University of BRISTOL

Computer System B

Dr. Alma Oracevic
alma.oracevic@bristol.ac.uk

bristol.ac.uk

Who am I to talk about network security?

- PhD – WSN security
- Research on IoT security and many more
- Teaching advance and network security
- Ethical hacking

Who else is with me?

- Dr. Sana Belguith
- Dr. Joseph Hallett
- Guest Lecturer

University of BRISTOL

The Plan for CSB

Intro to general security
Intro to Network Security
Network Security
Web Security +Firewalls
Further Crypto +TLS
Intro to Software Security
Intro to OS +File System
Memory manag.
OS in Details
Large org in real world

bristol.ac.uk

University of BRISTOL

Today!

- Security
- CIA
- Authentication
- Authorization
- Accountability (logs)

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)


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

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

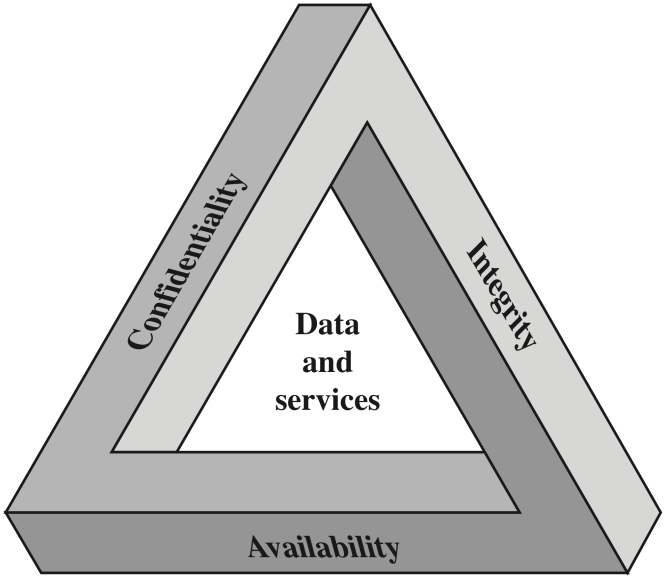
Integrity

- 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

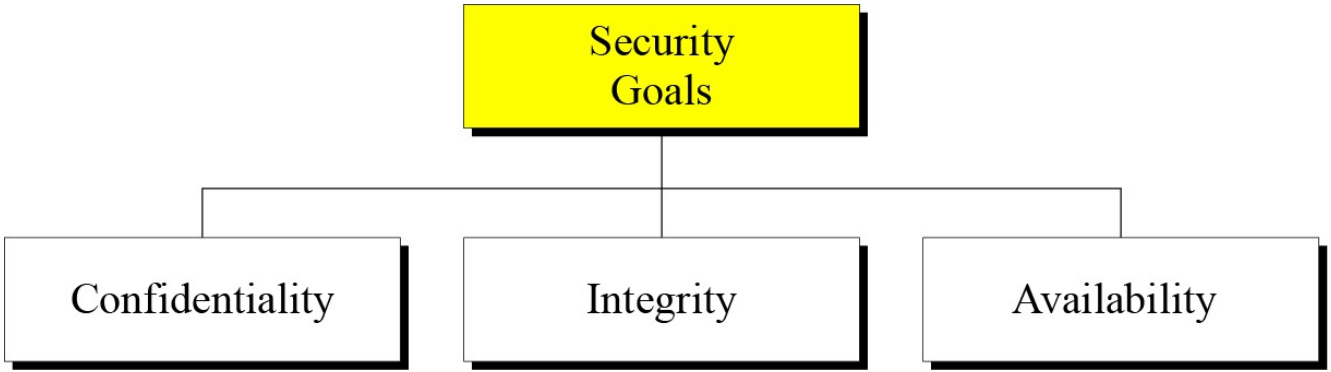
Availability

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

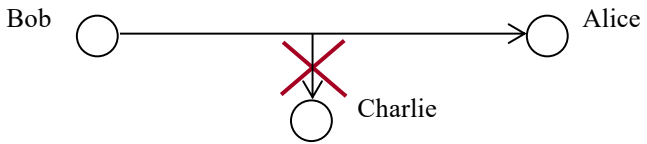
CIA Triad


Confidentiality
Integrity
Data
and
services
Availability

Taxonomy of security goals

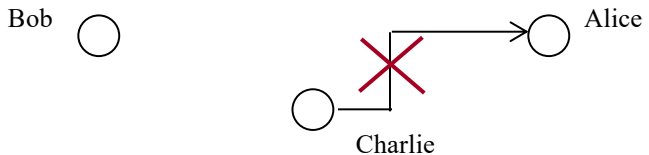


1. Confidentiality



2. Message integrity

3. Message authentication



Possible additional concepts:

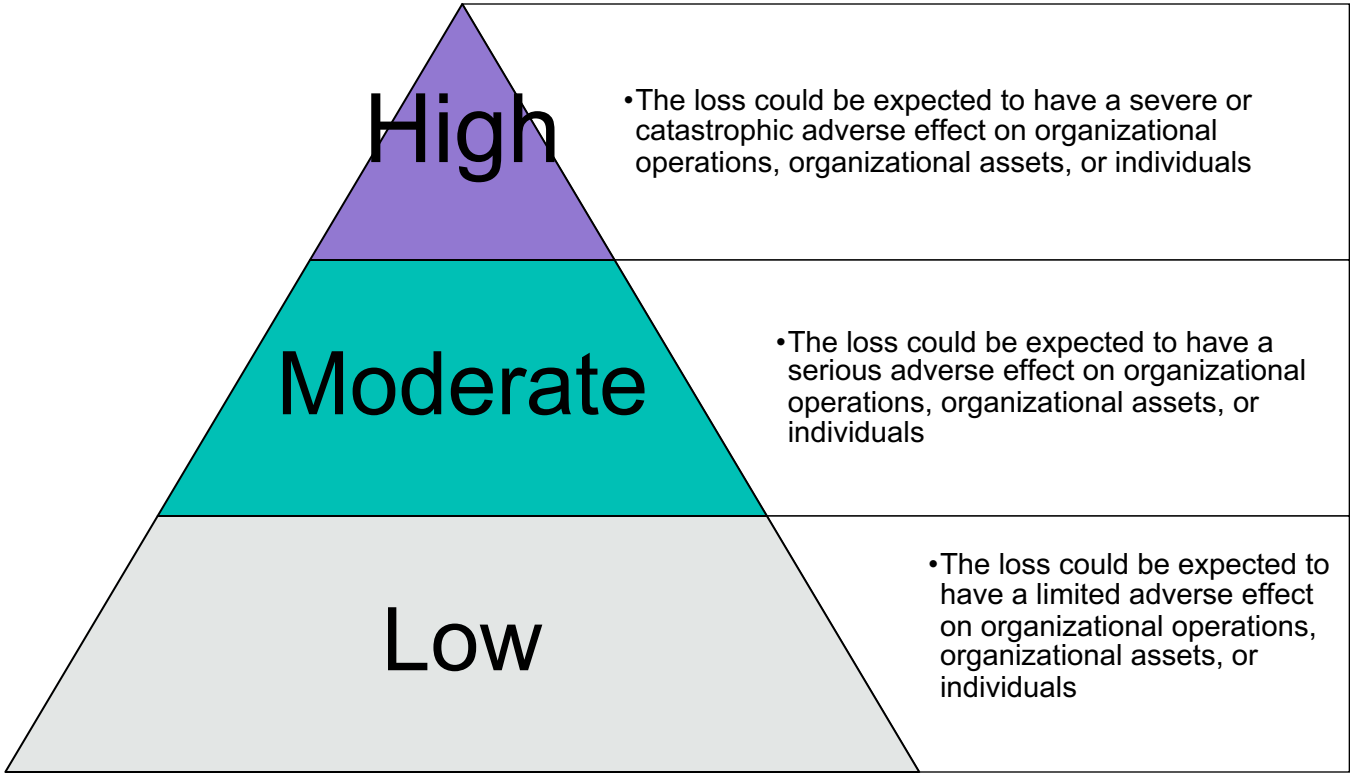
Authenticity

- 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



Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought

- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

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

Threats and Attacks (RFC 4949)

Threat

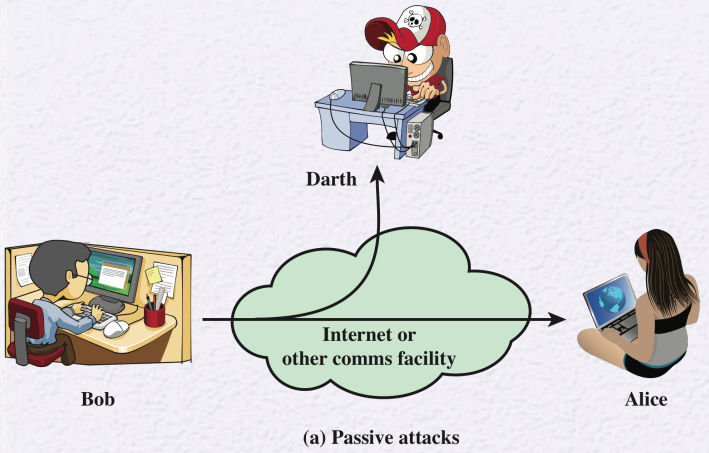
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

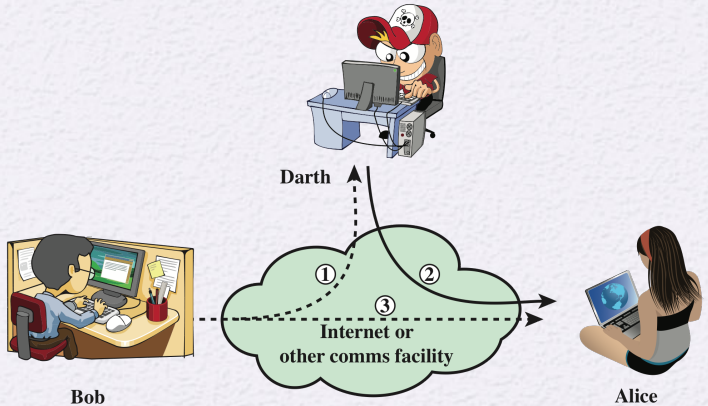
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

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

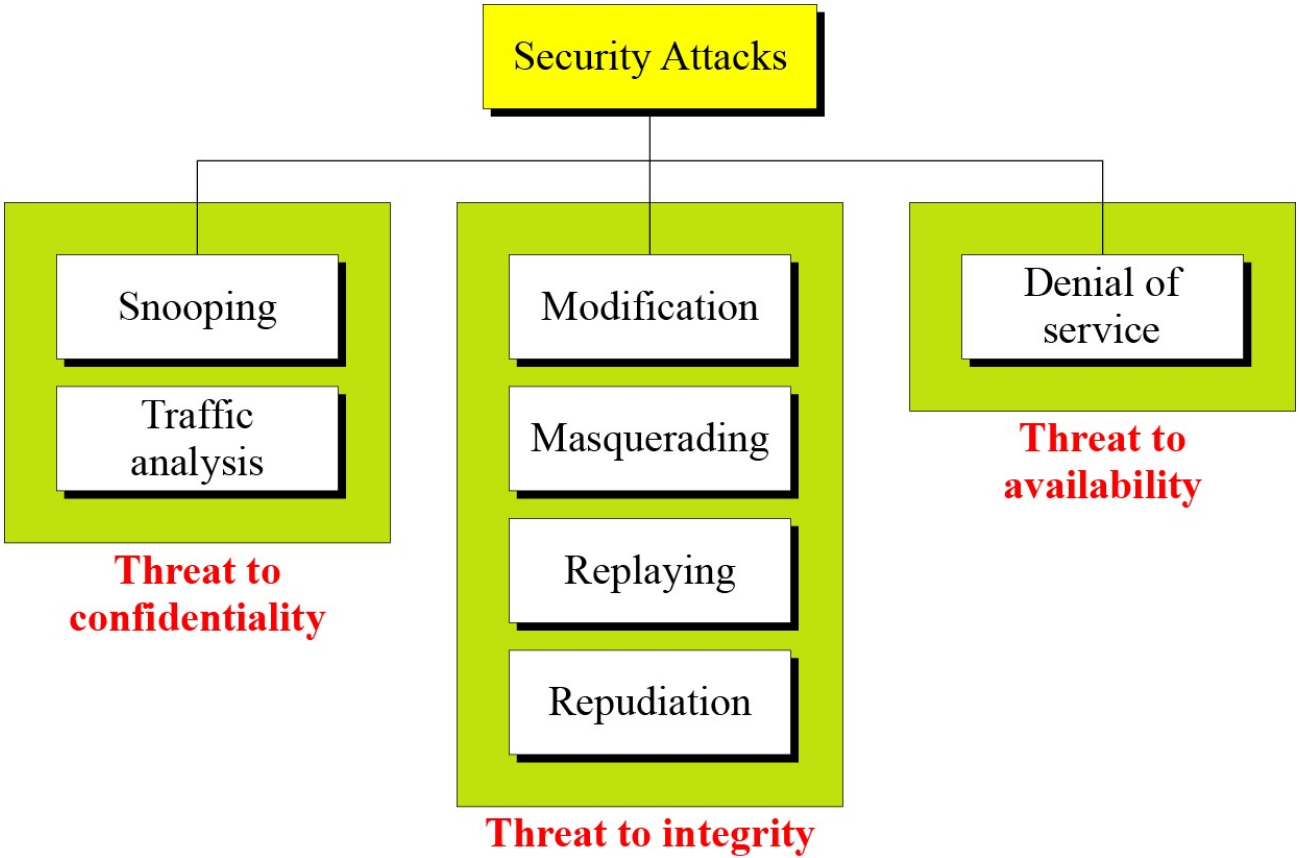
- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis

Active Attacks

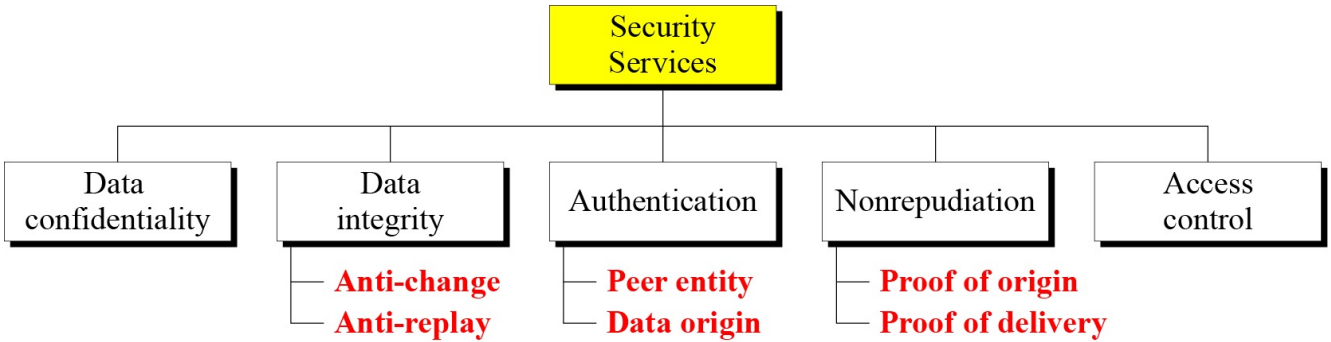
- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

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

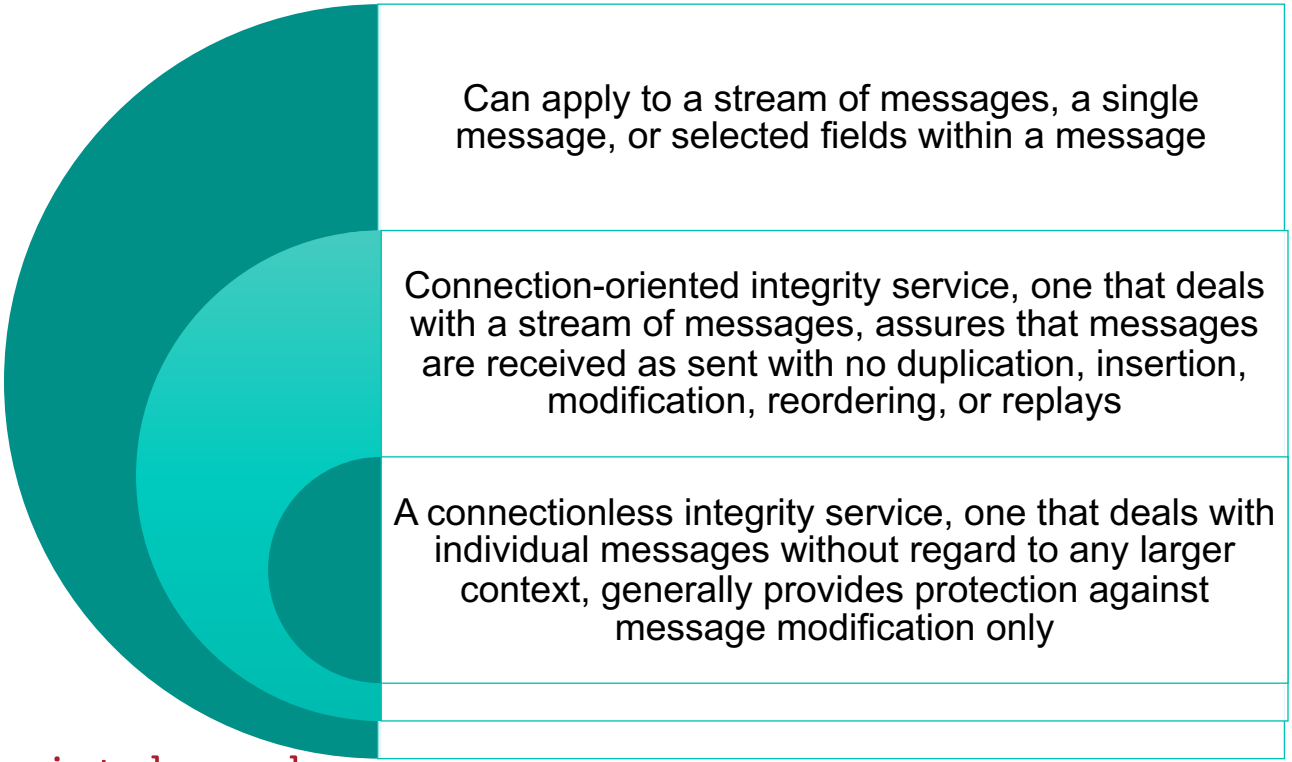
Security services



Data Confidentiality

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time
  - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The protection of traffic flow from analysis
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity



Nonrepudiation

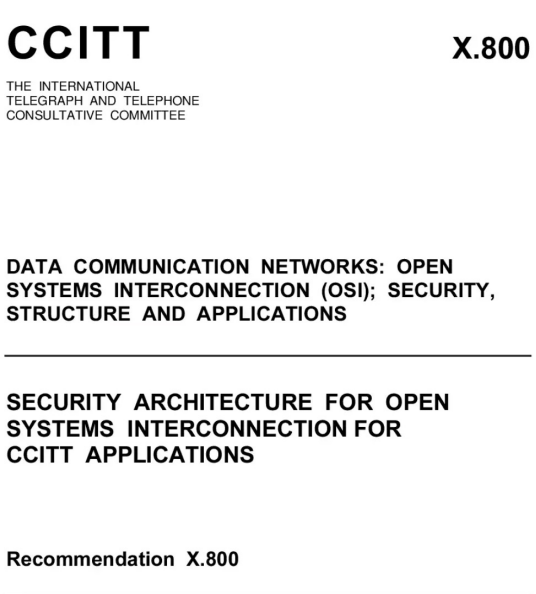
- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

Access Control

- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual

Security Services

- Defined by X.800 as:
  - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers
- Defined by RFC 4949 as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources



CCITT

X.800

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

Recommendation X.800

X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

Authentication:

***Or* who are you?**

Authorization:

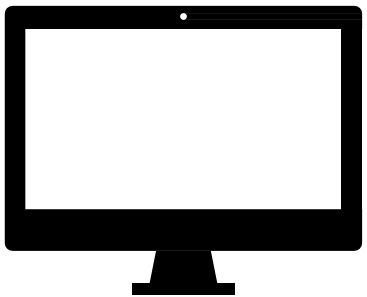
***Or* what can you do?**

Accountability:

***Or* who did what?**

Authentication

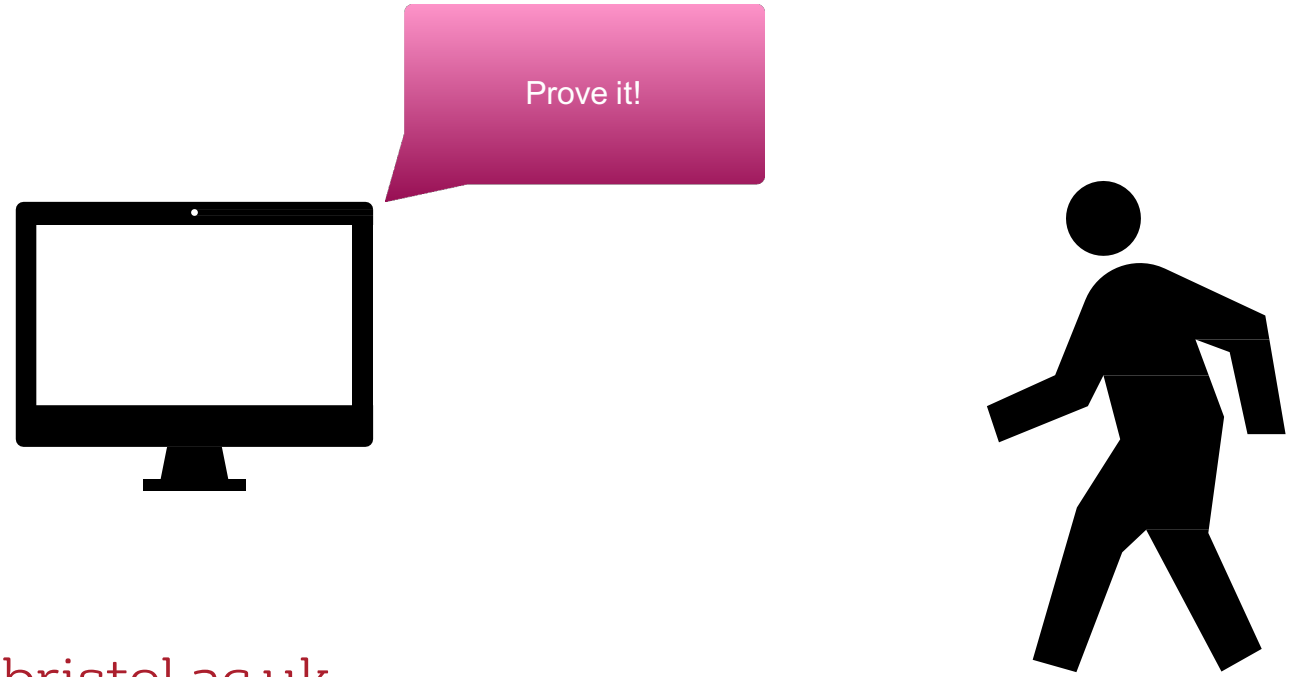
Who are you?



I am Alma and I'd like to use this computer…

Authentication

Who are you?



Authentication

- Concerned with assuring that a communication is authentic
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:
• Peer entity authentication • Data origin authentication

Authentication

3 Basic Mechanisms

Something you know

- Passwords

Something you have

- Keys

Something you are

- Biometrics and behaviours

Authentication

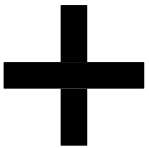
3 Basic Mechanisms

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

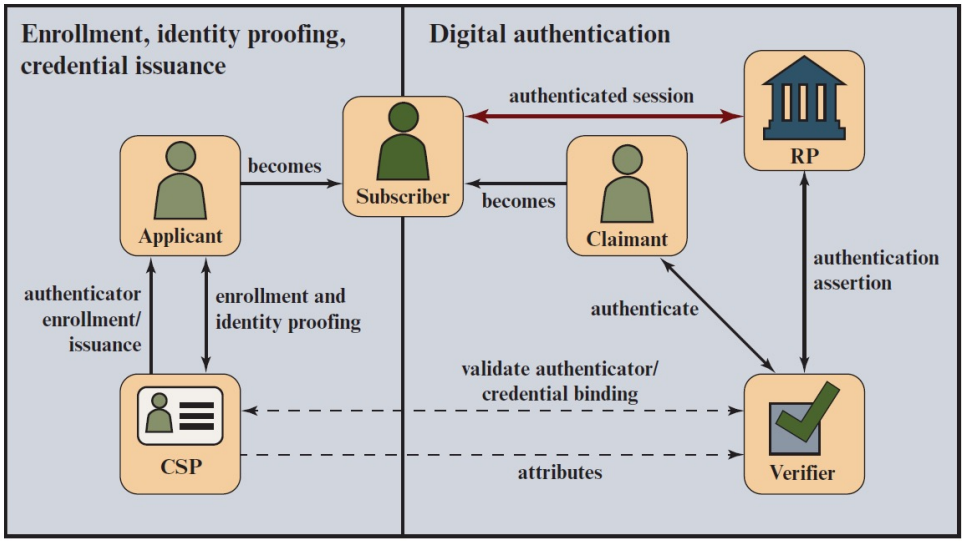
June 2017

Includes updates as of 03-02-2020

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

The NIST 800-63 Digital Identity Model



CSP = credential service provider
RP = relying party

Authentication

Keys

Something you have!

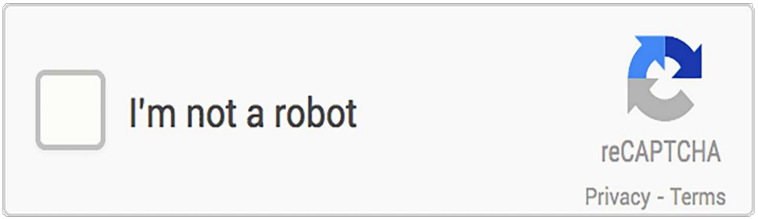
Typically a digital signature of some kind…

- 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

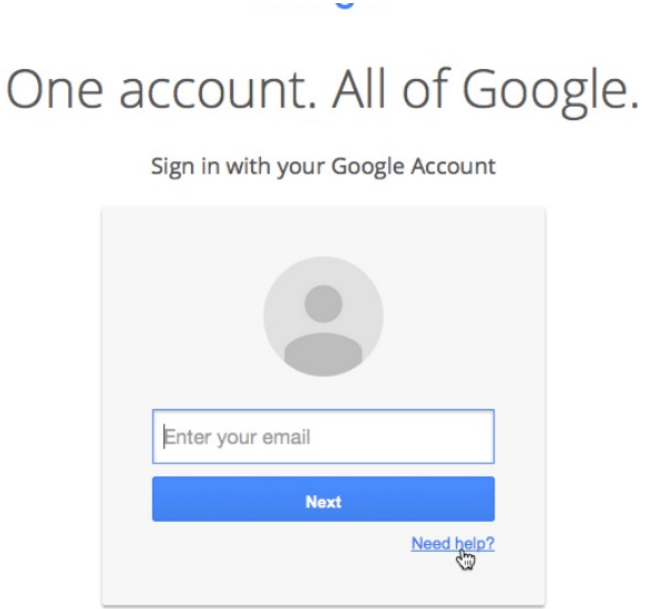
- How do you repudiate your fingerprints?
- How do you handle accessibility?

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…



Means of User Authentication (1 of 3)

There are three general means, or *authentication factors:*

Knowledge factor (something the individual knows):

- Requires the user to demonstrate knowledge of secret information.
- Routinely used in single-layer authentication processes, knowledge factors can come in the form of passwords, passphrases, personal identification numbers (PINs), or answers to secret questions

Means of User Authentication (2 of 3)

- Possession factor (something the individual possesses):
- Physical entity possessed by the authorized user to connect to the client computer or portal. This type of authenticator used to be referred to as a token, but that term is now deprecated.
  - Connected hardware tokens are items that connect to a computer logically (e.g., via wireless) or physically in order to authenticate identity. Items such as smart cards, wireless tags, and USB tokens are common connected tokens used to serve as a possession factor
  - Disconnected hardware tokens are items that do not directly connect to the client computer, instead requiring input from the individual attempting to sign in.

Means of User Authentication (3 of 3)

- Inherence factor (something the individual is or does):
  - Refers to characteristics, called biometrics, that are unique or almost unique to the individual.
  - Static biometrics:
    - fingerprint, retina, and face;
  - Dynamic biometrics:
    - voice, handwriting, and typing rhythm…

User-Authentication

- The process of determining whether some user or some application or process acting on behalf of a user is, in fact, who or what it declares itself to be
- Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server
- Authentication enables organizations to keep their networks secure by permitting only authenticated users (or processes) to access its protected resources
- User authentication is distinct from message authentication
  - Message authentication is a procedure that allows communicating parties to verify that the contents of a received message have not been altered and that the source is authentic

Authentication Principles (1 of 2)

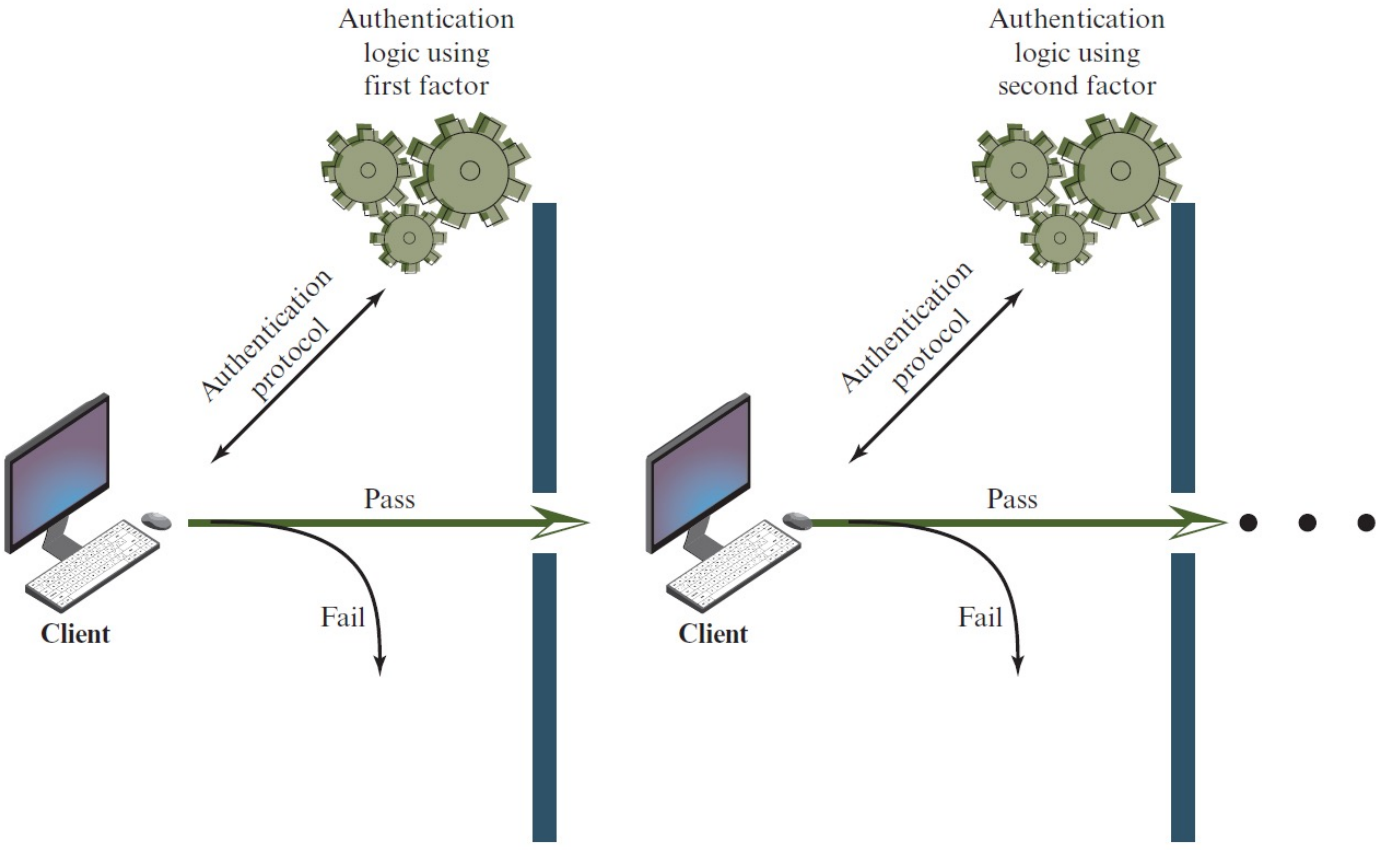
- **Digital identity:**
  - The unique representation of a subject engaged in an online transaction
  - The representation consists of an attribute or set of attributes that uniquely describe a subject within a given context of a digital service, but does not necessarily uniquely identify the subject in all contexts
- **Identity proofing:**
  - Establishes that a subject is who they claim to be to a stated level of certitude
  - This process involves collecting, validating, and verifying information about a person

Authentication Principles (2 of 2)

- **Digital authentication:**
  - The process of determining the validity of one or more authenticators used to claim a digital identity
  - Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate
  - Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as the subject that previously accessed the service

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

Mutual Authentication

Central to the problem of authenticated key exchange are two issues:

Confidentiality

Essential identification and session-key information must be communicated in encrypted form.

This requires the prior existence of secret or public keys that can be used for this purpose.

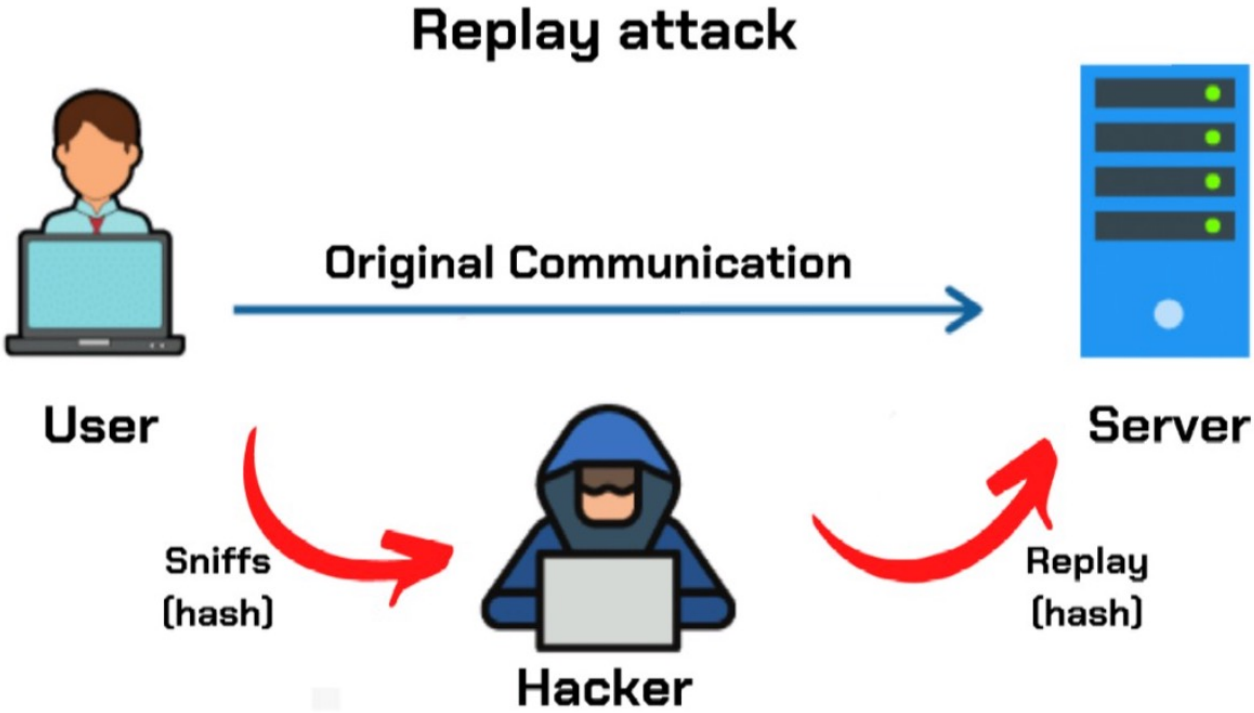
Timeliness

Important because of the threat of message replays!

Such replays could allow an opponent to:

- compromise a session key
- successfully impersonate another party
- disrupt operations by presenting parties with messages that appear genuine but are not!

What can go wrong?


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

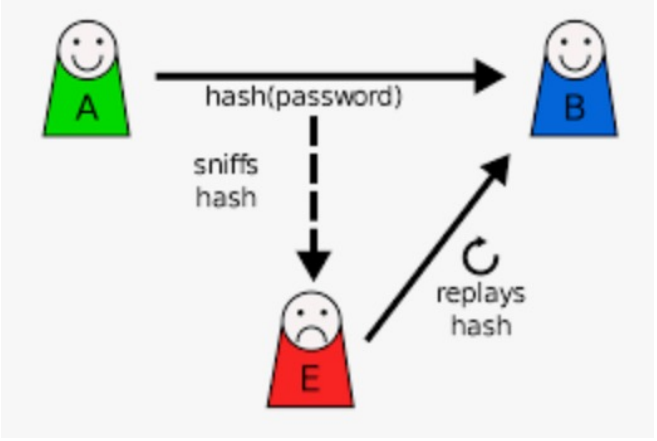
Replay attack

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.

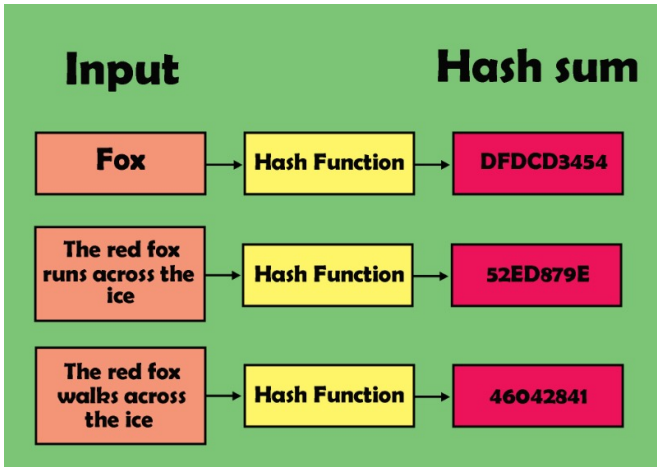
An opponent can replay a timestamped message within the valid time window, but in addition, the opponent suppresses the original message; thus, the repetition cannot be detected.

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.



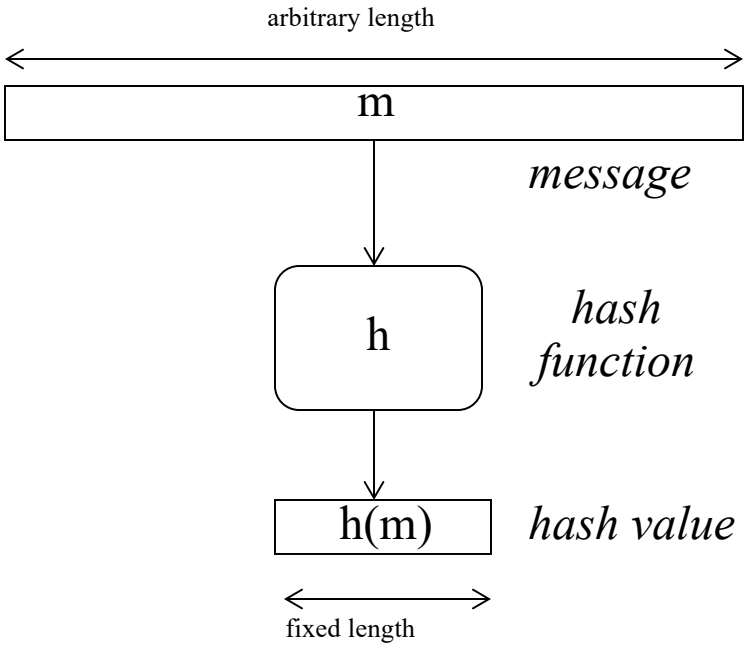
What is hash?

Introduction to Hash Functions



- Hash functions are auxiliary functions in cryptography.
- They are used e.g., for digital signatures, message authentication codes (MACs), key derivation, random number generators (RNGs),...

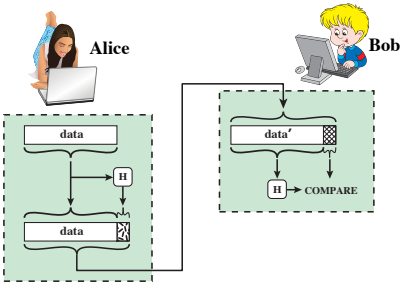
Hash Functions



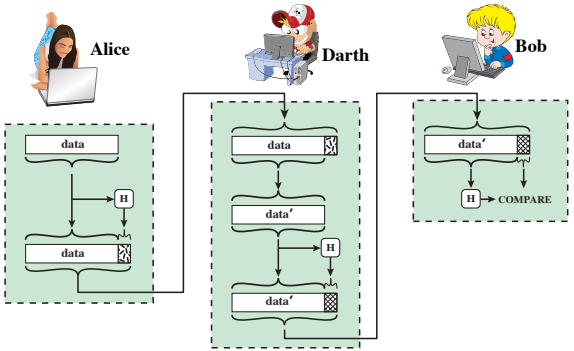
Hash functions

- Basic Requirements
  1) Public description, no key.
  2) *h(m)* can be applied to any size *m.*
  3) *h(m)* produces fixed length output.
  4) *h(m)* is easy to compute (hw and sw).

Hash functions



(a) Use of hash function to check data integrity



(b) Man-in-the-middle attack

Figure 11.2 Attack Against Hash Function

Hash functions

Security requirements

It is computationally infeasible

Property	Given	To Find
One-way	***h(m)***	***m***
Weak collision resistant	***m*** and ***h(m)***	***m'*** $\neq$ ***m***, such that ***h(m') = h(m)***
Strong collison resistant		***m'*** $\neq$ ***m***, such that ***h(m') = h(m)***

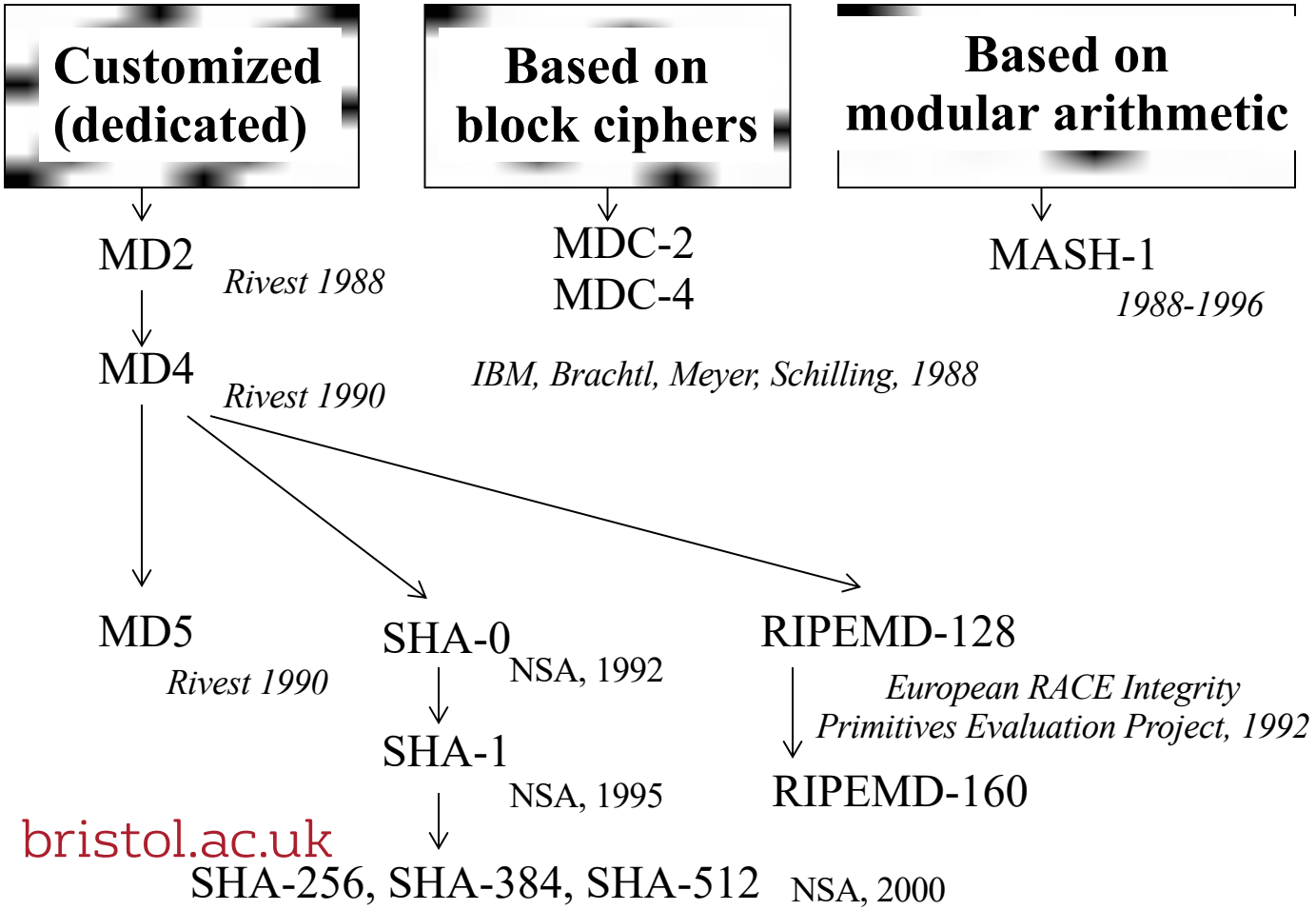
Hash functions

- Why is there no collision free hash function?

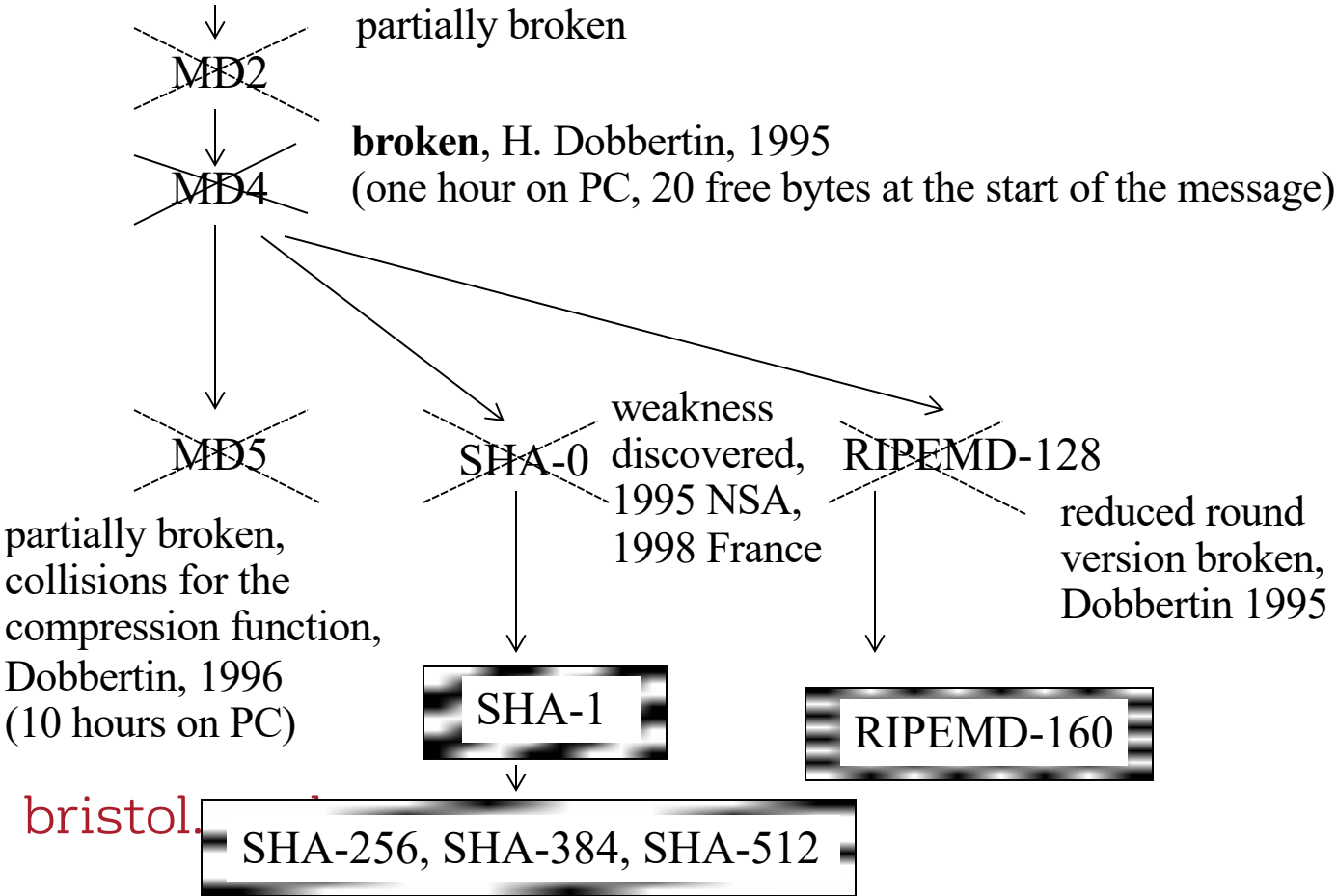
Birthday paradox

1st person, P[b'day] = 1
any person, P[b'day] on a specific date] = $\frac{1}{365}$
2nd person, P[b'day ≠ 1st person] = $1 - \frac{1}{365} = \frac{364}{365}$
3rd person, P[b'day ≠ 1st and 2nd] = $1 - \frac{2}{365}$
P[all 3 have different b'day] = $(1 - \frac{1}{365}) \cdot (1 - \frac{2}{365})$
for 46 ppl: $(1 - \frac{1}{365})(1 - \frac{2}{365}) \ldots (1 - \frac{45}{365}) = 0.052$
P[no two ppl. have b'day same] = 0.052
i.e. P[two have same b'day] = 94.8% !

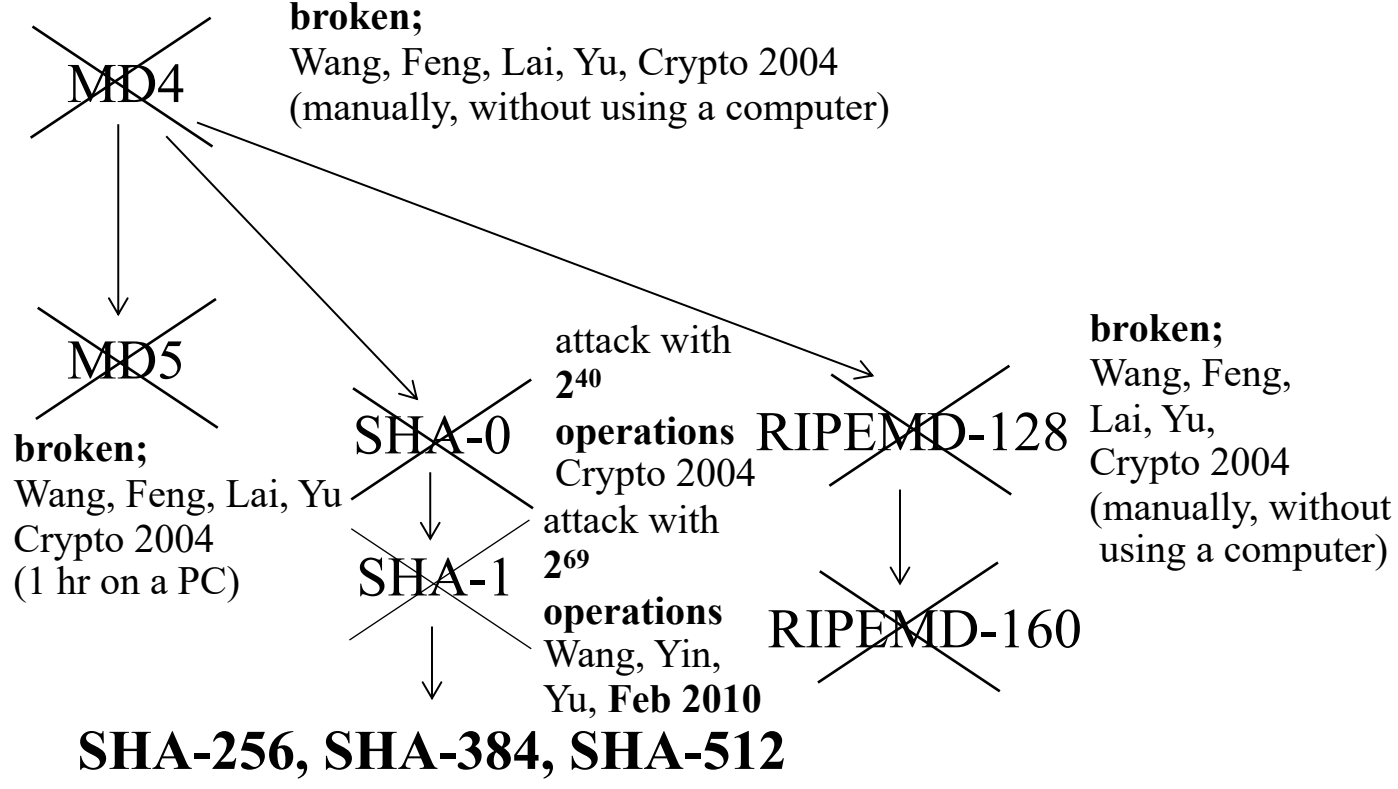
Hash function algorithms



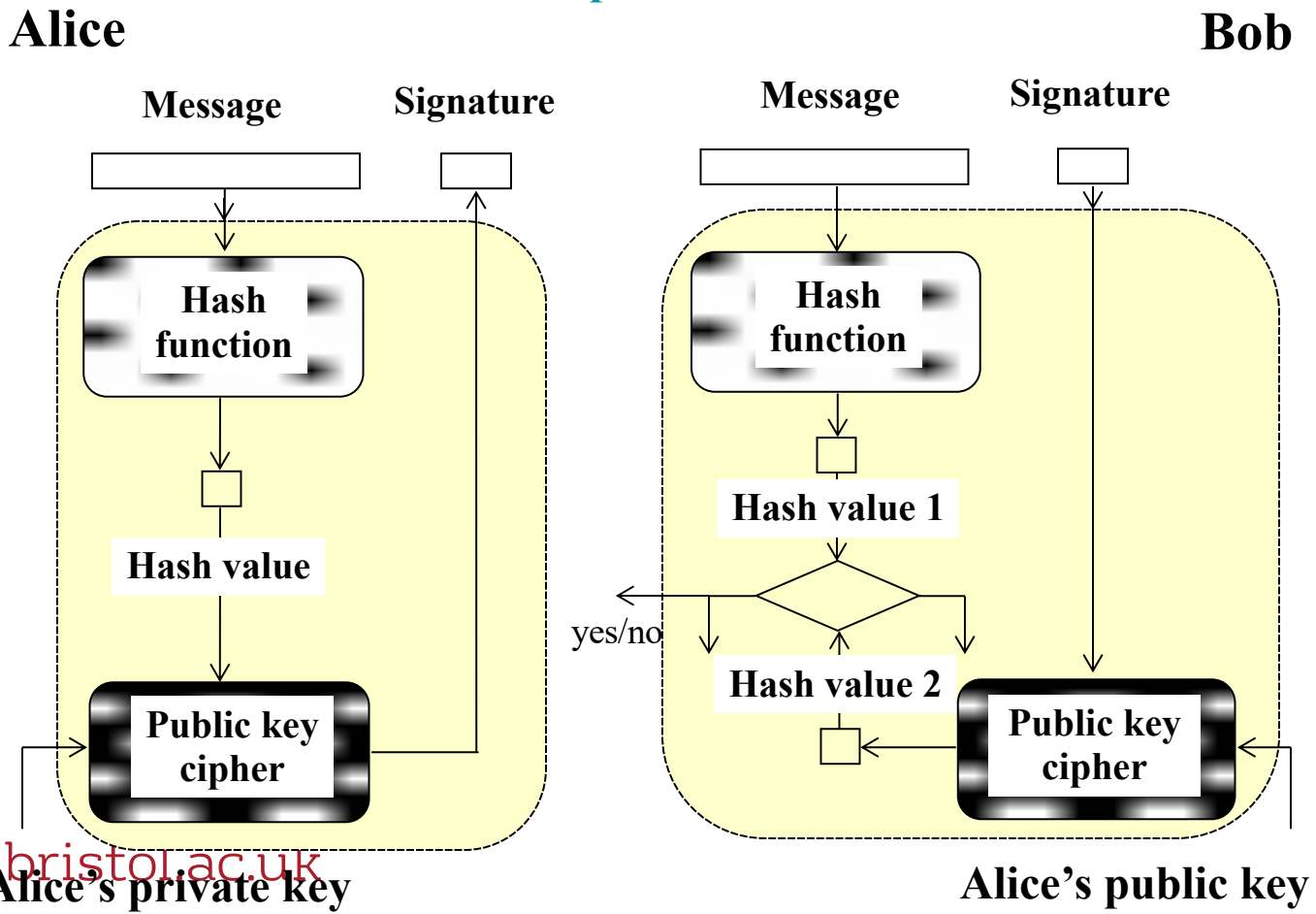
Security of dedicated hash functions



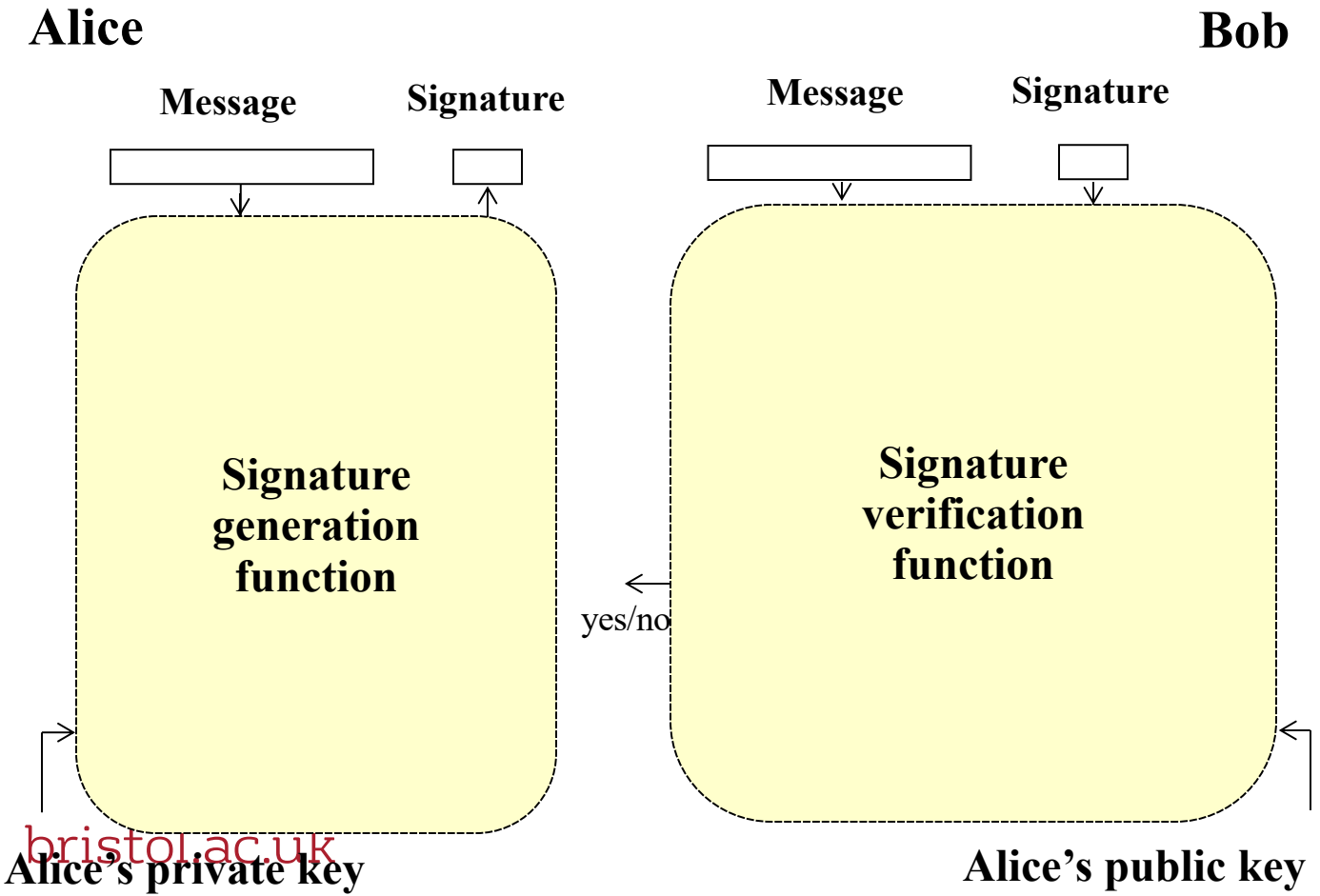
What was discovered in 2004-2015?



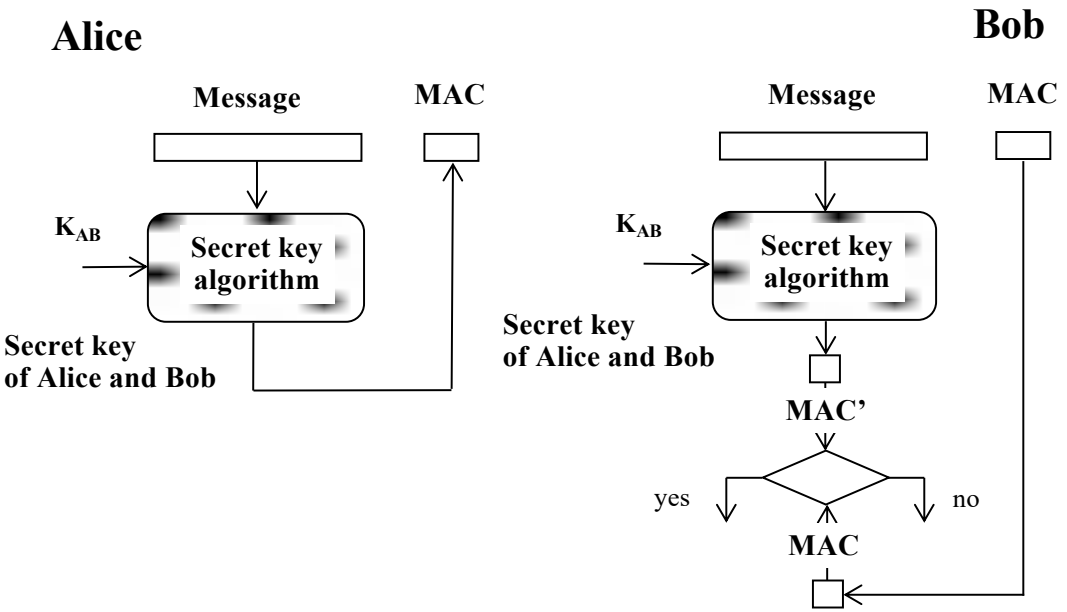
Non-repudiation



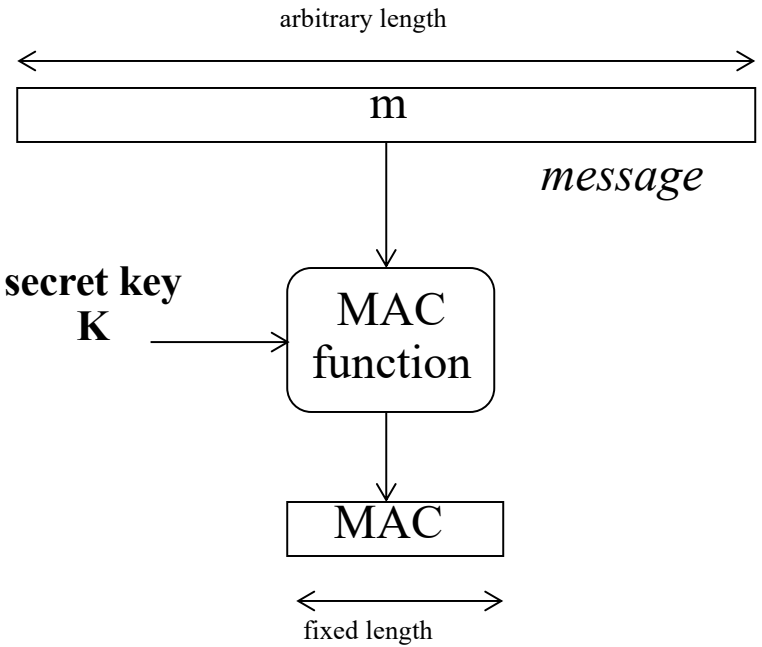
Non-repudiation



Authentication



MAC - Message Authentication Codes (keyed hash functions)



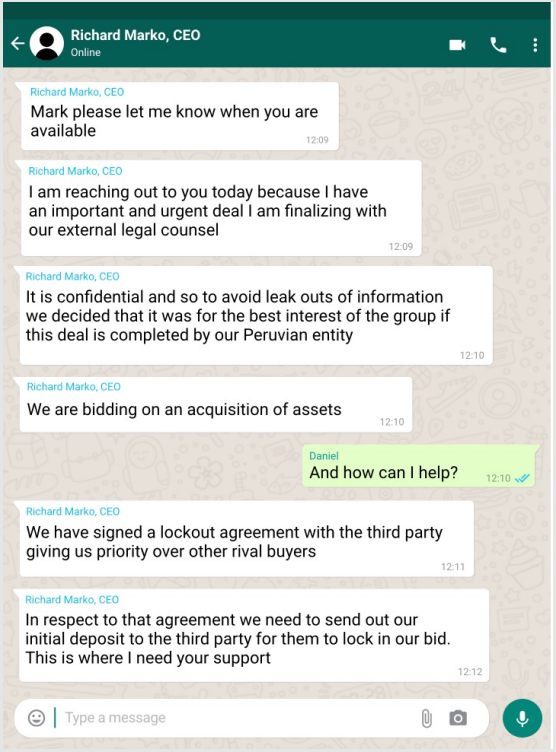
bristol.ac.uk

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.


A real story: Impersonation attack against ESET
Cyberattacks can happen to any organization.
In 2020, ESET faced CEO impersonation attempts via WhatsApp messages. The goal of this attempt was to fake the existence of a big bid that required a financial deposit.
Check out samples of these messages below.



Impersonation

Approaches to Coping With Replay Attacks (1 of 2)

- Attach a sequence number to each message used in an authentication exchange
  - A new message is accepted only if its sequence number is in the proper order
  - Difficulty with this approach is that it requires each party to keep track of the last sequence number for each claimant it has dealt with
  - Generally not used for authentication and key exchange because of overhead

Approaches to Coping With Replay Attacks (2 of 2)

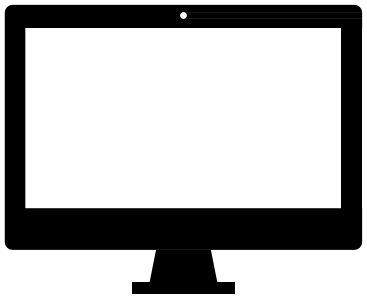
- Timestamps
  - Requires that clocks among the various participants be synchronized
  - Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgment, is close enough to A's knowledge of current time
- Challenge/response
  - Party A, expecting a fresh message from B, first sends B a *nonce* (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value

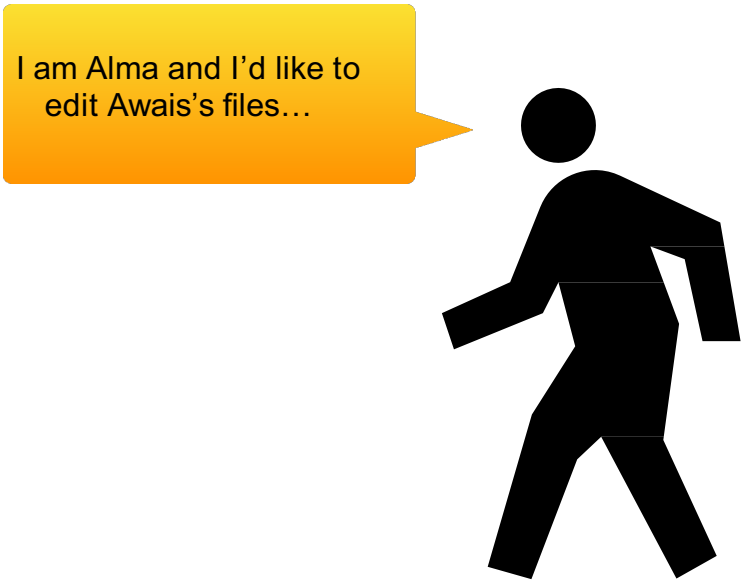
Authorization:

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

Authorization

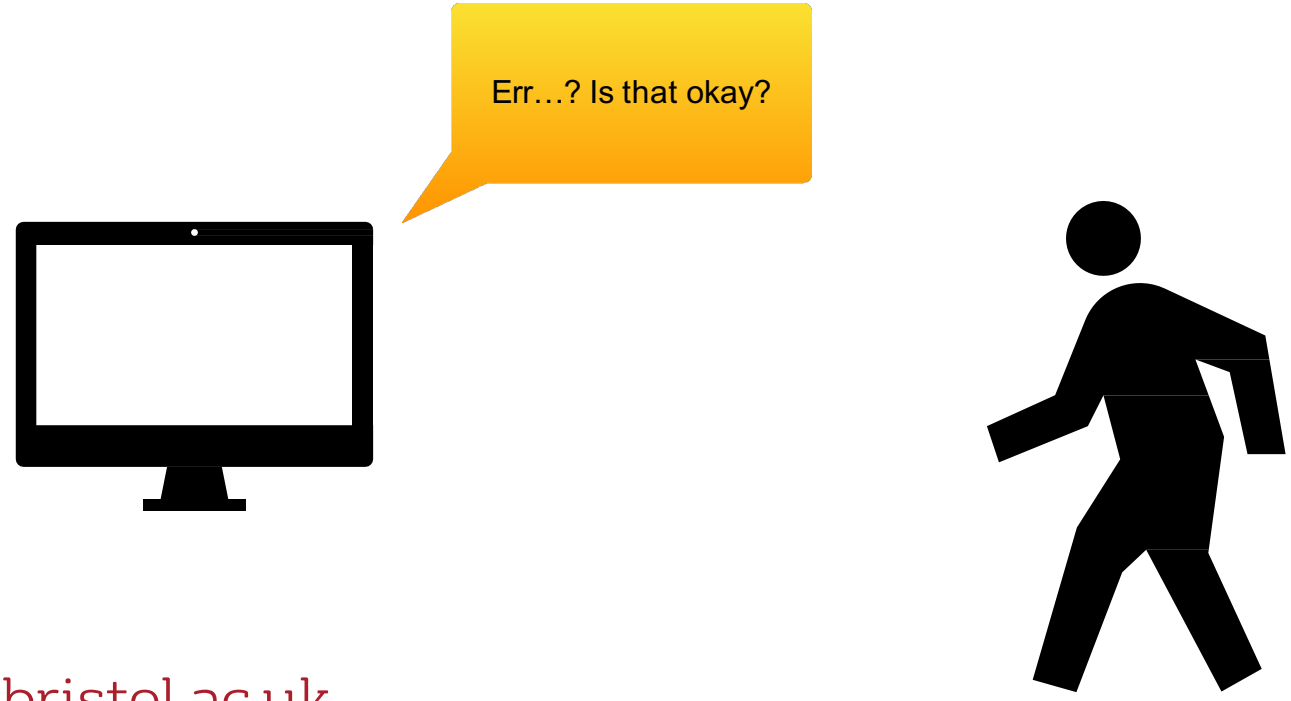
What can you do?





Authorization

What can you do?



Authorization

How do I change my password?

```
-bash-5.0$ ls -l `command -v passwd`
-r-sr-xr-x  1 root  bin  20936 Oct  5 00:47 /usr/bin/passwd
```


…there are some other *magic bits too*

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*

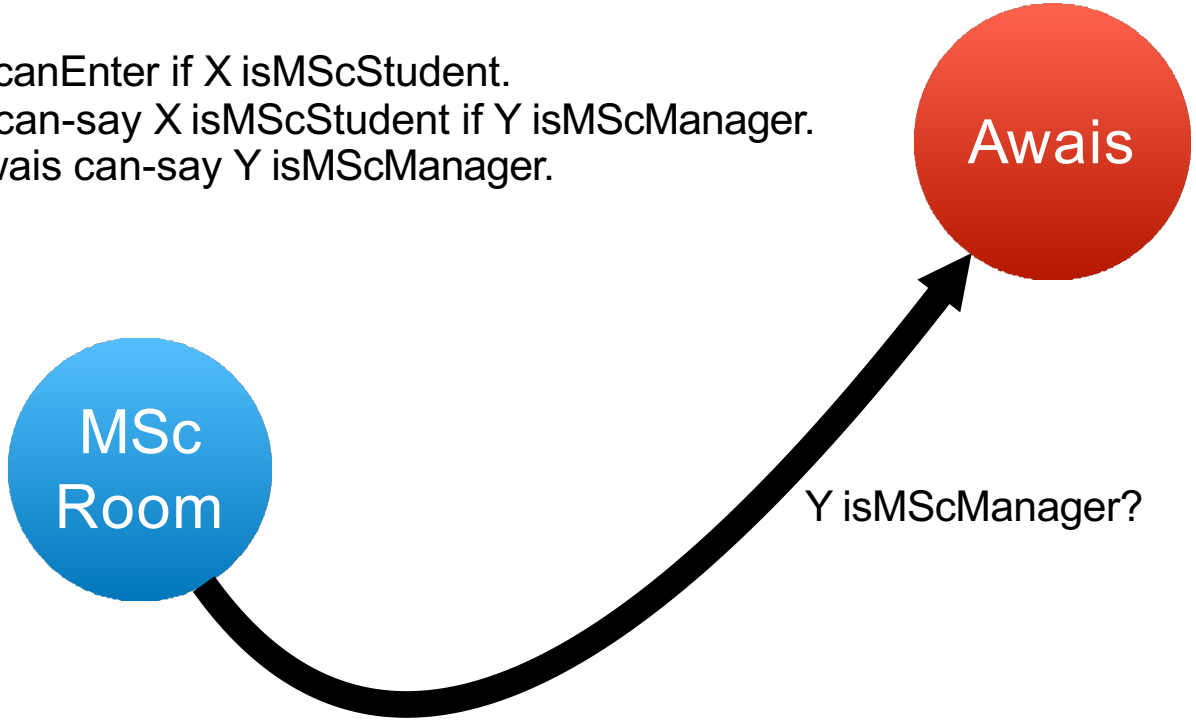
Bob wants to access the MSc room…

?- bob canEnter.

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

?- bob canEnter.

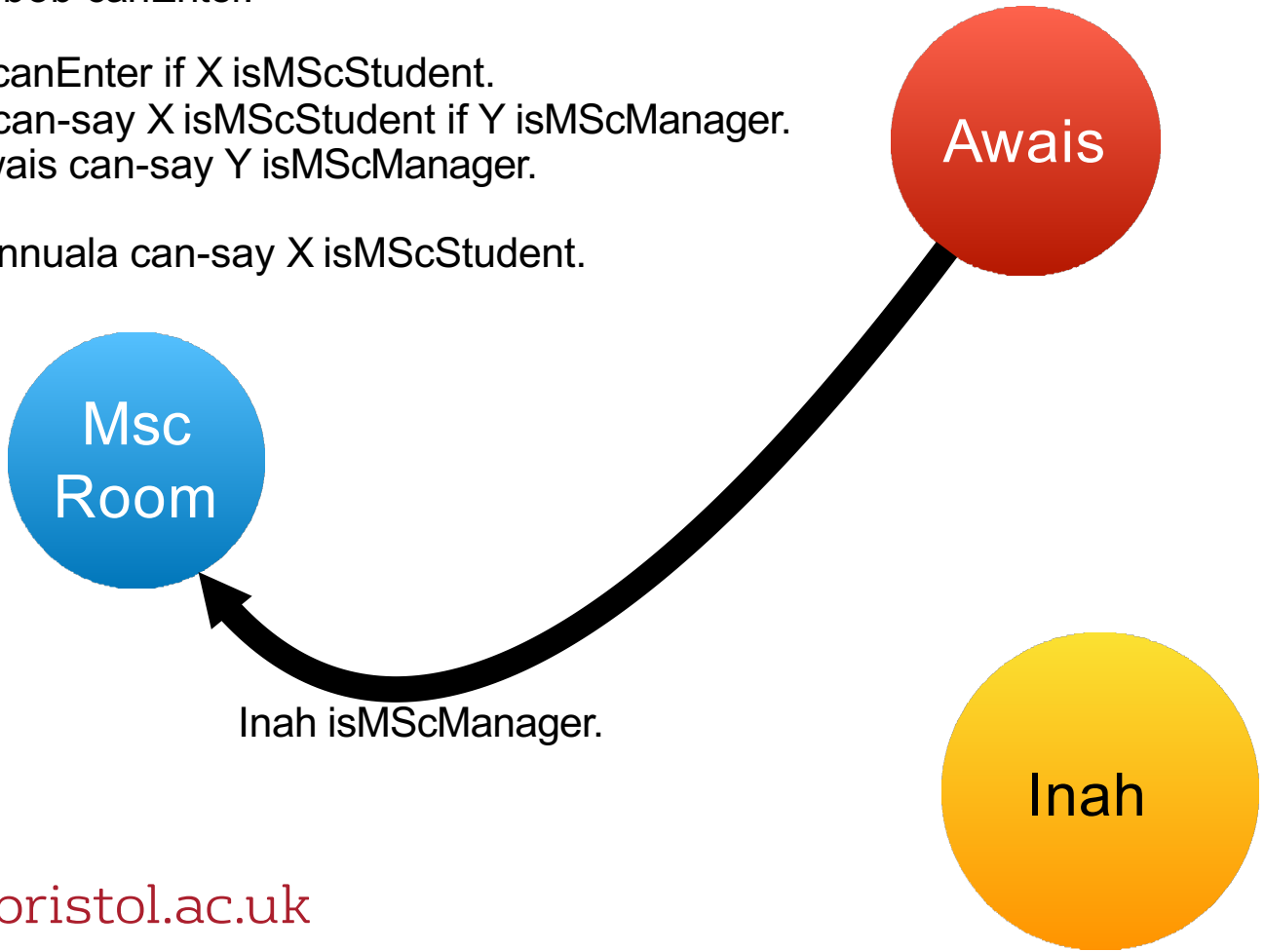
X canEnter if X isMScStudent.
Y can-say X isMScStudent if Y isMScManager.
awais can-say Y isMScManager.



?- bob canEnter.

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

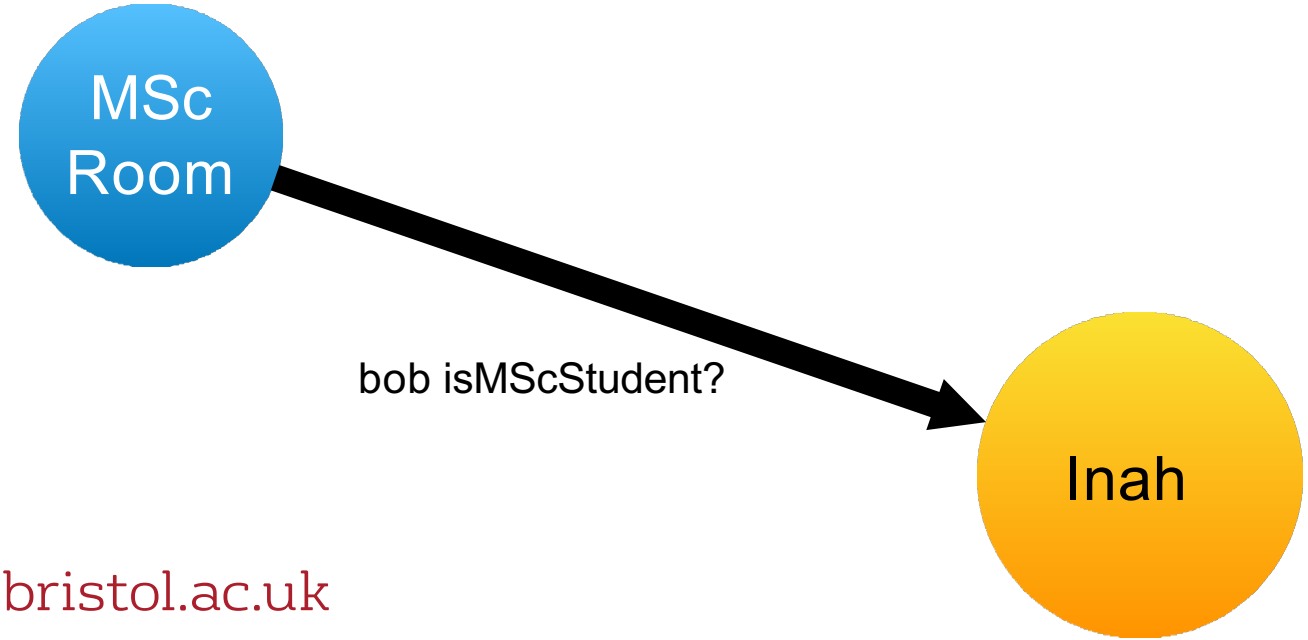
fionnuala can-say X isMScStudent.



?- bob canEnter.

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

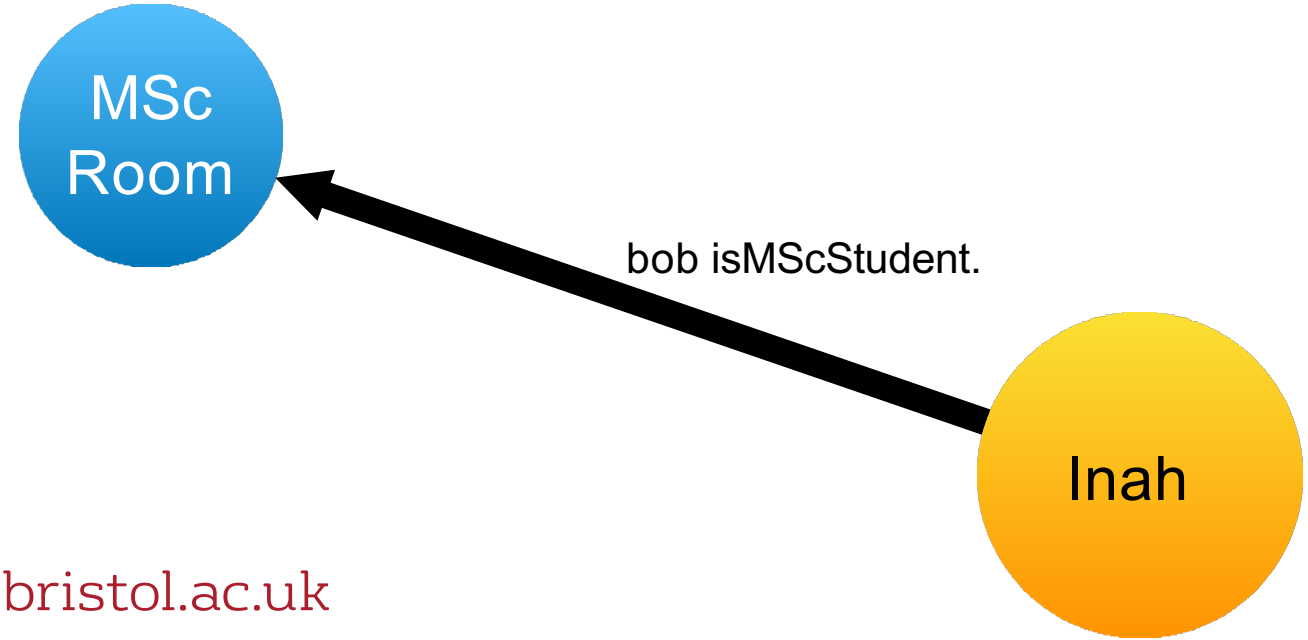
fionnuala can-say X isMScStudent.



?- bob canEnter.

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

fionnuala can-say X isMScStudent.



?- bob canEnter.

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

fionnuala 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>

Authorization

Role-Based Access Control

In the previous example Awais and Inah had jobs

- Awais could say who was a MSc manager…
- Inah could fulfill the role of a MSc manager…

RBAC lets us write policies with *roles.*

- Roles get assigned and removed at runtime
- More control than UNIX/POSIX DAC
- SELinux / SEAndroid

Authorization

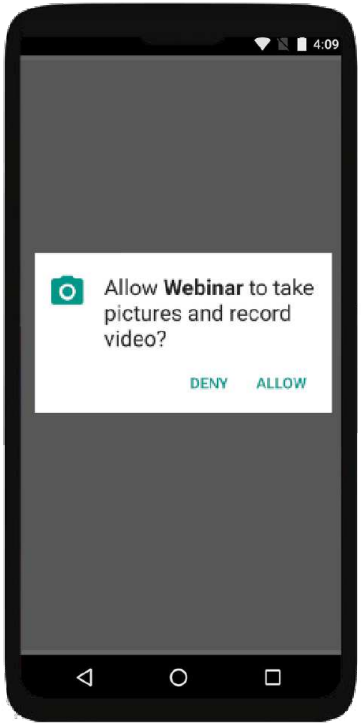
SEAndroid

Mobile OSs have permissions to access various system features…

Android implements its permission system atop a Linux RBAC system called SELinux (called SEAndroid)

Source code is online!

https://cs.android.com/android



Authorization

Other schemes

What about if instead of just having role we have them assigned dynamically based on the time of day?

- Gary the Gatekeeper can open the front gate between 9am–5pm
- Nigel the Nightwatchman can open the gate from 5pm–9am

Attribute-based access control (ABAC)

- Doesn't have to be time could be anything!

Authorization

XACML 3.0

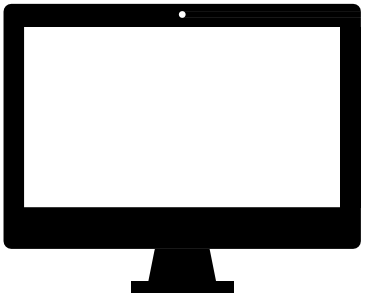
```
<xacml3:Rule RuleId="c01d7519-be21-4985-88d8-10941f44590a" Effect="Permit">
    <xacml3:Description>Allow if time between 9 and 5</xacml3:Description>
    <xacml3:Target>
        <xacml3:AnyOf>
            <xacml3:AllOf>
                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</xacml3:AttributeValue>
                    <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time" MustBePresent="false" DataType="http://www.w3.org
/2001/XMLSchema#time"/>
                </xacml3:Match>
            </xacml3:AllOf>
        </xacml3:AnyOf>
        <xacml3:AnyOf>
            <xacml3:AllOf>
                <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:time-less-than">
                    <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</xacml3:AttributeValue>
                    <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time" MustBePresent="false" DataType="http://www.w3.org
/2001/XMLSchema#time"/>
                </xacml3:Match>
            </xacml3:AllOf>
        </xacml3:AnyOf>
    </xacml3:Target>
</xacml3:Rule>
```

Accountability:

***Or* who did what?**

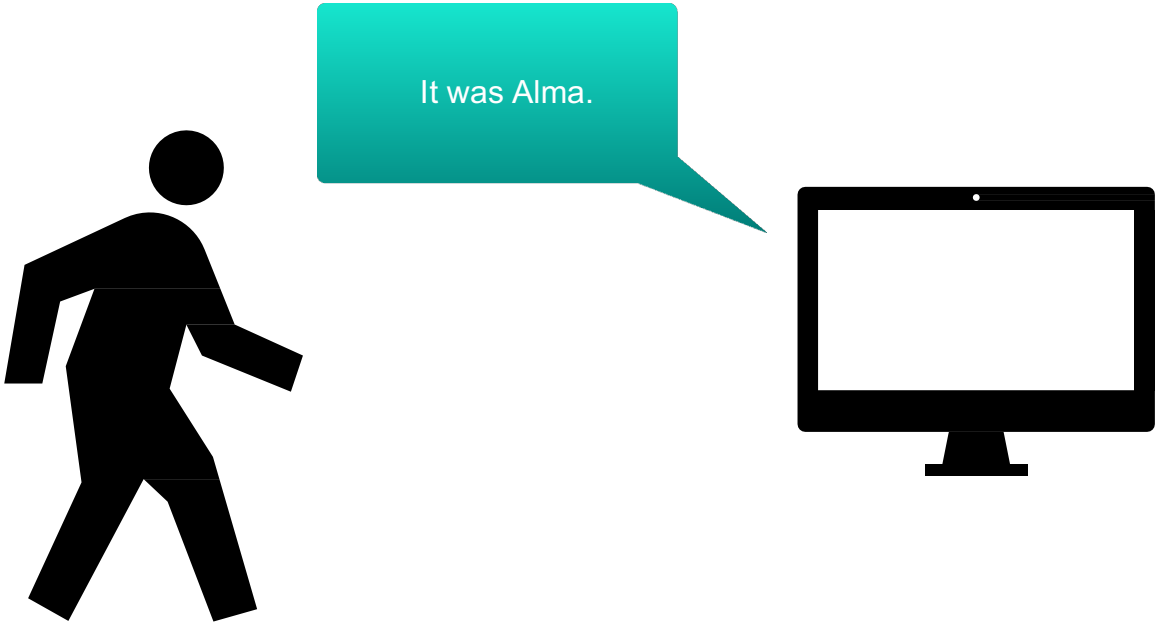
Accountability

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

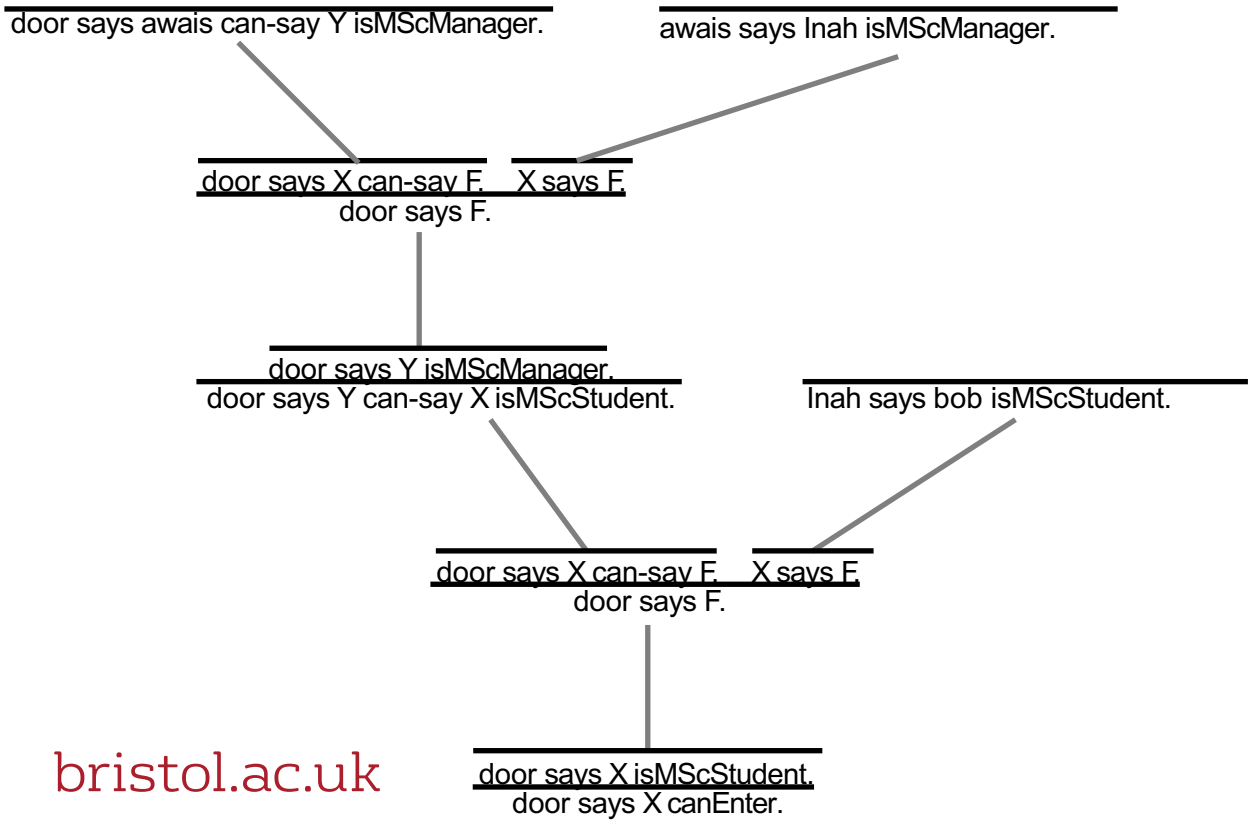
Suppose I have some authorisation logic making decisions about who I let in…

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

But checking a proof can usually be done quickly!

Check unconnected facts are known

Check transitions can be derived with one of the rules



Authentication, Authorization & Accountability

A whistle stop tour

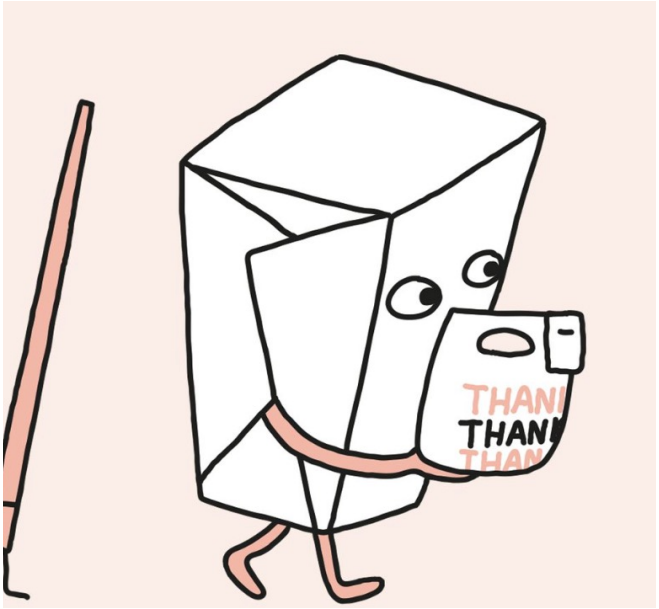
bristol.ac.uk

AAA Further Reading

- CyBOK's discussion of AAA is pretty good.
- SELinux Coloring Book
- 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