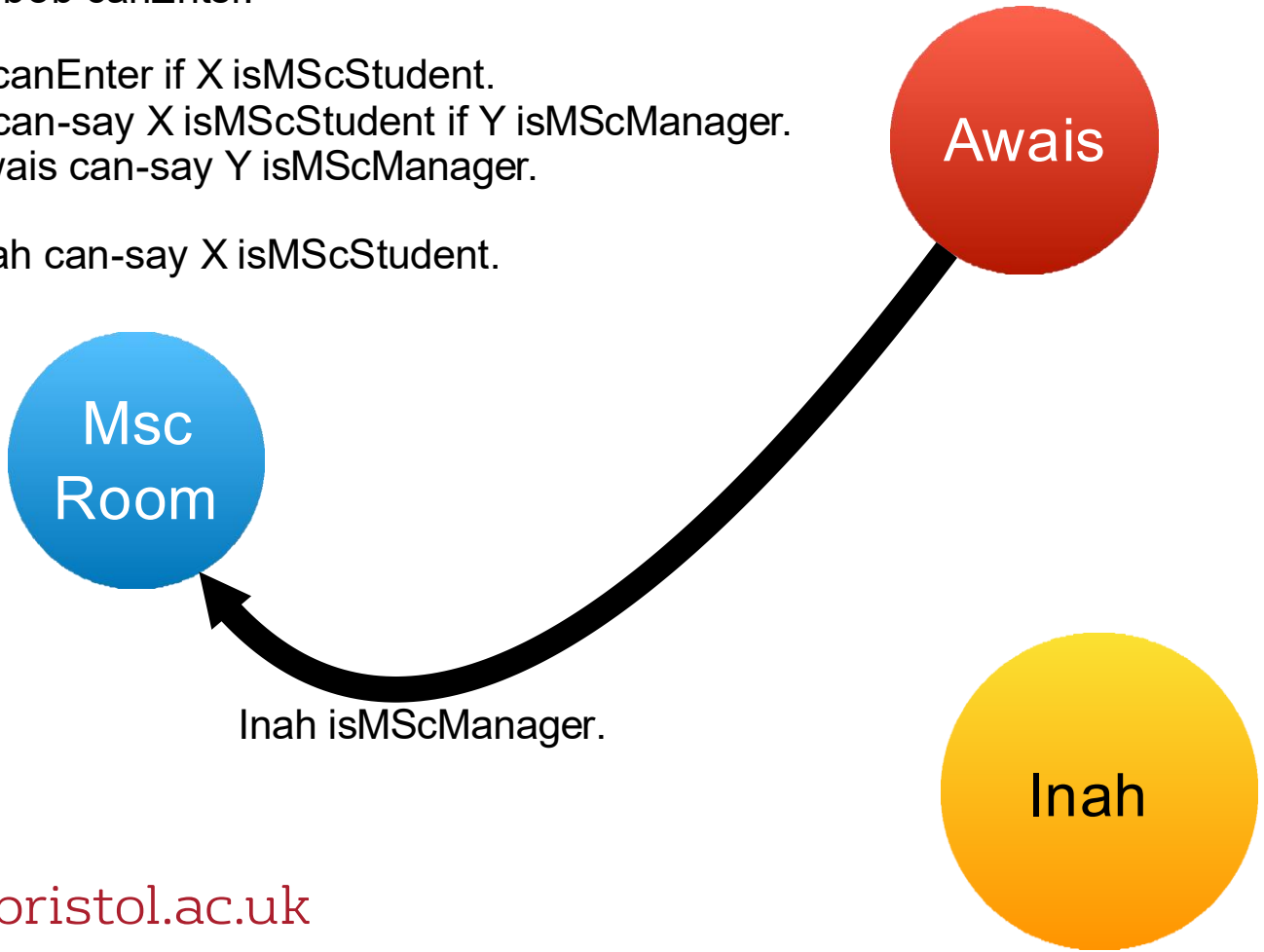
X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.



?- bob canEnter.

X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.

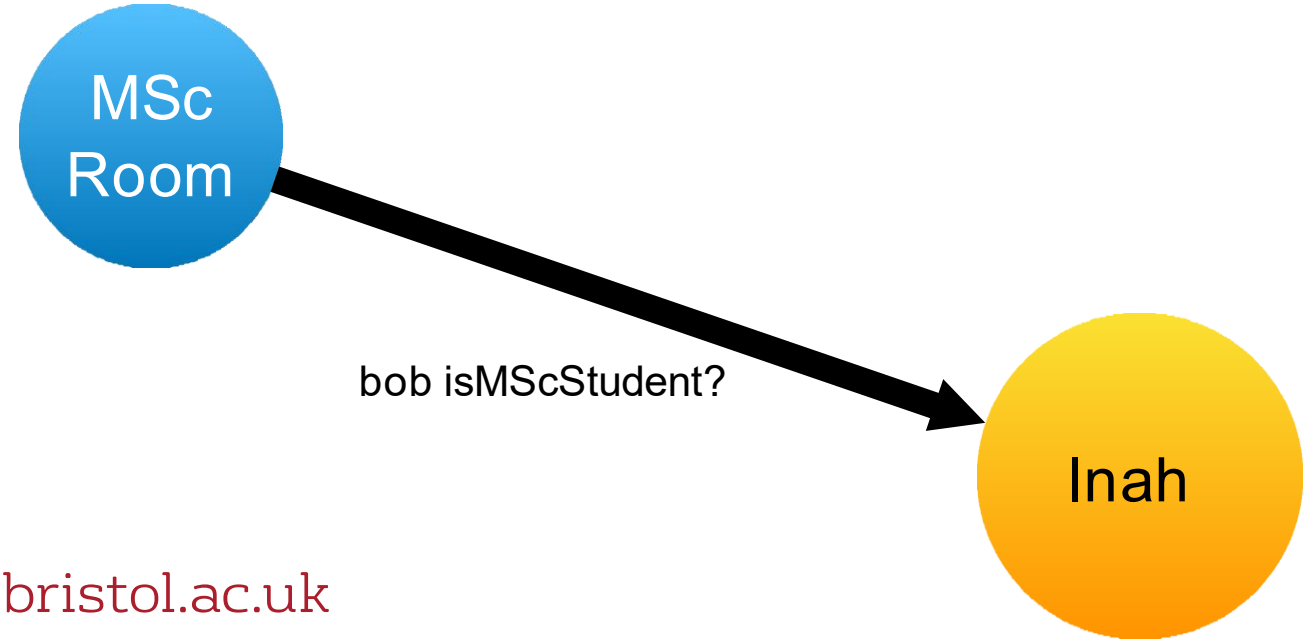
Inah can-say X isMScStudent.



?- bob canEnter.

X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.

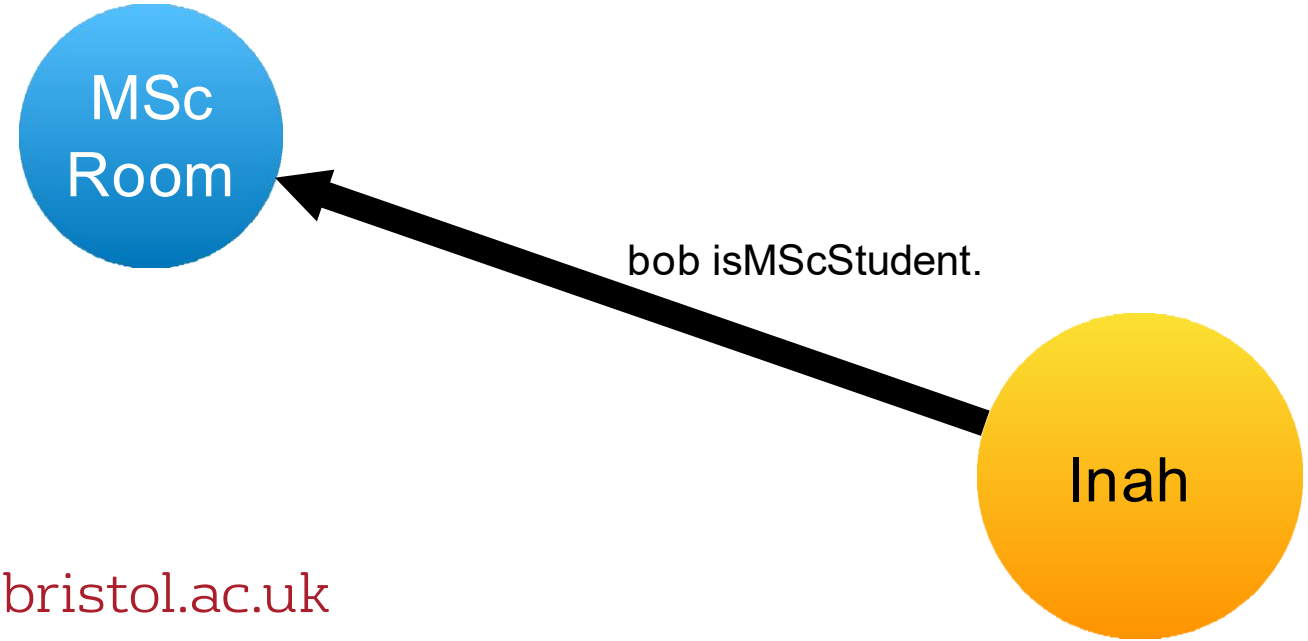
Inah can-say X isMScStudent.



?- bob canEnter.

X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.

Inah can-say X isMScStudent.



?- bob canEnter.

X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.

Inah can-say X isMScStudent. bob isMScStudent.

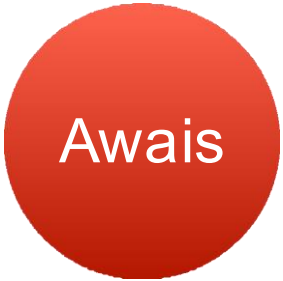
<opens the door>

?- bob canEnter.

X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.

bob canEnter.

<opens the door>

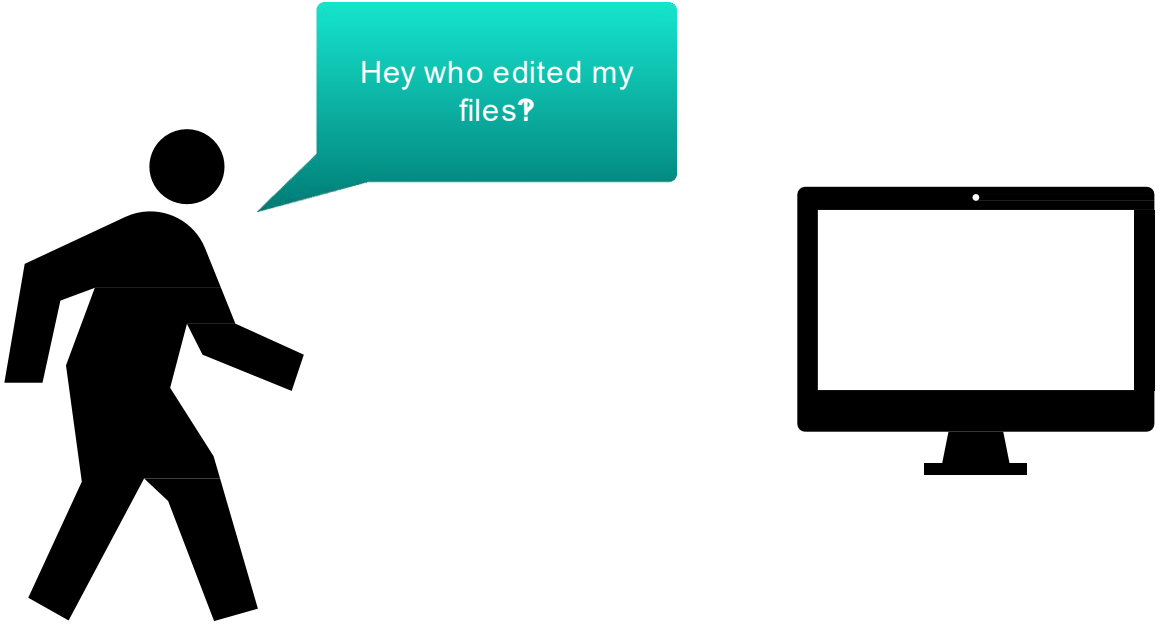


Accountability:

***Or* who did what?**

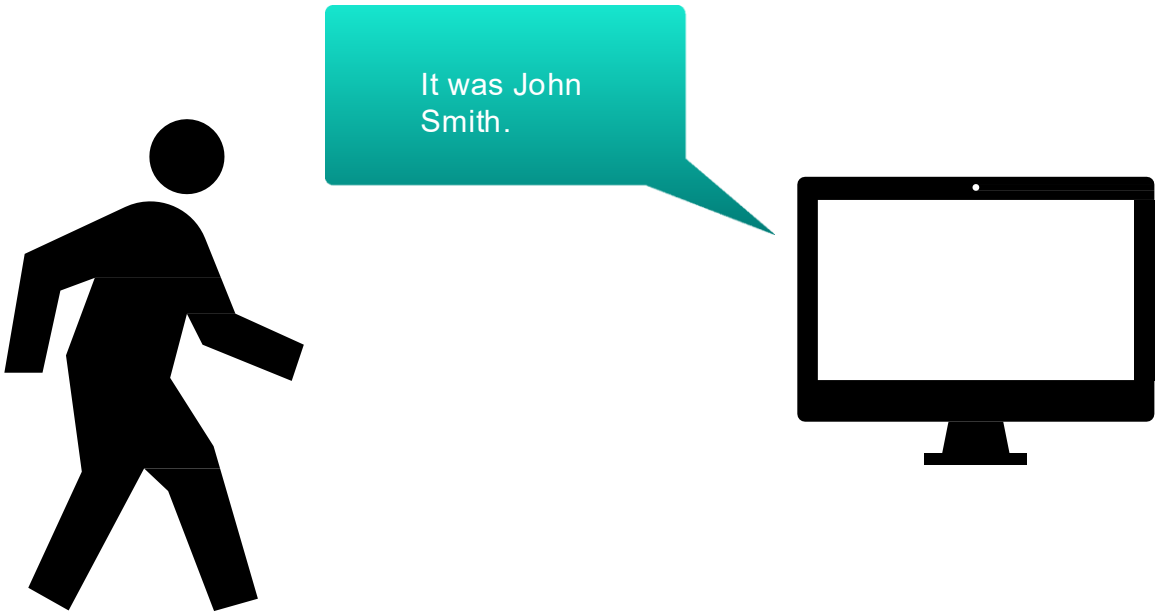
Accountability

Who did what



Accountability

Who did what




Logs

Accountability

Logging

Log as much as you can

- But don't be evil

Keep the logs *append* only

- And get them off the machine ASAP
- Hackers like to delete/modify logs

Standard-ish log formats

```
127.0.0.1 [01/Dec/2020:13:55:36 -0000] "GET /slides HTTP/1.0" 200 4007
```

Accountability

Proof Carrying Code / Digital Evidence

Suppose I have some authorisation logic making decisions about who I let in…

Deriving a proof that someone is allowed in can take a lot of time…

But checking a proof can usually be done quickly!

AAA Further Reading

- CyBOK's discussion of AAA is pretty good.
- NCSC Introduction to identity and access management
  - https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management
- Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. 1992. Authentication in distributed systems: theory and practice. *ACM Trans. Comput. Syst.* 10, 4 (Nov. 1992).

What did we learn today?

What is cybersecurity?

CIA

AAA

bristol.ac.uk