Dr. Phil Legg

Associate Professor in Cyber Security

Information Risk Management

07: Mitigations and Controls

Date

UWE Bristol | University of the West of England

Today

- Security Controls, and designing security controls
- Types of controls:
  - Procedural,
  - People,
  - Technical and
  - Physical

Security Controls

Three forms of control:

- Preventative controls: Reduce the likelihood of a loss event occurring
- Detective controls: Recognize when a loss event has/is occurring
- Responsive controls: Minimize impact when a loss event has occurred.
- ***Think of it as:***
  - ***Before, During, After***
  - *Responsive is sometimes considered as Corrective Controls*

Preventative:
Before the event,
e.g. locking out unauthorized users.

Detective:
During the event,
e.g. sounding an alarm when attacked.

Responsive:
After the event,
e.g. damage limitation and incident recovery

Security Controls

Relationship between controls:

- If Preventative controls were 100% effective, there would be no need for detection and responsive controls.
- If Detection and Responsive controls were 100% effective (e.g., some caught accessing sensitive data with intent is immediately locked out) we would not need prevent controls.

Preventative:
Before the event,
e.g. locking out unauthorized users.

Detective:
During the event,
e.g. sounding an alarm when attacked.

Responsive:
After the event,
e.g. damage limitation and incident recovery

Design of Security Controls

Technical Controls:

- Authentication, Anti-Virus, firewall

Physical Controls:

- Fences, doors, locks

Procedural Controls:

- Incident response processes
- Security awareness

Legal and Regulatory Controls:

- Privacy laws
- Policies
- GDPR, Computer Misuse Act

Control Categories

- Asset level controls: Controls applied directly to manage the frequency and/or magnitude of loss from events that can affect assets (e.g., system configuration and patching, passwords, access privileges, logging, backup and recovery tools and processes, door locks, and HVAC systems)
- Variance controls: Controls intended to minimize the variance of asset level controls over time (e.g., policies, standards, education and awareness training, well-defined processes, automation, auditing and testing, and remediation). Managing variance is key to asset-level control effectiveness over time.
- Decision-making controls: Help stakeholders define, adjust and enforce expectation, and allocate resources for risk management objectives

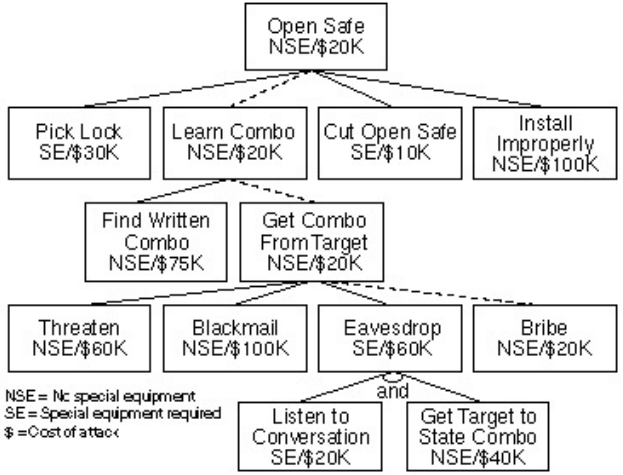
Guidance of Risk Controls

- Understand what you care about, and why
- Think about situations in which you could be compromised
- Balance cyber risks against other types of risk
- Be aware of the strengths and weaknesses of risk management techniques

- https://www.beta.ncsc.gov.uk/collection/risk-management-collection?curPage=/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security

Attack Trees

- A means to model possible attack scenarios: https://www.schneier.com/academic/archives/1999/12/attack_trees.html
- Can we apply this to our risk treatment? Think about the outcome first, and then work backwards to identify suitable mitigation / points of intervention
- Identifying attack patterns for insider threat detection: https://www.sciencedirect.com/science/article/pii/S136137231530066X



Here, cheapest route to open safe with no special equipment is to bribe target.

Mitigation of risk would be to pay the target more – less susceptible to bribes – then threaten or eavesdrop become cheaper routes

UWE Bristol | University of the West of England

Procedural Security Controls

- Policies, standards, procedures and guidelines
- What are the differences between these?

Procedural Security Controls

- Policy – high level statement of an organisation's values, goals and objectives in a specific area, and the general approach to achieving them. *E.g., Information Security Policy*
- Standard – more prescriptive than policy, states what needs to be done and provides consistency in controls that can be measured. *E.g., The ISF Standard of Good Practice for Information Security*
- Procedure – set of detailed working instructions that will describe what, when, how and by whom something should be done. *E.g., Handling Copyright Infringements Notification Procedure*
- Guidelines – not obligatory buy can provide advice, direction and best practice in instances where it is difficult to regulate how something should be done (e.g., out of office working). *E.g., Guidelines for using Dropbox and other cloud storage providers*

Procedural Security Controls

- Policies, standards, procedures and guidelines

- Documentation needs to be clearly written and precise.
- Where possible, statements should contain positive rather than negative ‘do not’ cases – promote the correct way rather than the wrong way of doing things.
- Need to be endorsed by senior management, and have clear ownership (e.g. HR, manager)

Incident Response

- 5 phases of incident management:
  reporting, investigation, assessment, corrective action, review.
- Incident report includes who they are, where they are, contact details, brief description of incident, any danger to life health or company assets, any actions taken so far, and time of incident.

- Cross-sectional team from organisation that deal with incident response.
- Liase with law enforcement and national bodies (if deemed appropriate):
  - Computer Emergency Response Team (CERT) UK
    - GovCertUK, MODCert
  - National Crime Agency (NCA)
    - National Cyber Crime Unit (NCCU)
  - Centre for Protection of National Infrastructure (CPNI)

People and Security Culture

- Information assurance becomes useless if the people it aims to protect are not security-conscious.

- How can we create a security-conscious culture within the organisation?
  - *Need to understand procedures*
  - *… and to understand people.*

Security Awareness

- All employees should be aware of the risks that exist within the organisation – and why they are risks.
- Training needs to be relevant to the staff in order to be effective.
- Staff may be familiar with confidential issues – what about integrity and availability though?

Contracts of employment

- Terms and conditions of employment, with legal standing.
  - Responsibilities of the employee to the organisation
  - Obligations of the organisation to the employee

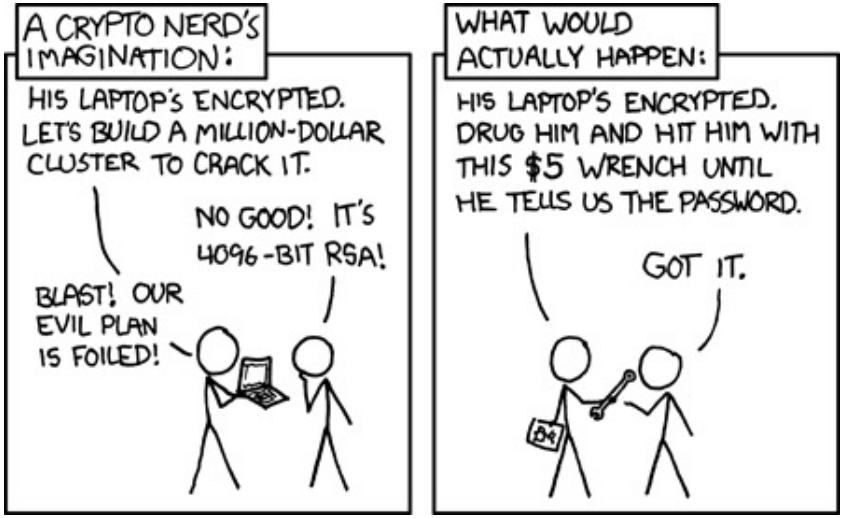
- Non-disclosure/confidential of information
- Acceptable use of company assets
- Ownership of intellectual property
- Acceptable standards of behaviour and conduct

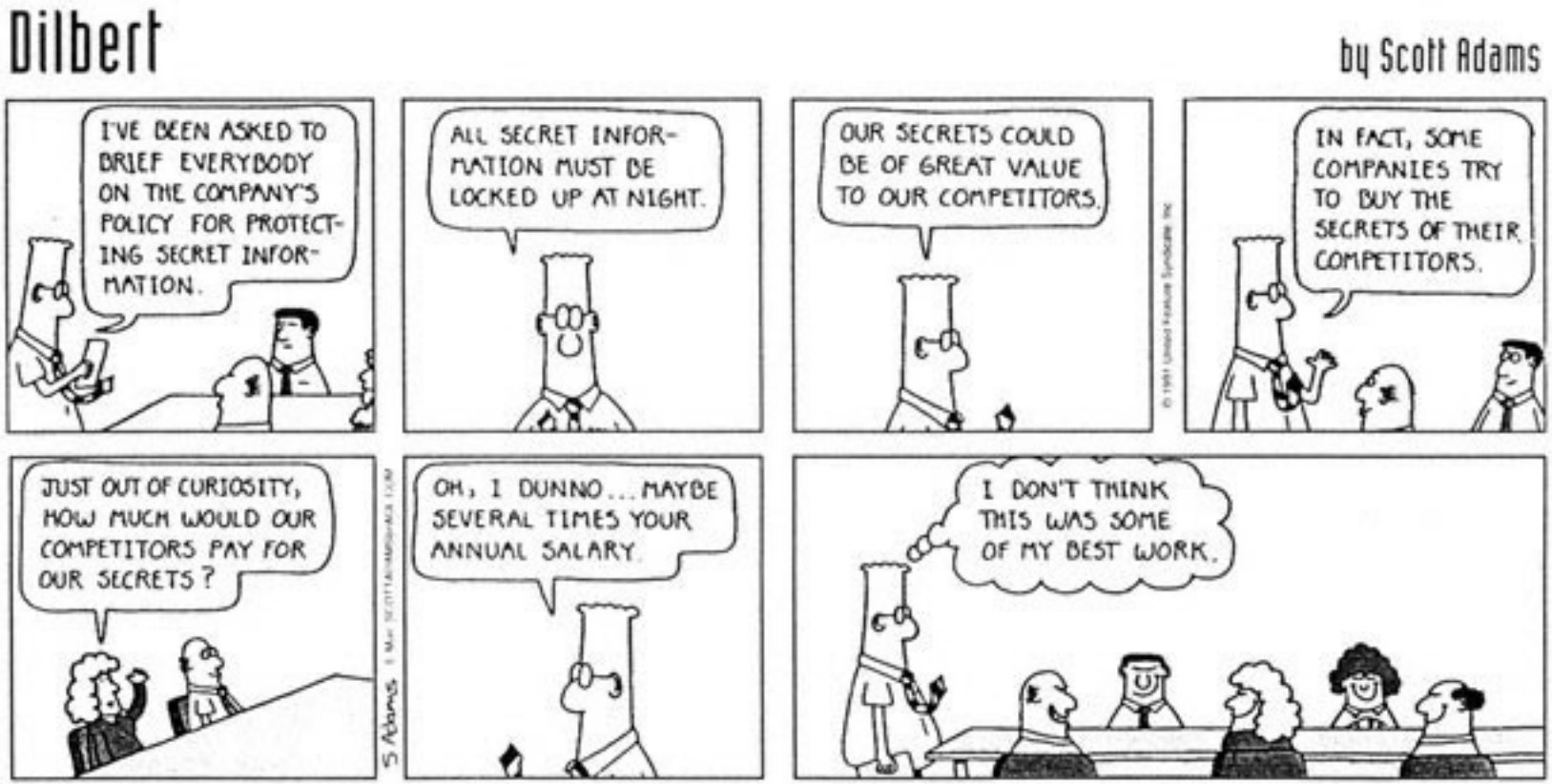
Segregation of duties and avoiding dependence

- One person may not perform the duties for more than one role where there could be a conflict of interest
- Limit scope that individual has to attack, or perform system misuse.
- Limit dependence that organisation has on any one individual.

Human Factors

- The greatest security vulnerability by far is the human
- Attackers will exploit social etiquette to conduct their attack.
- "Social Engineering" – to engineer a social situation that provides an advantage or a means of attack.





Discussion:
"What are the security challenges of social engineering?"

UWE Bristol | University of the West of England

Social Engineering – Passwords

- Passwords
  - Commonly used passwords (mother's maiden name, pet, school, teachers) are wide open to attack.
    - Attacker may attentively enquiry with victim.
    - Social Media is a big giveaway nowadays too!

Social Engineering – Passwords

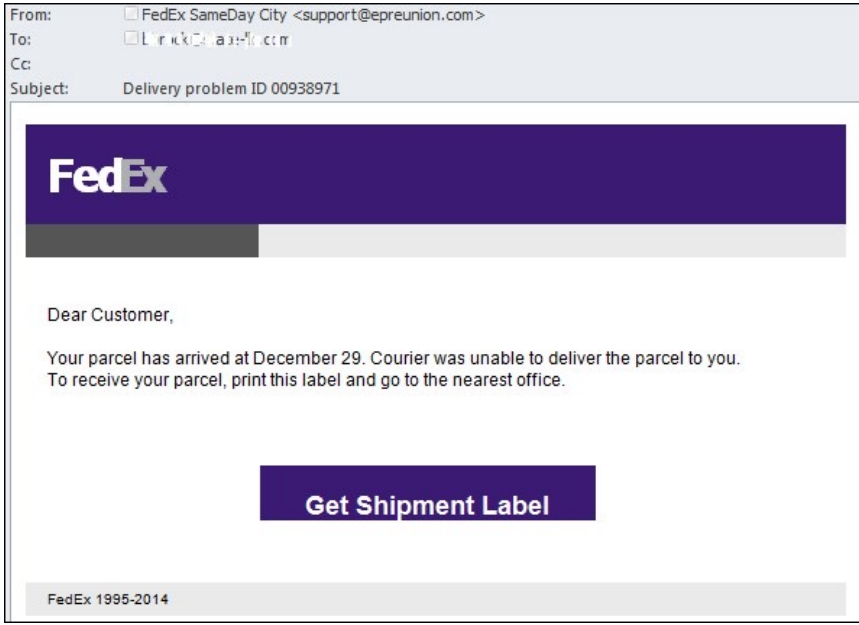
- 50% of Britons know someone whose account has been hacked
- One in six admit accessing someone else's account by guessing their password
- 10% have guessed a colleague's password
- Nearly half (48%) of those polled have shared a password with someone else
- Women are more likely to share their passwords than men, and over twice as likely to share it with their children
- As many as one in six use a password consisting of their pet's name

(https://grahamcluley.com/2013/08/pet-name-passwords/)

Social Engineering – Phishing

- Phishing e-mails still widely used and still quite successful among non-technical users.
- Spear-phishing e-mails are targeted towards particular users/organisations, with more specific details
  - More likely to be convinced this way!

- *"In the first quarter of 2015, the Anti-Phishing system was triggered 50,077,057 times on computers of Kaspersky Lab users. This is 1 million times more than in the previous quarter."*



UWE Bristol | University of the West of England

Social Engineering – Phishing

- Spear-phishing campaign impersonates as Snapchat CEO.
- Email requests payroll data for all employees.
  - Payroll department didn't notice it was a scam – they sent the details as asked.
- Employee personal data has been leaked – company now offering identity-theft insurance to employees as compensation.

- http://venturebeat.com/2016/02/29/snapchat-employees-targeted-in-phishing-attack-from-scammer-impersonating-ceo-evan-spiegal/

Social Engineering – Access

- What is social etiquette for holding doors open for others?
- Carrying heavy objects makes people more likely to comply.
- Who would ask to see ID to see whether this woman should have access?

Social Engineering – Theft

- E.g., A store operates security bag checks on staff at end of shift.
- Employee disguises stolen items by being ill in handbag!
- Should the security staff search the bag, despite being unpleasant…?
  - *Sounds extreme – but this was actually a real case that lasted months!*

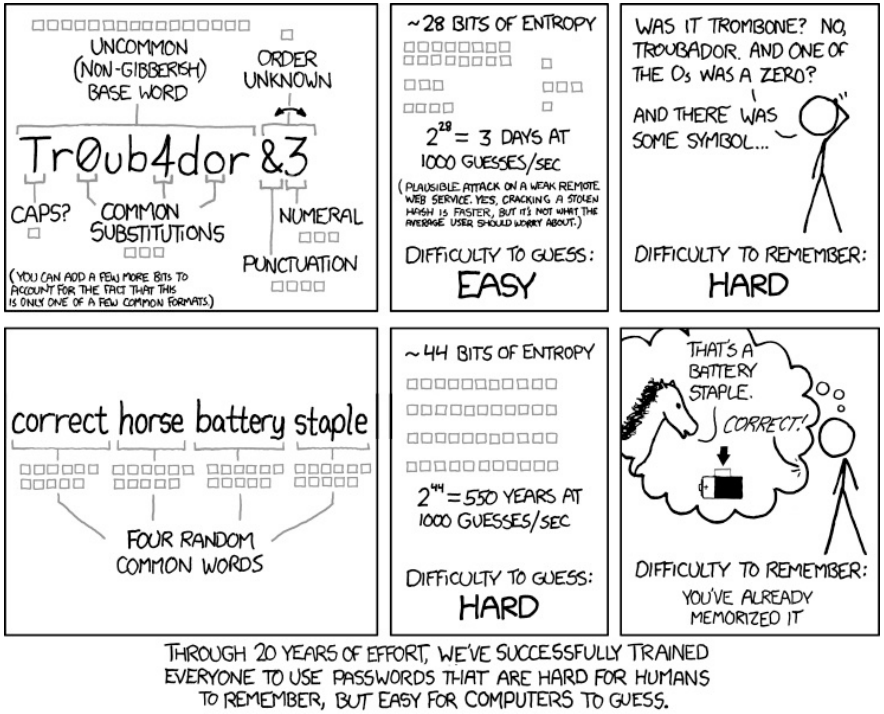
Vishing

- https://www.youtube.com/watch?v=lc7scxvKQOo

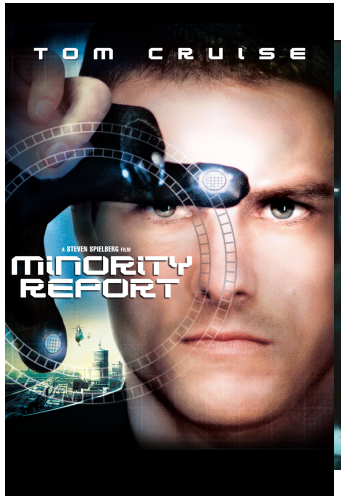
More social engineering

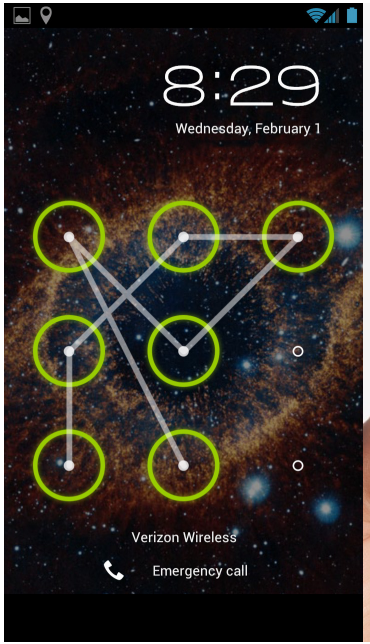
- http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411
- http://www.social-engineer.org/framework/general-discussion/real-world-examples/
- https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
- http://resources.infosecinstitute.com/social-engineering-a-case-study/
- http://money.cnn.com/2012/08/07/technology/walmart-hack-defcon/
- http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
- http://www.oii.ox.ac.uk/webcasts/?id=213
- https://lra.le.ac.uk/handle/2381/10288
- http://www.dummies.com/how-to/content/a-case-study-in-how-hackers-use-social-engineering.html
- http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack
- http://www.highbitsecurity.com/casestudies-socialengineering-hospital.php
- http://www.infoworld.com/article/2617997/security/ex-hacker-spills-secrets-of-fighting-social-engineering.html
- http://www.ieee-security.org/TC/SPW2014/papers/5103a236.PDF

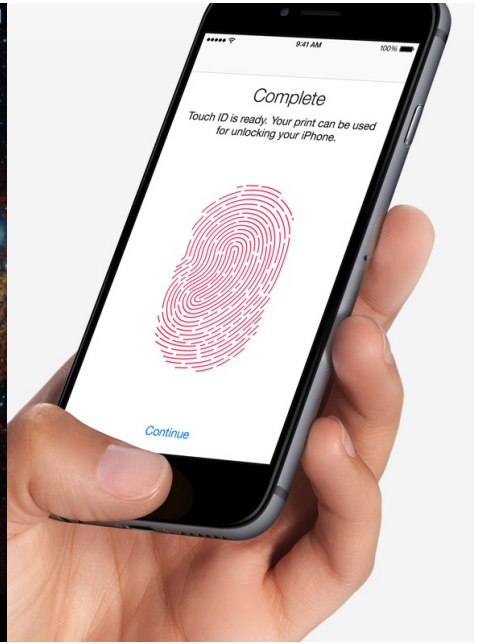
Technical Controls



Biometrics

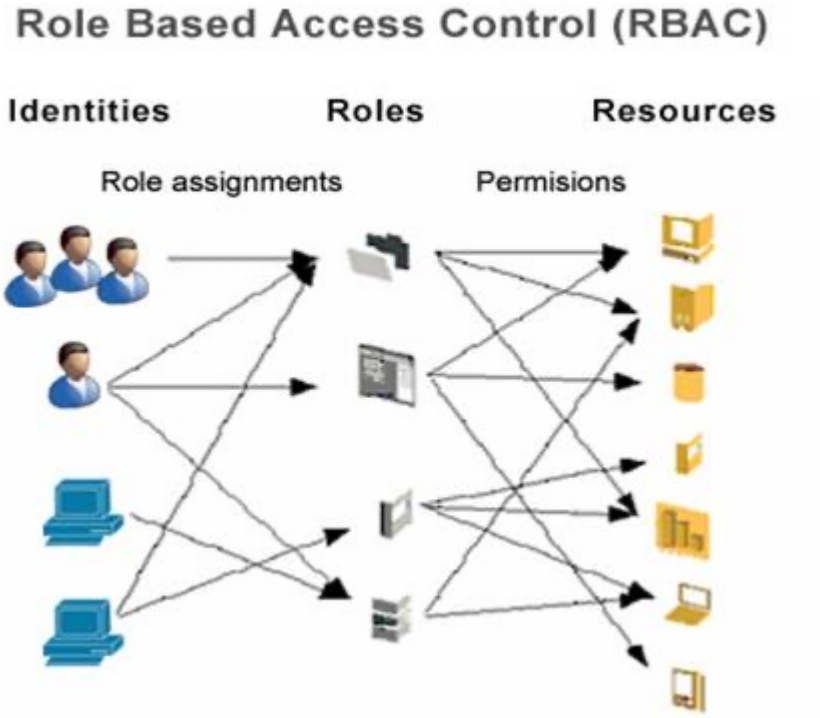

TOM CRUISE
A STEVEN SPIELBERG FILM
MINORITY REPORT


8:29
Wednesday, February 1
Verizon Wireless
Emergency call


Complete
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue

Role-based Access Controls

- 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!

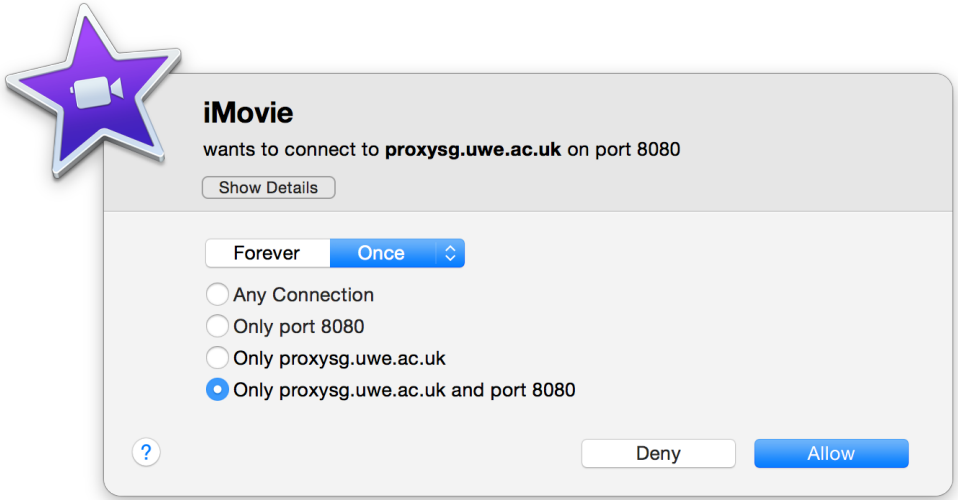


Anti Virus

- 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.



UWE Bristol University of the West of England

IDS / IPS

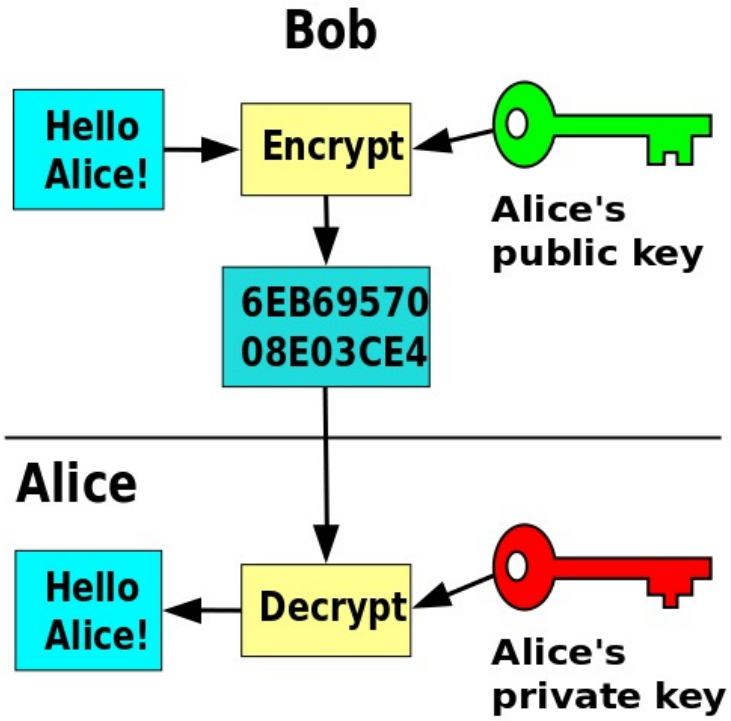
- Intrusion Detection Systems
  - Will alert to suspicious activity – e.g., Snort, BRO IDS.

- Intrusion Prevention Systems
  - Will alert AND will react to suspicious activity
  - E.g., automated response

- Many providers developing IDS/IPS solutions
- Incorporates ML techniques
- How to deal with false positives / false negatives?

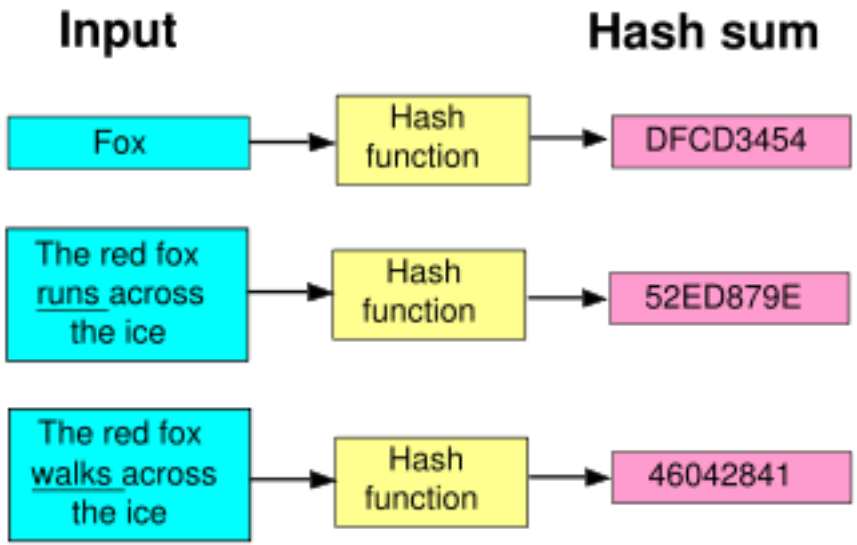
Cryptography

- 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)



Hash functions

- 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 Technical 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?

Physical Security

Clear Screen and Desk Policy

- How do we manage sensitive detail on a computer screen?
  - What if the user is distracted away from their desk? (e.g., making a coffee, vs. fire alarm).
  - Screensaver password – too short may cause frustration, too long may not be effective.
- How do we manage sensitive printed details?
  - Clear desk policy aims for no detail to be left on view.

Moving Information on and off site

- How do we manage data when it needs to be used offsite?
  - Need to avoid the "left it in the taxi" scenario!
- Inventory of offsite equipment – what is the procedure if this is lost/stolen/damaged?
- Remote access – only store the bare minimum locally?
- BYOD – what implications does this have?

Secure Disposal

- How should we securely dispose of data?
  - Many cases where data has been retrieved from hard drives after resale.
  - Secure delete by overwriting data with random data multiple times.
  - Better yet, physically destroy the disk! *(Recent price drops make this more feasible).*
  - Printed data should also be shredded
  - Avoid ‘dumpster divers’.

Guidance for Security Controls

- Information Security Forum (ISF)
  Standard of good practice: https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/
- COBIT (Control Objectives for Information and Related Technology) – another framework for IT management and IT governance, produced by ISACA. http://www.isaca.org/cobit/pages/default.aspx
- SANS Top 20 Critical Security Controls. https://www.sans.org/critical-security-controls/vendor-solutions/

- ISO27001: Annex A Controls
- NIST Cyber Security Framework

UWE Bristol | University of the West of England

Summary

- Primary objective of risk management is to identify suitable treatment options – mitigate where possible, else accept, remove, or transfer

- Controls may be Procedural, People, Technical, or Physical
  - A risk may have multiple controls across each of these domains

- Plenty of standards and guidelines exist for risk treatment controls
  - Need to determine suitability of controls for the business context
  - No “one-size-fits-all”