CS5285
Information Security for eCommerce

Prof. Gerhard Hancke
CS Department
City University of Hong Kong

1

Plan for today is admin, gentle introduction to information security!

Teaching Team

- Instructor:
- 

Teaching Materials

- Weekly lecture slides
  - Will be on Canvas few days before class.
  - After lecture will also put slides with additional comments
- Textbook:
  - William Stallings, *Cryptography and Network Security – Principles and Practices (any edition 3 – 8)*
    - *Additional reading and reference – core work in slides.*
- You have to check Canvas!
  - Announcements (these go to CityU email)!
  - Problem sets, tutorial solutions, etc.

3

Weekly Teaching Pattern

- Lecture (2 hours) 14:00-15:50
  - Traditional Lecture
  - Discussion on set reading/case studies
- Tutorial (1 hour) 16:00-16:50 (AC5 416) or 17:00-17:50 (AC5 417)
  - Theory course – we do problems/exercises on paper
  - Weekly question sheet
    - On Canvas (do not need to submit your answers)
  - Discussion
    - Open discussion 16:00-16:30/17:00-17:30
    - Discussion on tutorial solutions starts approximately 16:30/17:30
- 'Homework'
  - Short extra reading, usually on real-world events/systems with one or two questions.
  - Optional exercises…if you submit you get the answer
- Recording of Lecture and Tutorial session will be made available.

4

Assessment

- **40% course work**:
  - 2 take home problem sets (10% each)
    - Due in week 6 and week 13 (15 October, 3 December)
    - Late submissions get **zero** mark
  - 1 midterm-quiz (20%)
    - Midterm-quiz in week 7 (22 October)
- **60% final examination**
  - Must achieve minimum 30% mark in final examination

5

Plagiarism not tolerated!

Do not copy any source without proper citation/referencing.

ChatGPT

- Students are not allowed to use GenAI for any programming tasks, *or to solve any numerical/logic problems*.
- For writing assignments and reports, students are allowed to use GenAI, but its use must be acknowledged through proper citation and referencing.

6

Course Overview

Intended Learning Outcomes

Upon completion of the course, students should be able to:

1. Identify the organizational requirements of eCommerce systems on data protection.
2. Demonstrate knowledge of the factors which have impacts upon the security of eCommerce systems.
3. Make critique and assessment on the security of eCommerce systems.
4. Describe relevant regulations governing electronic transactions, data privacy protection, and web access.
5. Create design and analyze security mechanisms to protect eCommerce systems and transactions.

8

Understand the goal of the course

- This is a MSc module
  - This course does not require a background in security
  - Potentially lots of different student backgrounds here
  - This serves as an introductory course on information security
    - Mostly studying foundation cryptography and security protocols
    - The real-world relevance of basic principles are illustrated using e-commerce examples
- So course satisfaction is also your responsibility!
  - If you know everything come talk to me
    - We can do more – extra reading or personal discussion
  - If you think it is all too much talk to me
    - Unfortunately we cannot do less – but I can help you more
  - Any problem with course– talk to/email me! I am friendly!

9

Tentative Course Overview

- Week 1: Admin and Basic Security Terminology
- Week 2: Symmetric encryption
- Week 3: No class
- Week 4: Symmetric encryption
- Week 4: Number Theory/Asymmetric Encryption (29 Sept)
- Week 5: Integrity
- Week 6: Authentication (Problem Set 1)
- Week 7: Mid-Term Quiz
- Week 8: Key Management
- Week 9: Key Management
- Week 10: Computer Security
- Week 11: Network Security
- Week 12: Network Security
- Week 13: Revision (Problem Set 2)

Lecture 1

Introductory Security Concepts

11

Today's Lecture

- Information security
  - Basic concepts and terminology
- Where to find security protocols/algorithms?
  - Brief discussion of standards
- CILO1, CILO2 and CILO3

  (Security requirements and threats that impact systems, and basic standards for design)

12

What is a ‘security’?

- The security of a system, application, or protocol is always relative to
  - A set of desired properties: what do want to achieve?
  - An adversary with specific capabilities: what can they do?
- Why is this important?
  - Is good security not always secure?
  - We need to think: Appropriate? Strength? Cost?
  - Unconditionally vs computationally secure?

13

Study

We also design a secure system based on two things:
What security (service) do we need?
How powerful an attacker to we want to defend against?

What is the difference between theoretically (unconditionally secure) and computationally secure?

Theoretic security is always secure under all circumstance. This is difficult – for example no encryption algorithm (except one-time pad) is theoretically secure as you can do exhaustive key search.

Computational security is when it is not practically feasible to circumvent a service. For example, I could brute force an AES encrypted message but given current technology it will take me many many years.

Sometime people also make a decision based on cost – if an attacker needs to spend more money breaking the security than what he would make by breaking the security it is considered secure. This works for certain types of attackers but is not always the best approach given that attacker motives are hard to predict – they might not want to make money!

Can we make everything ‘secure’?

14

Security is also not always about technology…

We need to think in more general terms of system security rather than just cryptography (crypto is important but being secure goes beyond that).

Majority of problems in real life secure systems is not directly due to weak crypto – but rather crypto used in wrong way or non-technical (user) issues that weaken security.

See video on canvas…

However, before we get there we must have a strong understanding of crypto mechanisms.

Information Security

- Security is about the protection of assets.
- Thus, **information security** is the basis for protecting our **information assets**.
- There are three broad classes of protection measures:
  - **Prevention**: prevent your assets from being damaged.
  - **Detection**: detect when you assets have been damaged, by whom and how.
  - **Reaction/Recovery**: recover your assets, or recover from the damage to your assets.

15

Study slide – know difference between prevent, detect and recover. Always think if we discuss a mechanism or service how are we protecting – are we really preventing an attack or are with only detecting it.

For example, we prevent the attacker from getting plaintext if we encrypt well but we cannot prevent modification during transmission (we can however detect it).

Basic Security Goals

- How can our information assets be compromised?
- The most frequently used definition covers three aspects of information protection:
  - **Confidentiality**: prevention of unauthorised disclosure of information.
  - **Integrity**: prevention of unauthorised modification of information.
  - **Availability**: prevention of unauthorised withholding of information or resources.
- Commonly abbreviated to: **CIA**.

16

This is the most basic security goals known as CIA triad/triangle (nothing to do with USA Central Intelligence Agency!)

Someone else gets hold of them, data is changed, someone prevents me from getting to them.

There are more services to these three, but these are seen as the core three.

Threats

- Security is only desirable when there is a need to protect a system from a threat.

- A **security threat** is a possible means by which a security policy may be breached (e.g. loss of integrity or confidentiality).
- **Countermeasures** are controls to protect against threats.
- **Vulnerabilities** are weaknesses in the system (and/or countermeasures).
- An ***attack*** is a realisation of a threat (exploiting a vulnerability).

In the context of this model, a *security threat* is something that poses a danger to a system's security.

You must know these terms and the relationship between them.

Threats

- Threats can be classified as:
  - **deliberate** (e.g. hacker penetration);
  - **accidental** (e.g. a sensitive file being sent to the wrong address).
- The associated threats which CIA are responsible for countering are:
  - **Exposure of data**: the threat that someone who is unauthorised can access the data.
  - **Tampering with data**: the threat that the data could be altered from what it should be.
  - **Denial of service**: the threat that the data or service is unavailable when it is required.

18

Study slide

For the three threats which is accidental and which deliberate? All three can be both.

How can we lose confidential data?

Left on the train? Stolen laptop? Sent in the mail (UK Tax data)

Adversaries

- People whose aim it is to circumvent your security are generally called **adversaries**.
  - Sometimes called **intruders**, but not all adversaries are external to the system (insider threats).
- Adversaries act in two different ways:
  - **Passive** adversaries only attempt to get unauthorised access to information
  - **Active** adversaries take more direct action:
    - Unauthorised alteration
    - Unauthorised deletion
    - Unauthorised transmission
    - Falsification of origin of information
    - Unauthorised prevention of access to information

19

Study slide (you should not memorise what active adversaries can do, rather just think anyone that is not passive is active)

Are adversaries always third parties? No they could be a party you are talking to.

Are they always outside attackers? No, what about malicious insiders – what if one of the employees gets angry with his boss and decides to delete some files.

Think!
Someone reads your email – active of passive?
Someone sends email to your friend pretending to be you – active or passive?

Adversaries

- When designing a system, it is important to consider the background and capability of your potential adversary.
- Here are some common categories of adversary in the literature:
  - Casual prying by nontechnical users
    - Bored people…
  - Snooping by insiders
    - Bored people with access to your system…
  - Determined attempts to make money
    - Criminals, organised crime
  - Commercial or military espionage
    - 'Advanced Persistent Threats'
  - Hacktivists?
    - Unpredictable motivation and skill…

20

For reference – but keep in mind that adversary skills differs.

A prominent examples of hacktivists are Anonymous.

Security Services and Mechanisms

- A security threat is a possible means by which your security goals may be breached (e.g. loss of integrity or confidentiality).
- A security **service** is a measure which can be put in place to address a threat (e.g. provision of confidentiality).
- A security **mechanism** is a means to provide a service (e.g. encryption, digital signature).

21

Very important slide! This is the basic concept you must know.

Data Confidentiality and Integrity

- Protection against unauthorised disclosure of information.
- Integrity is protection against unauthorised modification of data

- Think back: What is 'protection' in each case?
  - Prevent, Detect, Recover?

22

Previously we only mentioned CIA as a basic model, however, several additional services can be identified.

Study slides 22-29 – you must be comfortable with the basic terminology.

Lets say we do a transaction online – should be protect the name and payment details of the customer? Yes.
What about the network address of the seller and buyer? Maybe.

What is information? Is it only data?

Is traffic flow confidentiality important? Lets say you encrypt the data but people can see when we sent it?
Decide what do you wish to protect and keep confidential.

Even if we make the 'data' confidential - we make the application layer payload confidential - that means the packet on the wire still has transport layer data (ports, sequences), network layer (destination address) and data link layer information.

Example, are encrypting routers in SWIFT networks (for secure financial messaging) – complete traffic confidentiality (cannot see destination) decrypt – look at network routing information, encrypt, send on.

What is data integrity? What is my goal here – I do not want data to change….

Does this sound more like prevention or detection?
Does it only look for malicious modification?
What is modification – does it mean that an attacker takes data and replaces it with other data?
Corruption, deletion, addition? All these count.

Confidentiality we wish to prevent (detect helps, but not good enough, we cannot recover really).

Integrity we cannot prevent, we need to detect, ideally recover.

Authentication

- **Entity authentication** provides checking of a claimed identity at a point in time.
  - Typically used at start of a connection.
  - Addresses masquerade and replay threats.
- **Origin authentication** provides verification of source of data.
  - Does not protect against replay or delay.
  - More examples later in the course…

23

What do you think the difference is?

You find a document online – it says I am the author. There is a digest on the document only I could have made.

I send you an email, you want to make sure it is really me. You ask me a question only I know the answer to.

Would it be good enough if I sent you a file I wrote earlier?

What is the difference?

Think about if you wish to pay for something. The merchant gives you a receipt, you sign it and he compares the signature to that on your card. You are authenticated (he has given you this paper and you signed it in a way only you can) – the merchant is sure you are owner of the card. (entity who paid is valid).

The merchant wants to get paid so he takes the receipt to the bank. This cannot prove to the bank that the person presenting the receipt is you but it does prove that the payment instruction was made by you (origin of the paper is valid)

Access Control

- Provides protection against unauthorised use of resource, including:
  - use of a communications resource,
  - reading, writing or deletion of an information resource,
  - execution of a processing resource.

24

subject action resource -- IS this person allowed to perform this action on this resource.

Non-repudiation

- Protects against a sender of data denying that data was sent (**non-repudiation of origin**).
- Protects against a receiver of data denying that data was received (**non-repudiation of delivery**).
- Example: analogous to signing a letter and sending via recorded delivery.

25

Most people talk about origin – and this is more common than you think.

Has anyone here done some form of non-repuduation of origin?

If you enter your PIN or sign when buying something is that seen as non-repudiation? You cannot go back and say – oh, I did not make that payment.

Delivery is the other way around – confirmation that the message was received. This might have some legal implications – many places contract law works differently – it might only come into effect if the contract was received.

Why is this important in e-commerce?

If we enter into a contract, we have a piece of paper, we get together and we sign the paper together.

What happens if you buy something online? You and the seller enter into a legal contract to exchange services (goods for money). What if one of you claim you did not enter into this agreement?

Think back to Threats…

- Examples of Services (threats)
  - Confidentiality (data disclosure)
  - Integrity (data alteration)
  - Availability (DoS)
  - Entity Authentication (masquerade)
  - Origin Authentication (forgery)
  - Non-repudiation (repudation – it did not happen!)
  - Access Control (illegitimate access)

Every service has associated mechanisms and threats.

In the context of this model, a *security threat* is something that poses a danger to a system's security. A *security service* is selected to meet an identified threat, and a *security mechanism* is the means by which a service is provided.

It is important to note the distinction between a security service, i.e. what is provided for a system, and a security mechanism, i.e. the means by which a service is provided. Hence *confidentiality* is a service, whereas *encryption* is a mechanism which can be used to provide confidentiality. In fact encryption can be used to provide other services, and data confidentiality can also be provided by means other than encryption (e.g. by physical protection of data).

Mechanisms

- A *security mechanism* is a means to provide a service .
- Can be divided into two classes:
  - *Specific security mechanisms*, used to provide specific security services, e.g. digital signature
  - *Pervasive security mechanisms*, not specific to particular services, e.g. event detection, labelling.

Security mechanisms exist to provide and support security services.

Divides mechanisms into two types:
- *Specific security mechanisms*, i.e. those specific to providing certain security services, and
- *Pervasive security mechanisms*, i.e. those not specific to the provision of individual security services.

An example of a specific mechanism is a digital signature scheme. It can be used to provide several different services – it can obviously be used to give a data integrity service, but it can also be used to provide an origin or entity authentication service even when data integrity is not required. Similarly there are other ways to provide a data integrity service which don't require digital signatures (e.g. MACs or routing controls).

An example of a pervasive mechanism is an event detection mechanism. It doesn't actively provide any security service. (You can't say that this data is transmitted confidentially because of the event detection mechanism.) However, it supports every security service by providing a way to detect compromises which may render specific security mechanism ineffective.

Mechanisms

- Examples of Services/Mechanisms
  - Confidentiality (encryption)
  - Integrity (MAC/digital signature)
  - Availability (redundancy)
  - Entity Authentication (authentication protocol)
  - Origin Authentication(MAC/digital signature)
  - Non-repudation (digital signature)
  - Access Control (Access control model)

28

These are things we will learn about in this course (not all of them, but most of them).

Algorithms

- Algorithms are used to build mechanisms
- Example of mechanisms/algorithms:
  - Encryption: DES/3DES/AES (modes) or RSA/ECC
    - CAST(Canada), MISTY1/Camellia (Japan), SEED (Korea)
  - MAC: CBC mode, HMAC
  - Digital Signature: RSA, DSA, ECC
  - Hash: SHA-3
  - Random number: True or Pseudorandom

29

You should be able to at least give me an example algorithm for each mechanism…especially since we discuss some of them later.

CAST is Canadian, Misty1 is Japanese.
Camellia is Japanese (Mitsubishi and Nippon), SEED is Korean

True random – based on observable random phenomenon.
Pseudorandom – appears random but deterministic (seed and key based on mathematical model, same seed for results same number sequence)

Where to we find security countermeasures?

Standards

30

From next week if I say lets discuss AES or RSA – why do you think we choose to discuss these? Who made these? Why are they used?

It is generally not a good idea to try and make your own algorithms…

What is a standard?

A “document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidance or characteristics of activities and their results, aimed at the achievement of the optimum degree of order in a given context.”

ISO/IEC Guide 2: 1996

You do not need to know this definition – for reference.

There are several important elements to this definition:

A standard is a document – a written document (not lecture, video, audio file). Not open to interpretation (speech tends to be influenced by the speaker), the content is clear and unambigious.

• Standards are developed by consensus. All the members of the developing body should agree that a standard meets its stated objectives before the standard is released. In practice this might lead to some arguments behind the scenes – as everyone is keen on their view.

• Standards should be approved by a recognised body. This body looks after the quality of the standard – acts as a guarantee as to the process followed, and in a way the due diligence put into its formulation. A bunch of people cannot get together and then bring out a standard – OK maybe they can write one, but there is no assurance as to the quality, and at any time these people can simply go ‘Sorry, we made some mistakes’.

While a standard body is often related to a country, it need not be a government agency. Indeed, many of the standards bodies that we will examine are not government agencies, although most have some formal agreement with their host country’s government. In particular, the publication of a standard *does not* imply any legal obligation. Legal obligation can only be delivered by a law or regulation that mandates compliance to a standard, a contractual requirement, or if compliance is claimed in the trade description of a product, process or service.

• Standards are given for tasks that are common and repeated. It is designed for a process that is going to happen over and over, and can be seen as best practice guidelines useful to many entities. In other words, a task that is only ever performed once will not be standardised. While you can have a standard for implementing networks in a commercial building, you cannot have a standard for implementing a network in the Computer Science department of CityU. Such a ‘standard’ would only be useful once.

• Standards should provide rules, guidance or characteristics of activities and their results. A standard is vastly

different from a textbook. It does not provide discussion on the theoretical basis of a subject, and it does not tell you when it is applicable or why it should be used. I standard might define the requirements of data integrity – but not why it is important or when it should be used. It is your job to recognise when a standard will be useful.

A standard simply consists of a sequence of user requirements and ways in which those requirements can be met – in other words, how to do things, not why. It is up to you to select the right standard.

• Standards should aim to achieve the optimum degree of order, in other words they should be the best advice that can be given in any situation. They should only allow the user to make sensible choices and not overwhelm them with different options.

•Furthermore, they should be made in an unbiased way, without regard to commercial or national pressures. Standard should be a neutral opinion of a number of experts on what is best practice. This does not mean the standard contains only one option or opinion, there might be many as there might be different situations where certain approaches work better – and where it is not productive to enforce a single idea. It will be left up to you to choose the one that best apply to you.

So everyone happy?
A document, argued out by experts, approved by someone, is unbiased and tells you how to do something.

Why standards?

"Standards are essential to trade in increasingly competitive markets. They ensure any business offering products, services or processes is:

- cost-effective and time efficient
- commercially viable
- credible
- safe."

You must read slide 32 and 33 and be able to provide a short discussion on the advantage and disadvantages of using standard in security (or anything for that matter).
This quote is taken from the British Standards Institute (BSI) website.

We could argue that it is reasonable that an information security standard could generally provide all four these advantages:

Explain how each one of these advantages apply to the information security sector:

Cost effective and time efficient – using standard cheaper than deal with a breach? no does not make breach cheaper.
Convinces a board?/management Yes, sounds good for making a case but this does not ensure it is cost effective.

You do not have to develop the solution yourself – take time, take experts and this comes up with an ad-hoc solution that is likely to be as good. A straight forward standard – bringing together a bunch of experts (where no contentious issues arise), can take up to 3 years. For a single company to come up with a solution to come up with a solution of similar quality takes longer? That is a lot of investment.
Using the standard divides this cost amongst everyone using the standard.

Commercially viable – customer feels more confident in your solution. The products appears more credible to the customer because our company is using best practice. Could open up a new market

Credible – ties into above.

Safe – Because you are taking best practice into account, and using a solution developed by experts the chances are our solution is safer?

IS THERE ANYTHING MISSING HERE?

In other words, are there any specific advantages to using information security standards?

Interoperability! Could tie into commercial viability – standards allow different entities to produce components that work together (without these entities having a relationship).

How to use standards?

- Three common ways to use a standard.
- Certification is when a neutral third-party attests to a claim of compliance.
- Compliance may be declared without recourse to third-party certification.
- Use as the basis for new design (use the parts you need)
- Most security standards do not really “require” certification.

Know the three uses of a standard.

So standard are wonderful – what do we do with them

1) We can read it, try and understand what the experts meant and then go off and do your own thing. Simply use the standard as starting point for a solution

2) Compliance: You take the standard, and implement the solution exactly as described therein. At the end you have implemented the standard exactly as stated to the best of your ability and you are thus complying with the standard.

3) Certification: You implement the standard to the best of your ability. You then get a neutral third party in to check what you have done and that you have done it as in the standard. This third party, who is generally trusted in this area, then attests to the fact that you have implemented that standard correctly.

Which of these are the best? Depend on your goal! Security decisions are driven by business decisions – if you find a weakness you do not just fix it. You fix it if the business benefit outweighs the cost of fixing it.

Certification might be best – but it costs money and takes time. It has to be worth it

in your business case – you have some business benefits (especially credibility) but this must be compared to the cost.

Bespoke solutions might be a bit risky, and lots of people do not like this idea of using a standard as a starting point – why go only a bit of the way? You might not want to implement everything, you might be a small company and the standard might have had a much larger enterprise in mind. Implementing the standard as a whole might be wasteful in that you implement aspects you do not need.

Some standards are meant to be starting points –

Technical standard 7498-2 OSI (Open Systems Interconnection) security architecture and it explicitly states do not implement this, use it as ideas.

Any product, service or process may claim to be compliant to a standard. As we have already stated, there are no legal ramifications for claiming compliance unless (a) compliance is mandatory under some act of law, (b) compliance constitutes some part of a contractual proceeding, or (c) compliance is used as part of a trade description. It is easy to see, therefore, that certification is not always needed.

Most security standards do not require certification.

Most of the security standards fall into one of two broad categories: they are either standards which define definite algorithms (in which compliance can be easily checked and certification is somewhat of an expensive luxury) or they provide guidance on how to produce a system or service (in which case they are advice and certification is not really intended).

Why not standards?

- The use of standards does have problems:
  - Consensus decisions imply compromise.
  - Documents can be inconsistently implemented.
  - Commercial pressure can lead to partial implementation.
  - Aggressive market strategies by companies who adapt or extend standards can undermine their usefulness.

So we have looked at what standards are, how wonderful they are and how they can be used. Lets consider some disadvantages.

There are several inherent problems with the standardisation process:

• Standards have to be agreed by a consensus of the members of the standards body. If a number of people get together they argue.

Since various members may have different points of view, especially when it comes to a standard with a very broad scope, this may mean that the only way to achieve consensus is to agree that the standard support a range of options and services – it ends up this way because to satisfy people and make them agree the standard might need to reflect some of their opinion.

So the standard might have some compromises or extra material. This makes full implementation of the standard costly and difficult. It is generally agreed that this is one reason why the OSI model “lost” to the TCP/IP model.

• Earlier we made a big deal about a standard being a written down, which is meant to be unambiguous. In practice, a standard is a document that is written by particular people and then read and interpreted by users. It is easy for typos and ambiguous phraseology to creep into any large document, especially if the users and/or the writers are attempting to interpret the document in a foreign language.

• Both commercial pressure and the range of options typically available in large standards means that companies often do not implement the full standard, but instead implement a subset of the functionalities contained. By doing this, they can still claim compliance while often being incompatible with other compliant products. This happens if different companies implement different options in the standard – meaning they are complying but their systems are very different.

• Lastly, it is possible for companies with large market shares to replace independent standards with their own proprietary versions. A typical method of doing this is to release a widely distributed product that adapts or extends a standard. A company will feel that they can improve on a standard, it will incorporate this standard into their product but add additional proprietary aspects. In this manner, the company can claim to be compliant while causing users to rely on functionality which is in fact proprietary. If this product is widely used it undermines the original standard.

• Are there any additional reasons why information security standard can be bad?

If you have a standard it is a nice target for attacks – if I can find a weakness then it inherently effects a lot of systems.

If a standard is broken it can take years to correct. One there is the standardisation process, but there is also the effect of having a lot of deployed systems. Think DES, when it started becoming apparent that the key length was not really good enough anymore – all these industries (especially banking) can not just change overnight. Once a standard is out there and widely used it is complicated to change.

International standards

- Main international standards bodies relevant to Information Security are:
  - International Organization for Standardization (ISO),
  - International Electrotechnical Commission (IEC),
  - International Telecommunications Union (ITU).

For slides 35-38, you do not need to know specific examples.

You need to know there are official standards bodies (defining standards at worldwide or national level), there are companies who make standards (often with commercial interest – some good some bad, and some you have to use like payment card standards) and there are Internet standards (which no on really looks after, simply technology that grows in usage, and once everyone uses it might be organised and published as a standard by IETS

Note that the information on these slide are not examinable in that you will not be expected to be able to list, for example, the European standards bodies. However, we will be discussing some general issues of standardization (especially for the Internet and commercial standard) that you need to know.

International standards

The main function of these bodies is the production of 'base standards'.

ISO produces standards on basically everything and started in 19th century– screw threads, photography, etc. In information security there is a collaboration between ISO and IEC bodies, who have formed a Joint Technical Committee (JTC1). Most of the

prominent security standards are ISO/IEC.

Any ISO standards can be purchased from local/national standard body(e.g. **Standardization** Administration of the People's Republic of **China** (SAC), or in Hong Kong you can buy from ITC)

Third body is ITU (usually ITU-T) – also quite old and established – formed to work on things like telegraph technology, now onto networks and telephones. anyone knows the main security standard?

In information security they are most known for X.509 which details PKI.

North American standards

- Some US standards bodes have assumed international importance:
  - IEEE (a professional engineering body),
  - NIST (a US federal standards body),
  - ANSI (the US member body of ISO).

North American standards bodies have become particularly important in security. The IEEE and NIST produce IT security standards of international importance.

IEEE (Institute of Electrical and Electronics Engineers) – my professional body.

What is a quite prominent IEEE standard? IEEE 802.11! Wireless networks.
IEEE work includes LAN security (IEEE 802.10), POSIX, and the IEEE 1363 public key cryptography standards.

NIST (the National Institute for Standards and Technology) (the successor to NBS national burea of standards) produces standards for use by Federal Government bodies. What is NIST main standards?
AES? SHA? DSA?
Very good in algorithms.

Also of global significance is the work of ANSI (the American National Standards Institute), interfaces with ISO. Particularly knows for its work on banking security standards (especially X9 standards) and biometrics.

Note that the information on this slide is not examinable.

Internet standards

- The Internet is a loose collaboration between government, industry and academia.
- Internet standards are produced by the *Internet Engineering Task Force (IETF)*.
- Are there problems uniquely associated with Internet Standards?

Remember that no one really controls the Internet…

The operation of the Internet relies on interconnection standards, primarily those designed specifically for Internet operation. The Internet is managed by the *Internet Architecture Board (IAB)*; however, the development and review of Internet standards is the responsibility of the *Internet Engineering Task Force (IETF)*.

The IETF is sort of loose organisation and in a way there are many standards and on the other hand there are not many standards. There are about 6000+ RFC(request for comments) and anyone can produce one – advice, algorithms and protocols – and these are widely used such as SNMP. Small number of RFCs eventually become IS (Internet Standards) – example of this is how to run a DNS server.

There is no reason to not use an RFC – it tends to get refined and then if enough people start using it (especially large companies microsoft/cisco) it become a defacto standard (this is not an official standard but everyone is using it).

Keep in mind that the IETF has no real authority to tell anyone what to use - there is no real authority because the Internet is not a controlled entity.

Internet Standards are quite odd things. Why is it hard to produce reliable Internet standards?

Strangely - products tend to be interoperable – large companies works together, almost like a standards body – your product needs to work with theirs. Defacto standard –> interoperability.

Big problem – once a standard is being used it is used by everyone. Once again if there is a standard and something goes wrong with it is difficult to correct.

We spoke about this earlier, and mentioned banking standards, but in this case it is worse because there is no central entity with the authority to make people to change. Who is going to tell millions of people to update their web browser? This has a follow on effect that companies need to keep their new products backward compatible (because there users are not keeping up), in turn this further encourages users not to update. This means you could have weak solutions hanging around for years, because it is just to impractical and hard to completely get rid of.

Company standards

- Companies themselves also sometimes issue *de facto* standards for techniques that have been patented. These include:
  - PKCS (Public-Key Cryptography Standards, published by RSA Labs.)
  - SECG (Standards for Efficient Cryptography Group, a large group including Certicom, VeriSign and NIST).
  - PCI (Payment Card Industry) Data Security Standards

Companies something produces standards either on their own or as member of a consortium. These groups can often be quite fluid in terms of membership and activity but, nevertheless, have made important contributions to information security.

Company standards are usually motivated by the need for public confidence in a particular algorithm or system that might not be getting much attention in other standards. For example, PKCS is promoted by RSA because they really wanted people to use public key cryptography. It was tied to their business case (founded basically on the RSA algorithm) . However, ISOs attempt to bring out some standards in this area back in the 80s was not very successful, so RSA took it on themselves to come up with standards (and did quite a decent job of it).

SECG is mainly concerned with elliptic curve cryptography and has only published two standards, whereas PKCS appears to be more active and covers all the basic public-key encryption systems. SECG seemed to have been dormant for several years, but there are signs that it is preparing to start work on new standardisation activities, perhaps motivated by recent advances in elliptic curve cryptography.

Finally, PCI (Payment Card Industry) standards. There is an entity called the PCI SCC (Security Standards Council), who sets a number of standards on the security of payment systems (essentially card payments). Visa/Mastercard, AMEX, Discover and JCB all had their own best practice programs – decided to put these together.

Cornerstone is the PCI DSS Data Security Standard for organisations accepting/processing payments (for example, deals with handling payment card information), but also have documents on PTS (PIN Transaction Security) for device vendors/manufacturers (essentially guidelines for PED security). Also the PA-DSS Payment Application DSS for software vendors (applications running on cards or on POS, etc).
You want to accept Unionpay, Mastercard, Visa, Amex? You need to be PCI compliant!

Any reasons these would not be seen as standards?

As per previous definition:

Standard body?

Consensus?

Are the completely unbiased?

In some cases the standards might be good – put together like any accepted standard. Although there is always a feeling that the user needs to check the process, participants – whereas there is a little more credibility when standard bodies involved because we assume someone like ISO checked the quality of document and process.

There is a question as to whether these documents can truly be considered standards. It is certainly true that they provide, for common and repeated use, rules, guidelines or characteristics for activities or their results. However, they are not established by consensus, nor are they aimed at the achievement of the optimum degree of order in a given context.

Their sole aim is to increase profit for the business, although they may achieve this by giving important advice (for example, as a PR exercise, to promote interoperability, or simply by increasing the market's knowledge of the importance of a subject). Nevertheless they cannot really be considered impartial and should be treated with appropriate care.

You have to be careful – does the fact that someone makes money out of a standard make it a company standard? No, some bodies charge for standards but do not gain from standard being implemented (e.g. by selling products).

The end!

Any questions…