Cryptography Across Jurisdictions

Jack Bradbrook

Plan For this week

- Review some things from previous weeks.

- Try and get the legislation and legal topics out of the way so after this week we can cover protocols and recap some things.

Revisiting previous lectures briefly

- Having had a another look through the spec and the BCS website I just wanted to quickly tie some things together from previous weeks

- Review what is meant by certain terminology that might appear on the test.

- Recap one or two things.

Theory Of Cryptographic Techniques.

- From the Spec:

1.4 Show how poorly applied cryptography can become a threat vector. Indicative areas of study include, but are not limited to:
  - ECB mode
  - Collision attacks
  - Random number generation problems

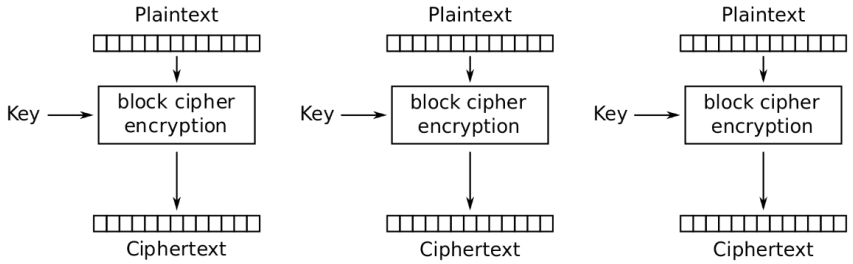
1.5 Explain the significance and role of entropy in cryptography and discuss security problems associated with entropy.

- Do we now have an idea of what collision attacks are?

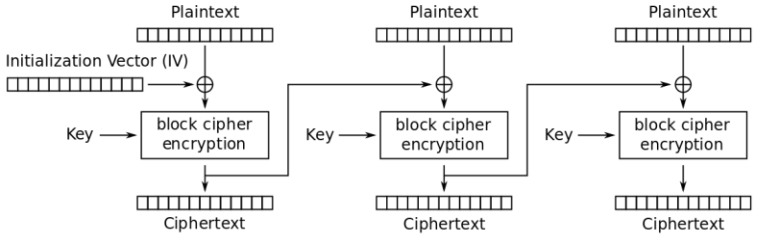
- Are any of us familiar with the term “Entropy” in relation to randomness?

Electronic Code Book (ECB) Mode Vulnerabilities, Recap

- Of the three main ways you can use block ciphers ECB, CBC, CFB, The Electronic Codebook (ECB) is the weakest.
- ECB is the Weakest because each bit of the key maps directly onto each part of the cipher text.
- With Cipher Block Chaining (CBC) and Cipher Feedback CFB Mode (CFB) we use the previous cypher text part of the message to influence the encryption of the subsequent parts. This adds confusion.



Electronic Codebook (ECB) mode encryption

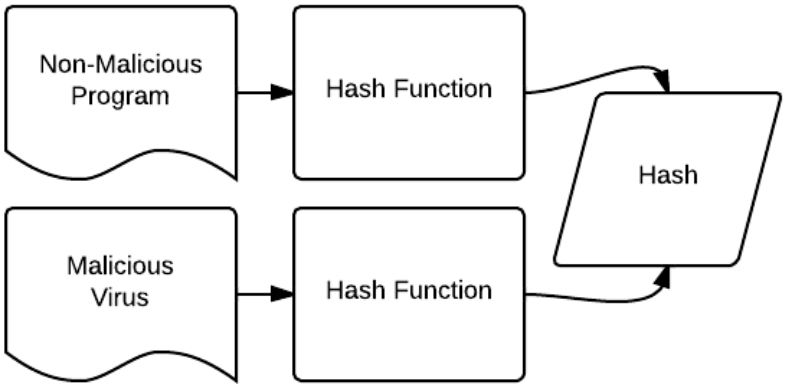


Cipher Block Chaining (CBC) mode encryption

Collision attacks

- A collision attack is where a Hacker has access to a hashing algorithm and tries to find an input which generates the same hash value as something else in order to fake authentication.

- For example I try and hash values to get the same result as a hashed string for a password, if I find a collision with the password hash I can hash the input I used as a valid Password to log in as that person.



Question From the Paper

4 A collision attack on MD5 attempts to find which of the following?

A Two messages that will produce two different hashes.
B One message that will produce two identical hashes.
C One message that will produce two different hashes.
D Two messages that will produce identical hashes.

Answer

D Two messages that will produce identical hashes.

“Jack teaches his lectures every Friday afternoon” -> “BC5351FFAE”

“BkYPqDpYPDjxxxh8YMrqzKoBoc7Yk8ytaRiyXorK8qCdIccg” ->“BC5351FFAE”

- We can fool people if we can produce identical hashes.

Entropy

- **Entropy** is how unpredictable something is.
- The higher the Entropy the more randomness there is.
- We've already been through this but I didn't use the term "Entropy"
- Remember the first lecture where we looked at random number generation and talked about what it meant for something to seem random.
- Importantly there's different levels of randomness.
  - In cryptography we don't use true random numbers we use pseudo random numbers.
  - We have to use pseudo random numbers that can't be easily predicted.
  - Using a natural source of randomness like Radiation is ideally better than using a potentially predictable computer method for generating random numbers

Question From The Paper

- Lets have a go!

5 Entropy in a computer system may be used for which one of the following purposes?

A To detect intrusion attempts by their signature.
B To verify passwords at login.
C To create session keys.
D To scan attachments for threats.

Answer

C To create session keys.

- We know the main purpose of generating random values in cryptography is to produce secure keys. Random keys prevent patterns from appearing in the cipher text.
- If an attacker can generate the same session keys as us using a the process then they can break into our system.
- If our method isn't very random then patterns will exist in the cipher text that can use to determine the key.
- If the key is very random then it has a high **Entropy.**
- If in doubt about this go back to the first lecture we did (02CryptographyIntroduction)

Deployment of Cryptography:

- From the Spec:

2.4 List some of the practical issues encountered in implementing cryptography. Indicative areas may include, but not be limited to:

- Historical consideration of broken cryptographic systems
- Theoretical vs practical security

Historical Consideration of Protocols

- In the past Cryptographic protocols relied on obscurity more than robustness of the algorithm
- The Caesar cipher is easy for anybody to break without a computer if they know that the cipher text is encoded with that cipher.
- In Modern Cryptography systems need to adhere to Kerckhoffs's principle.
- I.e. “A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.”

Theoretical VS Practical Security

- Most of the time we talk about cryptography from a theoretical perspective.
- We want to know secure an algorithm is against an attacker who is very intelligent and has a lot of computing power, people like the NSA, GCHQ etc.
- How secure can we possibly make our communications as secure as possible.

In Real Life

- In Real life there are financial and organisational costs associated with cryptography.
- It adds complexity to IT infrastructure.
- It can make it harder for some people who need to use data to easily access it.
- In most cases people in the outside world don’t care about most of the data an organisation produces.

Getting the Balance Right

- The key to real world security is understanding the tools available and deciding when they do and don't need to be used.

- Are you sending classified information for the MOD where hackers are likely to try and access the information?

- Or are you managing a web server for a local library?

- This is largely why we have Regulatory frameworks and standards to help us make decisions about which protocols and algorithms to use.

Regulatory Bodies and Resources

Topics:

- To meet the course criteria we need to look at legal issues and regulating bodies involved in cryptography and cyber security:

- Today we will aim to

Cover all of the following:

3. Cryptography across jurisdictions (20%, K2)

In this key topic, the apprentice will discuss legal issues relevant to cryptography (particularly when crossing national borders) and describe UK, EU and US export control of cryptography and the Wassenaar Arrangement. Outcomes should include an ability to:

3.1 List the regulatory frameworks in place in different jurisdictions, covering such topics as:
- International Traffic in Arms Regulations
- DPA
- FoI
- The Combined Code
- Sarbanes-Oxley and their areas of governance
- RIPA 2000
- Key escrow
- International Data Encryption Algorithm (IDEA)

3.2 Describe some of the legal issues related to cryptography with respect to national borders.

3.3 List a range of resources available to obtain advice concerning cryptography and security. For example, but not limited to:
- CAVP
- CVE lists
- Open vs. closed reviews
- ISO
- OWASP
- SANS
- NIST
- NCSC

Legal Acts:

- International Traffic in Arms Regulations
- The Data Protection Act
- Freedom Of Information Act
- The Combined Code
- Sarbanes-Oxley and their areas of governance
- Regulation of Investigatory Powers Act 2000
- International Data Encryption Algorithm (IDEA)

- In order to meet the module specification we need to talk about some legal issues and pieces of legislation that involve cryptography

Export Control

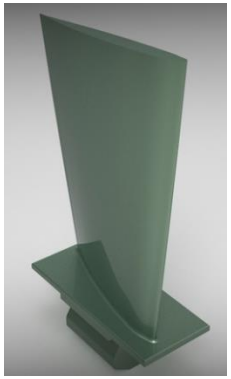
- Most developed countries have some form of what is known as **Export Control**.

- **Export Control** exists to prevent science and engineering that has potential military applications from being exported outside of a country either deliberately or accidentally

- The government must first decide that export of these items is ok to the recipient state.

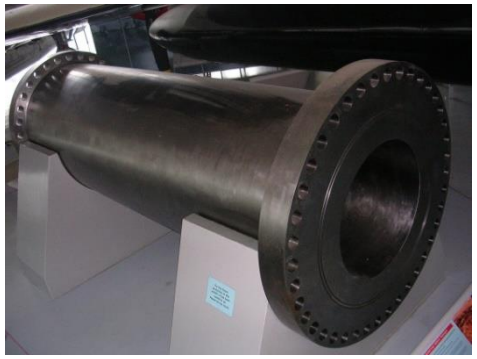
Dual Use in Export Control

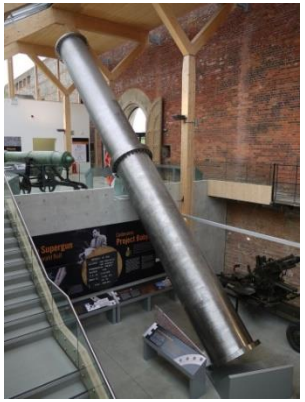
- Exports don't need to be specifically military related to be regulated by Export control law
- If an object has the ability to pose a threat when used differently by somebody else it's referred to as being **dual use** and is also controlled by export control law.
- Cryptography can be considered a technological development which has military applications, even though it also has many civilian applications



Example Project Babylon:

- In 1991 the Iraqi government commissioned the production of huge pieces of steep tube to be made in the UK.
- These pieces of tube were said to be part of an oil pipeline.
- Actually part of an enormous gun designed to fire warheads into neighbouring countries.
- Finally stopped half way across Europe after leaving the UK.





International Traffic in Arms Regulations

- "**International Traffic in Arms Regulations** (**ITAR**) is a United States regulatory regime to restrict and control the export of defence and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives."

- "Until 1996–1997, ITAR classified strong cryptography as arms and prohibited their export from the U.S."

- Export control body: What does this mean and why is it important?

International Traffic in Arms Regulations (ITAR)

- Controls the export of:

- **Defence Articles** – Guns, Aircraft, Satellites and Software, these are items that are used for defence.

- **Defence Services**
  - Helping to assist foreign parties with acquiring Defence Articles,
  - Providing technical data to a foreign party
  - Providing military training to a foreign party

What actually is an Export?

- In the US and the UK If you move an article outside of a country's jurisdiction even for an instant you have exported it.
  - This includes transferring data over servers based in different country's

- If you are within a country's jurisdiction but you show information which is considered an **article** to a member of another country then you have exported that article.

  - E.g. you show somebody the designs for an aircraft without actually giving them the designs.
  - This is called a **Deemed Export**
  - The person may not have a physical copy of the data but if they gained an understanding of the technology and they can recreate it from memory then it has been exported.

Jurisdiction lists

- An export is deemed ok based on two variables:
  - The item or service being exported
  - The country that it is being exported to

- Countries are grouped into categories based on the deemed level of threat of exporting to those countries based on national intelligence, each category has a level of risk associated with exporting arms to countries in that category for example:

Schedule 4 Countries.
The countries listed below are subject to military end-use controls:

- Armenia and Azerbaijan
- Belarus
- Democratic Republic of Congo
- Democratic People's Republic of Korea
- Iran
- Iraq
- Ivory Coast
- Lebanon
- Liberia
- Libya
- Myanmar (Burma)
- Republic of Guinea
- Sierra Leone
- Somalia
- South Sudan
- Sudan
- Syria
- Zimbabwe

Software as Defence articles

- Some general examples of Defence articles are:
  - Certain Cryptographic Algorithms.
  - Embedded software on military arms, e.g. software running on an aircraft or missile.

- Organisations that develop or handle this kind of software can face legal action if they face an audit and the audit finds they have failed to adhere to export control policy.

- These organisations should have measures in place to manage how they work on and control the distribution of such software.

Regulation of Investigatory Powers Act 2000 (Updated in 2016) (RIPA)

- UK legislation that gives Government bodies (Police, MI5, GCHQ, NHS, Tax Authorities etc) the right to do the following:

    1. Demand access to a customers surveillance from Internet Service Providers (ISPs)
    2. Allow mass surveillance of communications
    3. Demand ISPs fit equipment to facilitate surveillance
    4. Demand Access is granted to protected information
    5. To allow monitoring of an individuals internet activities
    6. Prevent resistance of internet activities being revealed in a court of law.

- The body does not need to provide a reason to do the above.

Reference: http://www.legislation.gov.uk/ukpga/2000/23/contents

Regulation of Investigatory Powers

- Extremely Controversial Legislation.

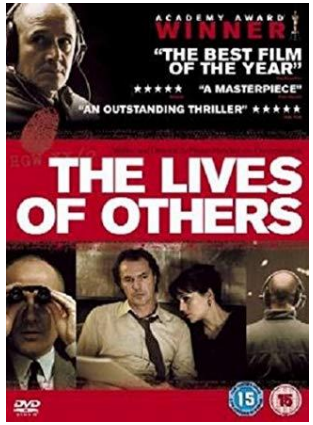
- Arguments for it:
  - If you can access peoples internet traffic and personal information you can more easily stop paedophiles, terrorists, people who cause harm to everyone else.
  - If you aren't a bad person then you have nothing to hide so why do you care about privacy?

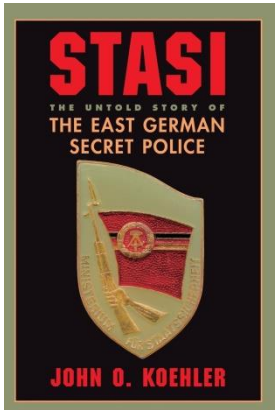
- Arguments against it:
  - Personal and political freedom is based on the privacy of individuals and their confidence in that privacy.
  - If the government knows everything you do and your views then they have the ability to stop you either with direct force or manipulation.
  - If you disagree with the government and their position then the government has the ability to stop you.
  - Democracy is vulnerable without personal and political freedom.

- If we have time: https://www.youtube.com/watch?v=6KoC1b8XBC0

Example: The Stasi

- During the cold war the soviet controlled government in East Berlin ran the biggest surveillance operation ever undertaken on the general public.
- 2% of the entire population of east berlin were working as spies so 1/50 people you met would report you to the secret police if you said something unfavourable about the government.
- You wouldn't know who was and wasn't a spy so you had to assume everyone was.
- The state listened to peoples phone calls and sent spies to befriend political activists to learn information about them.
- https://www.youtube.com/watch?v=ha1jM9HAs6c





Sarbanes-Oxley Act (SOX)

- An Act passed in the United States in 2002

- All publicly traded US companies must comply.
- Idea is to increase public confidence in companies and prevent investor fraud.

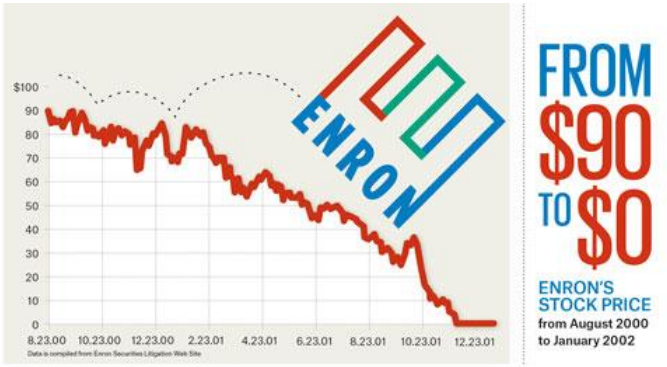
- A large company is generally a stable company unless:
  - The industry it works within is hugely damaged or changed by a shift driven either by the economy as a whole or technology.

  - E.g. Financial crash
  - E.g. Technological / paradigm change leaving the companies product obsolete (Kodak/ Blockbuster).

  - There is fraud committed within the company meaning that the information about the stability of it is not accurate

Historical Fraud

- The Sarbanes-Oxley Act was introduced after senior figures in several large companies were revealed to have committed fraud by altering or deliberately hiding the companies accounting data.
  - This lead investors to believe the company was doing better than it actually was.
  - This is illegal.
  - Before Sarbanes-Oxley this was very easy to do.



- https://www.youtube.com/watch?v=Mi2O1bH8pvw

Fraud Prevention with SOX

- Requires The Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) of companies to sign off the accuracy of the companies financial statements.

- Makes people at the top of a company accountable for the finances of a company.
  - They can personally go to jail if investor fraud is committed.

- Company must provide a description of its internal processes, how company manages its staff, what security measures it takes to protect its data etc.

- Company must hire an external financial auditor to validate the accuracy of their accounting.

SOX and Cyber Security

- SOX requires organisations to have:
  - "systems in place that protect against data tampering - both internally by unauthorized personnel as well as externally by malware or hackers."
  - "security systems that can protect the handling of data which should be verified independently. All data must be made available to auditors, including financial records as well as any potential security breaches."
- Essentially the IT security adopted by a company should prevents its own staff as well as hackers from tampering with the financial data of that company

The Data Protection Act (DPA)

- Controls How Personal Information is used by Organisations, businesses and Governments.
- If an organisation looses your personal data you must be informed within 3 days.
- Failure to meet the DPA can result in large fines (up to 4% of organisations turn over)
  - Strong incentive for companies to take it seriously!

https://www.gov.uk/data-protection

What is Personal Information

- Personal information is information which can be used to identify a person such as their:
  - Name
  - Contact Details
  - Location
  - Race
  - Sexual Orientation.

What does the DPA say?

- Personal data must be:
  - Used fairly, lawfully and transparently
  - Used for specified, explicit purposes
  - Used in a way that is adequate, relevant and limited to only what is necessary
  - Accurate and, where necessary, kept up to date.
  - Kept for no longer than is necessary.
  - Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

General Data Protection Regulation (GDPR)

- New European Law on data protection and Privacy which came into affect in 2018, the regulation aims to achieve similar aims as DPA. Most organisations care more about GDPR than the DPA.

- The following are the key principles of GDPR:

1. Lawful, fair and transparent - *There has to be legitimate grounds for collecting the data and it must not have a negative effect on the person or be used in a way they wouldn't expect.*

2. Limited for its purpose - *Data should be collected for specified and explicit purposes and not used in a way someone wouldn't expect.*

3. Adequate and necessary - *It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected.*

4. Accurate - *Reasonable steps must be taken to keep the information up to date and to change it if it is inaccurate.*

5. Not kept longer than needed - *Data should not be kept for longer than is needed, and it must be properly destroyed or deleted when it is no longer used or goes out of date.*

6. Integrity and confidentiality - *Data should be processed in a way that ensures appropriate security, including protection against unauthorised or unlawful processing, loss, damage or destruction, and kept safe and secure.*

Exercise Take a few minutes:

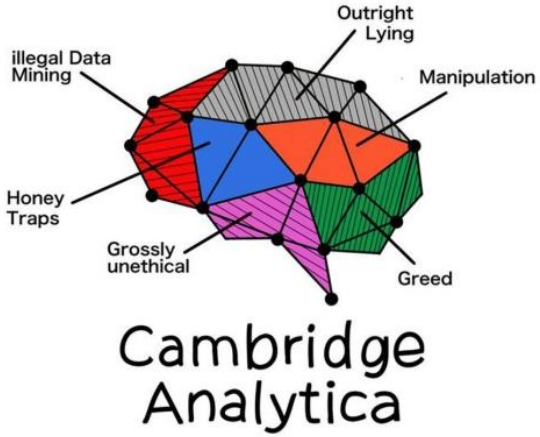
- Why do we need the Data Protection Act and General Data Protection Regulation?
- What would happen if there weren't laws regarding Data Protection?
- Why can't we expect companies to protect personal data by themselves?

Some Considerations:

- Without legislation companies can do whatever they want with the data they have.
- The task of a company is to make money.
- Personal data is extremely valuable, a large set of personal data tells somebody a lot about a big group of people.
- Data allows organisations to better understand individuals, what their opinions, desires and fears are.

Example: Cambridge Analytica

- Facebook + Cambridge Analytica scandal
- Probably the best known widespread misuse of personal data in recent years.
- Peoples information was taken without their knowledge and used for a purpose they had no knowledge of.
- https://www.youtube.com/watch?v=zb6-xz-geH4

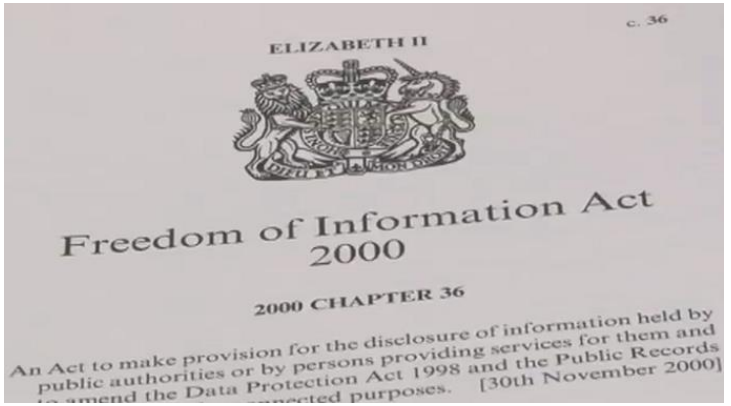


The Freedom of Information Act (FOI)

- The Freedom of Information Act 2000 provides public access to information held by public authorities.

- It does this in two ways:
  - public authorities are obliged to publish certain information about their activities; and
  - members of the public are entitled to request information from public authorities.

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/



Why Do we have FOI?

- On Principal the governments activities are funded by Tax Payers (The people of the state) Those people are affected by the activities of the government.

- Those people have the right to find out what their money is spent on and how actions taken by the government may affect them.

Exceptions to FOI

- The Freedom of Information act does not permit access to be granted access to certain specific pieces of information such as:
  - Information accessible by other means
  - Information supplied by, or relating to, bodies dealing with security matters
  - Court records, and information held in relation to court proceedings
  - Prejudice to effective conduct of public affairs
  - Personal information – Protected by Data Protection Act
  - Information provided in confidence
  - Information whereby disclosure is prohibited by an enactment or would constitute contempt of court

Resources For Legislation

- Tools/ Services:
  - Cryptographic Algorithm Validation Program
  - Common Vulnerabilities and Exposures lists
  - Open vs. closed reviews
- Educational Organisations:
  - Open Web Application Security Project
  - International Organization for Standardization
  - Escal Institute of Advanced Technologies
- National Institute Of Standards And Technology
- National Cyber Security Centre

Tools and Services

Common Vulnerabilities and Exposures (CVE Lists)

- A public Dictionary of cyber vulnerabilities.
- Before 1999 different cyber security tools had their own databases of different vulnerabilities in protocols and other pieces of software
  - This made it more time consuming to be sure if something had a security vulnerability.
  - This meant it was hard to see if the different security tools were actually referring to the same vulnerability in a piece of software/ protocol.
- CVE Website: https://cve.mitre.org/about/index.html

National Cyber Security Centre (NCSC)

- Government Organisation working to improve cyber security across the UK by bridging the gap between Industry, Government and academia.

- Provides advice to organisations on how to keep themselves secure, alerts organisations to security threats being experienced by other organisations at that time.

- Aims to add cyber security at a national infrastructure level.
  - For example preventing known spam addresses from outside the UK sending anything into the whole of the UK

- https://www.youtube.com/watch?v=P6YZHsppgLU

National Cyber Security Centre

a part of GCHQ

The Combined Code (I missed this topic out in lecture, will go over)

- Now more commonly known as the UK Corporate Governance code.
- The system by which companies are controlled by the government.
- Boards of Directors are govern companies.
- The shareholders are the owners of a company but they are not directly responsible for the governance of the company
- The shareholders role in governance is to appoint directors and auditors that provide them with confidence that appropriate government of the company is taking place.

The Board of Directors

- The board of directors is responsible for setting the companies strategic aims and providing leadership to put them into effect.

- The boards actions are subject to laws, regulations. They are judged by the stakeholders and determine the success or failure of a company.

Poor behaviour of companies

- Companies have been known to engage in illegal conduct:
  - Diverting funds from pensions
  - Laundering criminal money
  - False accounting.

IT Crowd: Irregularities in the pension fund scene:
https://www.youtube.com/watch?v=cEpKcBkkVMY

Stakeholders

- A stakeholder is anybody who has an interest in a company.
- Most people think of stakeholders in terms of:
  - Shareholders
  - Employees
  - Customers
  - Suppliers
  - The government (Tax)
- These are what is known as **Financial Stakeholders** If the company looses money, they lose money

Interest Stakeholders

- In addition to **Financial Stakeholders** there are also **Interest Stakeholders.**

- Interest stakeholders don't make or lose money based on the companies performance but the way the company conducts itself does affect them.

- They Include:
  - **Activists** e.g. environmental activists
  - **Competitors** e.g. if a company breaks the rules then a competitor feels more pressure to do the same to remain competitive
  - **Media e.g.** The media reports on events which affect companies and their conduct
  - **Regulators** e.g. Auditors, The Stock Exchange.

Corporate Social Responsibility

- Companies are encouraged to consider the impact that their business has on wider society

- Corporate Social Responsibility is about ensuring that sustainable development happens within the company so that there are benefits for all stakeholders (economic, social and environmental)

Open Web Application Security Project (OWASP)

- Non profit Organisation dedicated to web application security.
- All material is freely available.
- Documentation, tools, videos and forums to help developers make applications more secure.
- Open project – Anybody who discovers a way to improve application security can contribute to OWASP

OWASP

Open Web Application Security Project

Escal Institute of Advanced Technologies (SANS)

- US based company which provides training and certification on a range of cyber security topics including:
  - Network defences
  - Penetration Testing
  - Digital Forensics
  - Security Auditing
- Their YouTube Channel is worth checking out for good material on computer security: https://www.youtube.com/user/TheSANSInstitute/videos?view=0&sort=p&flow=grid

Standards

International Organization for Standardization (ISO)

- Independent non governmental organisation with members from 164 countries
- Develops and manages International standards in order to ensure quality and consistency across organisations across the globe
- Standards are created for everything you can possibly think of from how to run businesses to how medical software should be designed and written.

ISO

Why ISO is important

- Often in order to bid for government work or work within a regulated industry a company will need to prove it meets a range of different ISO standards so as to provide assurance to the government that the company works according to best practices.

- E.g. Your company needs to write software according to ISO13485 in order to be considered to write medical software Properly.

- A company you want to work with in the medical industry needs to know that you do this correctly before they are prepared to work with you.

- https://www.youtube.com/watch?v=oq1Zi_V4KyE

ISO and cyber security

- ISO 27000 standards are all based around helping organisations improve their cyber security.

- Currently there are 46 individual cyber security standards

- The most significant standard is ISO 27001

ISO 27001

- Provides specification for Information Security Management System (ISMS)
- This system provides a framework for how an organisation manages the risks associated with cyber security issues that could compromise their business critical information.
- Can be applied to any kind of organisation of any size.

What does ISO 27001 give us?

- It aims to help an organisation preserve the following with regards to its data:

  - Confidentiality
    - Only authorised individuals can access the information
  - Integrity
    - Only authorised individuals can change the information
  - Availability
    - The information has to remain available to all the legitimate people who need it within a specified time

How does it provide this

- The framework requires an organisation to have Controls also known as **Safeguards** in place, safeguards can be any measure used to help provide Confidentiality, Integrity and Availability.

- Say I work at a company and I want to take my work home on a memory stick.

- The company should have safeguards in place if it follows ISO 27001 to preserve the Confidentiality, Integrity and Availability of the data on that memory stick.

- This could include:
  - Making sure the Memory stick is encrypted.
  - Making sure the password to decrypt the memory stick is adequate.
  - Making me as the employee sign a statement when I join to say that I am accountable if I decrypt the contents of the memory stick while at home and there is a leak of the data.

ISO 27001 Conclusion

- ISO 27001 has many benefits to organisations such as helping organisations which use it to remain compliant with The Data Protection Act.

- Animated overview of the standard: https://www.youtube.com/watch?v=io6w3Yw4q9w&

National Institute Of Standards And Technology (NIST)

- Organisation for controlling and regulating measurement standards.
- Based in the USA.
- Doesn't try to provide standards for everything like ISO, just measurement, this is crucial for technological development including cryptography.
  - We need measurement standards to judge how secure cryptographic methods are

Cryptographic Algorithm Validation Program (CAVP) – Part of NIST

- Program for validating security of cryptographic algorithms.
- If someone invents a new cryptographic algorithm and wants to put it on the market place there needs to be some reassurance that it is secure before people have the confidence to buy or use it.
- CAVP performs testing on new algorithms and signs them off as being considered secure enough for general use if it passes all of the tests.

CAVP

Cryptographic Algorithm Validation Program

CAVP certification

- Once validated an algorithm is allowed to be used by government departments for encrypting sensitive but not classified information:
  - Classified: Requires protection against unauthorised disclosure for reasons of national security.
  - Sensitive: Information not designated as classified but warrants enhanced protection. E.g. personal data, general government/ corporate data

CAVP Approved Algorithms and Protocols

CAVP currently has already verified the following protocols and will continue to check any changes which are made to them:

Block Ciphers	AES, Triple DES, Skipjack (decryption only) Tests for ECB, CBC, CFB and OFB modes.
Block Cipher Modes	CCM, CMAC, GCM / GMAC / XPN, Key Wrap, XTS
Digital Signatures	FIPS 186-4: DSA, ECDSA, RSA FIPS 186-2: DSA, ECDSA, RSA
Key Derivation Functions	KBKDF
Key Management	KAS
Message Authentication	HMAC (FIPS 198-1)
Random Number Generation	DRBG
Secure Hashing	SHA-2, SHA-1 SHA-3

Reference: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

Cryptography and National Borders

- Different countries naturally are suspicious of cryptographic algorithms developed within other countries.

- Many Cryptographic algorithms in the past have been developed by the National Security Agency (NSA) in the US which is an arm of the government. Likewise in the UK much cryptographic work has been done by the Government Communications Headquarters (GCHQ)

Cryptography and National Boarders

- Edward Snowdon revealed that some of these algorithms had known flaws which the NSA used or deliberately placed within the algorithms in order to break into encrypted traffic upon their adoption by the general public and other states.

Open Vs Closed Standards

- Most open source encryption methods are open to scrutiny from anybody, anyone can download the source code and run it themselves.
  - This is how they gain international trust.

- By contrast government software used for military applications is often not open. The general public never get to see the source code.

- It’s important that we have open reviews for public cryptographic algorithms. If there is a vulnerability it’s important that whoever finds it is able to voice their concerns.

Open Vs Closed Reviews

- We can take an open and closed approach to reviewing tools and software as well:

- **Open Reviews**
  - Anybody can leave a review.

- **Closed Reviews**
  - Only specific verified people can leave reviews on something.

Cryptography and National Boarders in relation to GDPR

- When transporting personal info between European countries over the internet or otherwise it is a legal requirement to adhere to encryption standards specified by the GDPR.

How should we implement encryption?

- When implementing encryption it is important to consider four things: choosing the right algorithm, choosing the right key size, choosing the right software, and keeping the key secure.
- Over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. You should regularly assess whether your encryption method remains appropriate.
- It is important to ensure that the key size is sufficiently large to protect against an attack over the lifetime of the data. You should therefore assess whether your key sizes remain appropriate.
- The encryption software you use is also crucial. You should ensure that any solution you implement meets current standards such as FIPS 140-2 and FIPS 197.
- Advice on appropriate encryption solutions is available from a number of organisations, including the National Cyber Security Centre (NCSC).
- You should also ensure that you keep your keys secure, and have processes in place to generate new keys when necessary to do so.

Next Week and beyond…

- Next Week:
  - Cryptographic Protocols:
  - Defining protocols,
  - Quick review of the IP protocol stack,
  - Tunnelling/ IPSec, SSL,
  - HTTPS
  - GSM,
  - Key Escrow

- Week after:
  - Revision
  - Probably go back to block ciphers and look at some specific examples of them to clarify their usage.
  - Look at some cyber attacks on protocols and algorithms.
  - Designing policies and practical considerations.