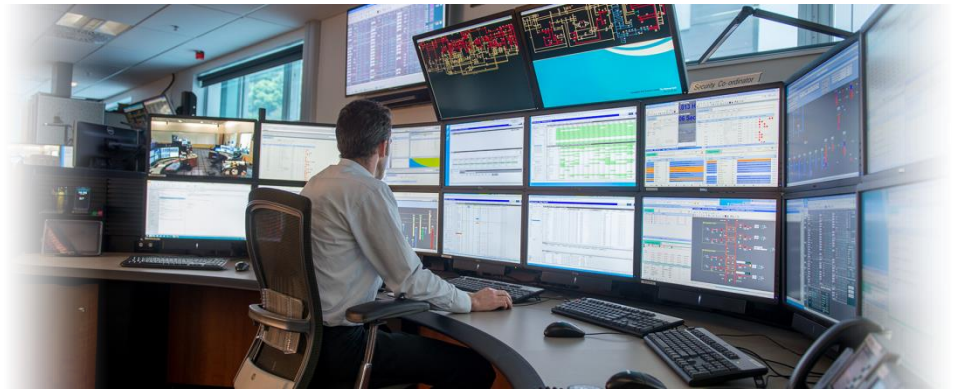
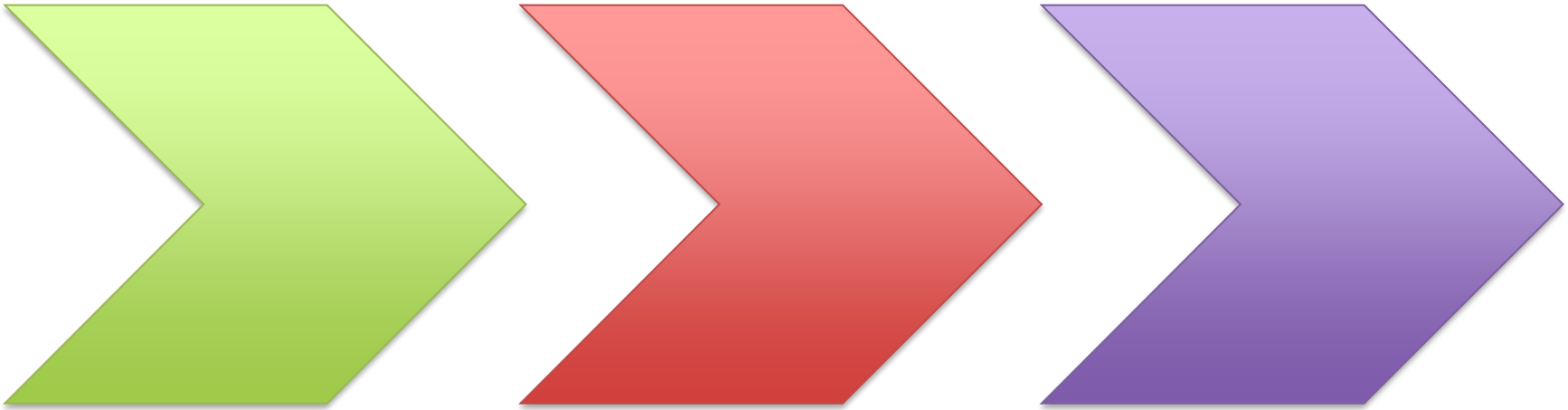
Technical Security Controls

Technical Security Controls

- How can we maintain a secure technical environment?
- How can we communicate, and yet maintain security?
- How can we protect ourselves from malicious activity?



Design of security controls



Preventative:	Detective:	Corrective:
Before the event, e.g. locking out unauthorized users.	During the event, e.g. sounding an alarm when attacked.	After the event, e.g. damage limitation and incident recovery

Design of security controls

Physical controls
e.g., fences, doors, locks.

Procedural controls
e.g., incident response processes, security awareness.

Legal and regulatory or compliance controls
e.g., privacy laws, policy

Technical controls
e.g., user authentication, anti-virus, firewalls.

What are we securing against?

- Viruses, Worms, Trojans
- Botnets
- Distributed Denial of Service
- Rootkits
- Backdoors
- Data Fraud
- Systems sabotage
- Theft

Zero-day exploits

An attack that can exploit a (as of yet unresolved) vulnerability.

Given the 'unknown' nature of the vulnerability these are worth big money!

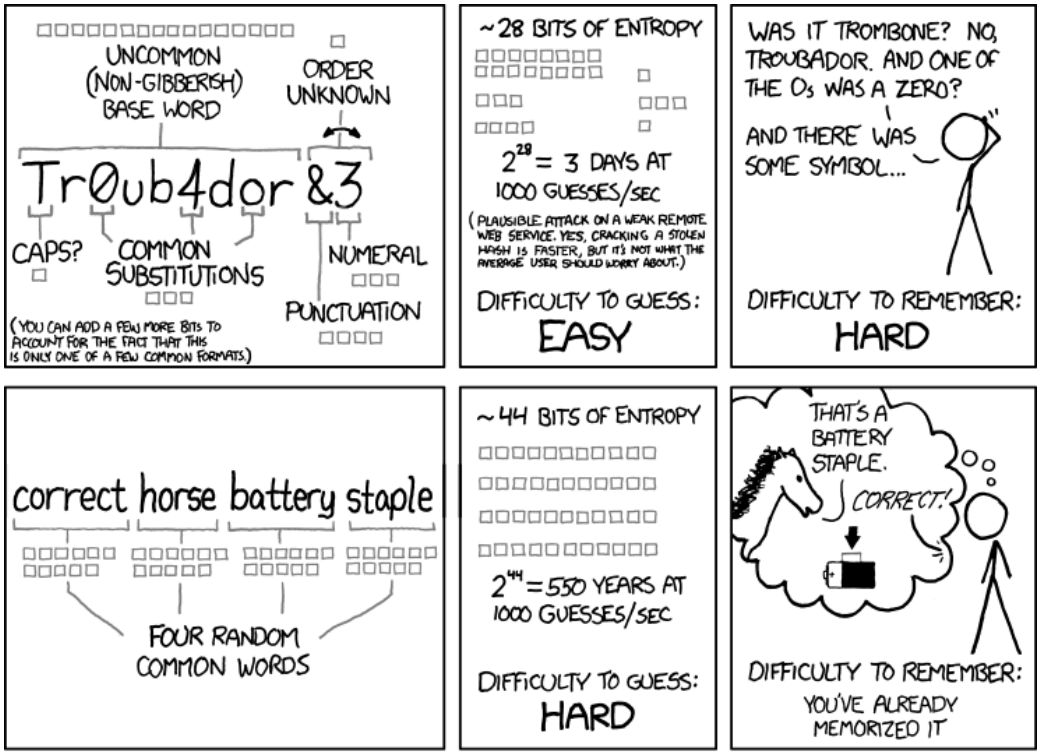
Who are we securing against?

- External attackers
  - Hackers, script kiddies, governments, hacktivists...
- Internal attackers
  - Employees, contractors, management, suppliers…
- *"Employee's are a company's greatest asset and yet also their greatest threat".*

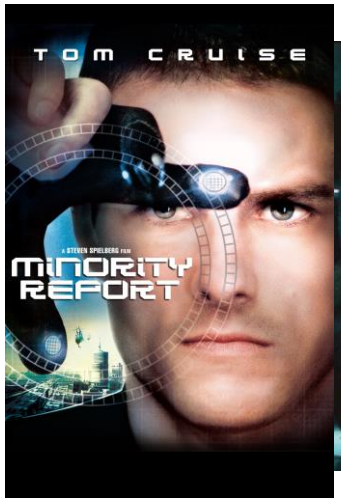
User authentication

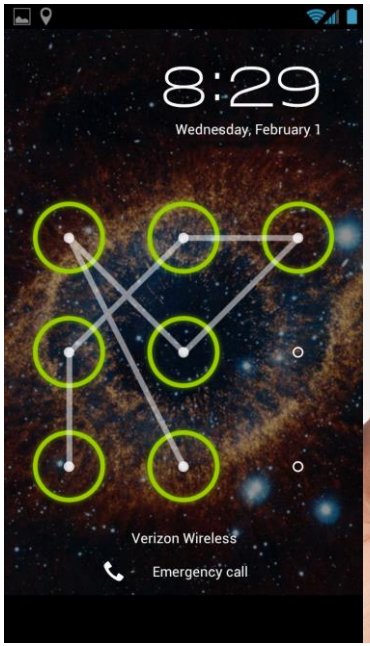
- User must authenticate that they are authorized to access the system.
  - Password
  - Pattern
  - Biometrics (e.g., fingerprint, iris)
- What are the weaknesses in these methods?

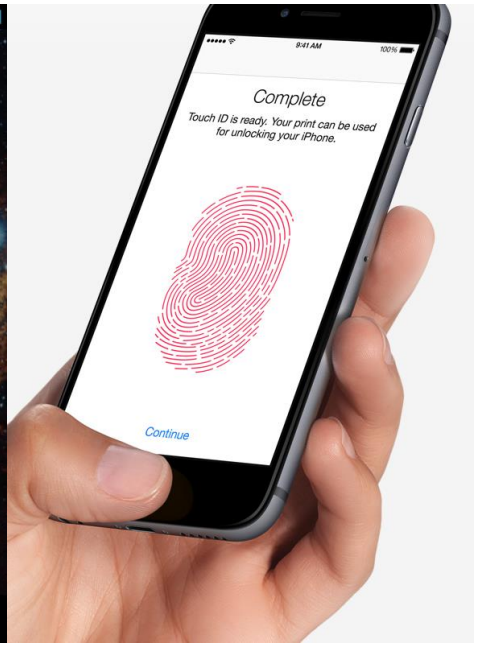
User authentication



User authentication

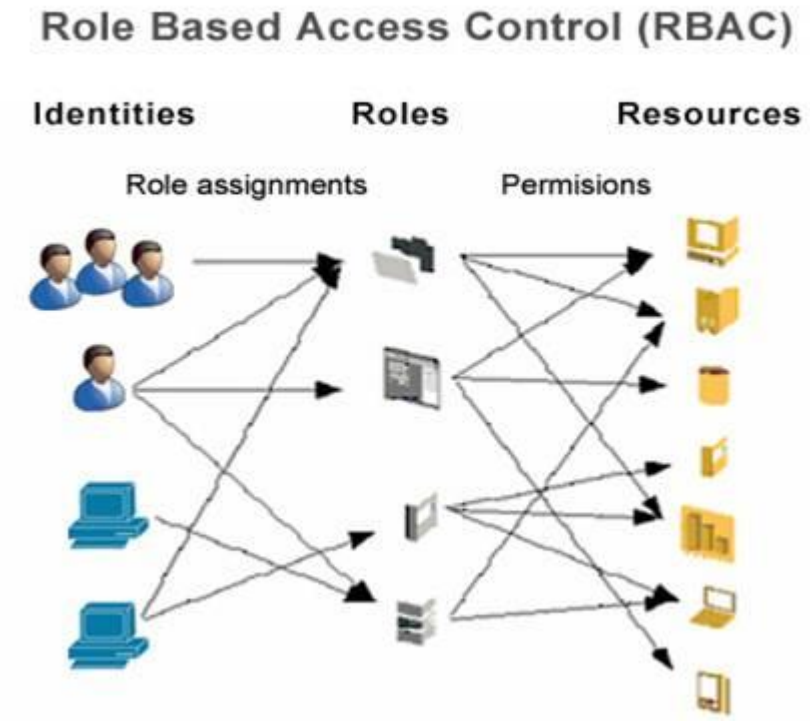






Role-based Access

- Groups of users may be granted different access controls (**r**ead, **w**rite, e**x**ecute).
  - E.g., Owner can **rwx**, others can only **read**.
- Effective for collaborative environments
  - but only if managed correctly!

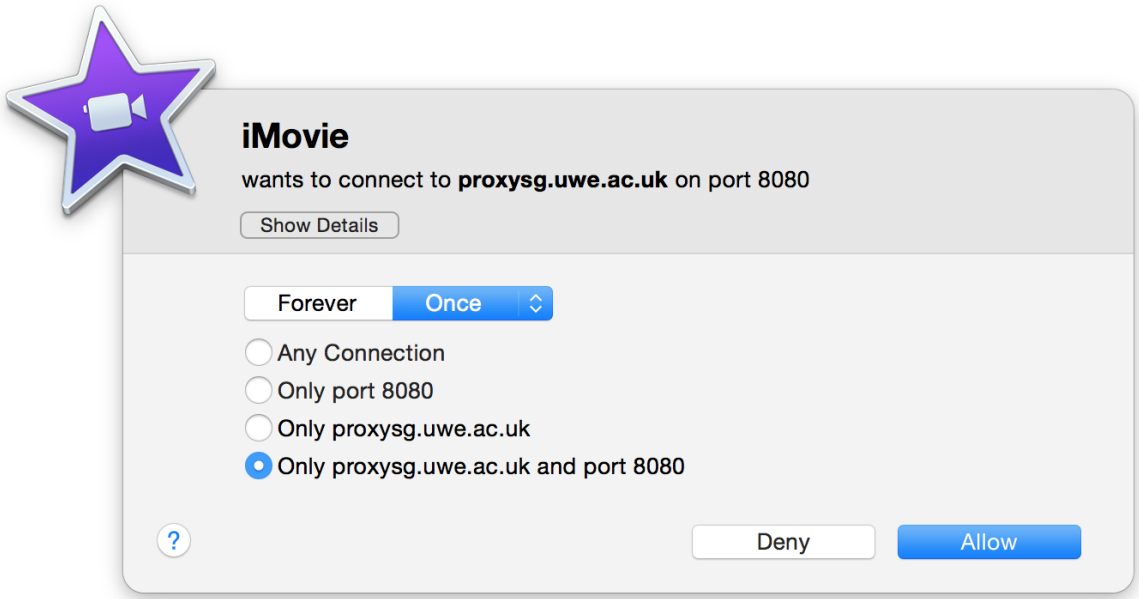


Anti-virus

- Signature-based detection – comparison between file system and known viruses.
  - Relies on definition updates to protect against new threats.
- *Norton, McAfee, Kaspersky, AVG, Avast, Comodo, ClamXav*… many commercial products.
- Malware developers aim to circumvent signatures to avoid detection – e.g., compression and encodings.
- Be aware of fake anti-virus products also!

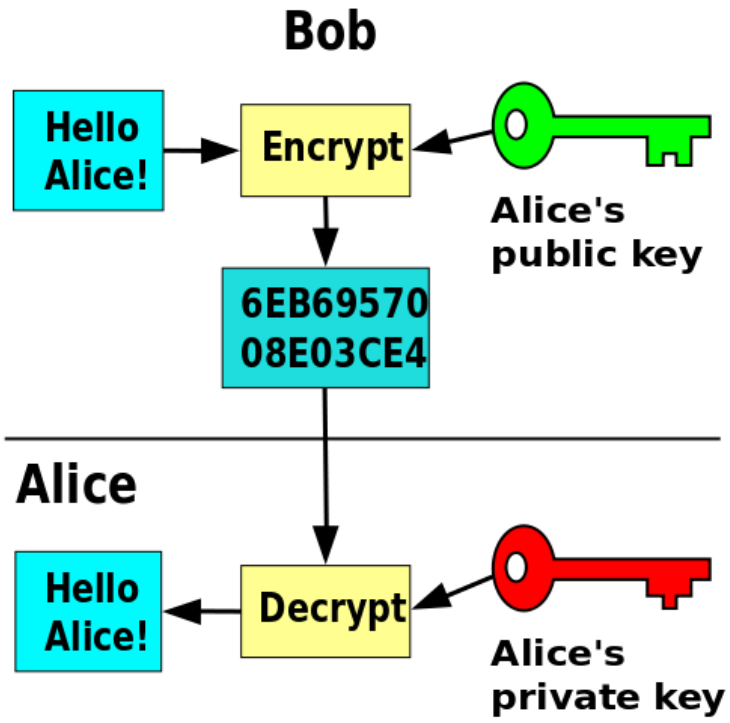
Firewall

- Monitors inbound network connections.
  - User to decide whether a connection should be allowed (create a 'rule' to accept or block).
- Some firewalls also monitor outbound connections (e.g., Little Snitch, ZoneAlarm).
- Requires user to make the security decisions.
- IDS (intrusion detection systems) are related, more sophisticated tools used at enterprise-level.



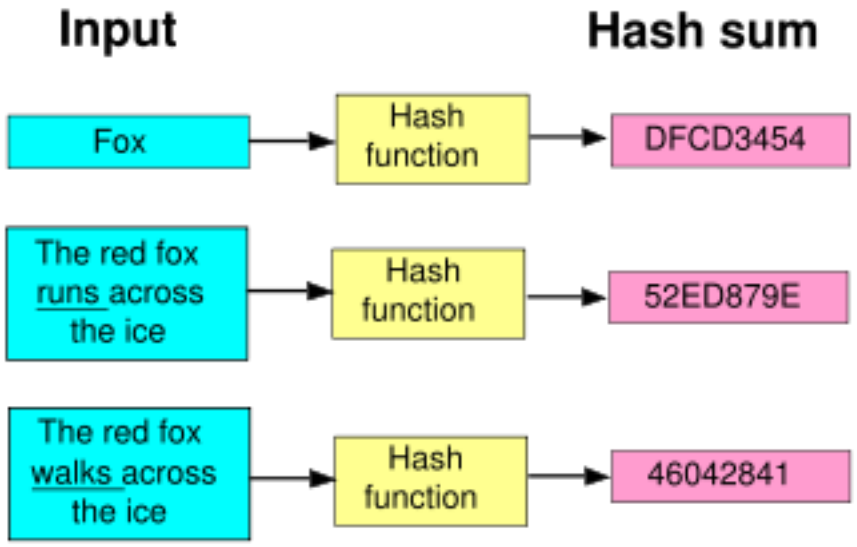
Cryptography

- The practice of secure communications.
  - Fundamental to how the Internet operates!
- Public-key encryption
- Used for authentication, and for digital signing.
- Encryption discussed in Officials Secrets Act 1989 - http://en.wikipedia.org/wiki/RSA_(cryptosystem)



Hashing

- Similar to cryptography, however is not bi-directional.
  - Text can be hashed, but hash can not reveal text.
  - What are the vulnerabilities in hashing? Collisions? Md5, sha1, sha2…
- Uses include storing and transmitting passwords, validating file content, and digital signatures.



Future of security

- Anomaly detection…
  - Less signatures – focused on the change in behaviour instead of checking against signature.
  - Can extend beyond virus protection – what about malicious insiders who don't require malware?
  - How to avoid a high false positive rate?
- Continuous authentication…
  - Combining biometrics with behavioral patterns
  - Traditional security check occurs only at login – how can we be sure user is acting under duress?

So how do we stay secure?

- Understand the technologies available, but also understand their limitations.
  - Antivirus, firewall, authentication.
- Prioritize efforts – what is the most important asset to protect? Is it data?
- Well-managed Role Based Access Control, and having employees who respect this.

Tutorial: Technical security in ISMS

- **What** and **Who** are the technical risks for your chosen organisation?
  - What is the procedure for managing these?
  - Are there any limitations in the current practice?
  - Do they currently have a technical security policy?
- What are the pros and cons of using encryptions techniques?
  - How do these relate to your organisation?
  - Do they currently have an encryption policy?