



Information Security Group

**IY5601**

**A. Introduction to application security design**

Chris Mitchell

<http://www.isg.rhul.ac.uk/~cjm>

[c.mitchell@rhul.ac.uk](mailto:c.mitchell@rhul.ac.uk)

1

All corrections and suggestions for improvement to this course material are gratefully received – please send any comments to:

[c.mitchell@rhul.ac.uk](mailto:c.mitchell@rhul.ac.uk)

Please feel free to re-use all or part of this presentation; however, if you do, it would be much appreciated if an acknowledgement of Royal Holloway as the source of this material could be given. I would also value learning about your experiences with this material.



Information Security Group

## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources

2

This lecture is divided into the following eight main parts:

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources

In this preliminary part the structure and scope of the course are briefly reviewed, as are the methods of delivery and examination.



Information Security Group

## Course website

- All lecture material will be made available via the course website:  
<http://www.isg.rhul.ac.uk/~cjm/IY5601>
- This site will be updated during the course, and also (if necessary) in the run up to the examination.


3

All lecture material will be made available via the course website:

<http://www.isg.rhul.ac.uk/~cjm/IY5601>

This site will be updated during the course, and also (if necessary) in the run up to the examination.

If any problems are encountered accessing (or printing) this material, please contact the author at: [c.mitchell@rhul.ac.uk](mailto:c.mitchell@rhul.ac.uk)



Information Security Group

## Focus of course

- This course is primarily technical in its focus.
- That is, it looks at the technology necessary to develop individual secure applications, rather than considering the security of an entire enterprise (which is a much larger subject).

4

This course is primarily technical in its focus. That is, it looks at the technology necessary to develop individual secure applications, rather than considering the security of an entire enterprise (which is a much larger subject).



Information Security Group

## Structure of course

- The course is divided into four main parts:
  - A. Introduction to application security (1 week)
  - B. Payment and e-commerce applications (3 weeks)
  - C. Web applications (3 weeks)
  - D. Identity management (3 weeks)
- This, of course, leaves one week for over-runs, extra material, and concluding material.

5

The course is divided into four main parts:

- A. Introduction to application security (1 week)
- B. Payment and e-commerce applications (3 weeks)
- C. Web applications (3 weeks)
- D. Identity management (3 weeks)

This, of course, leaves one week for over-runs, extra material, and concluding material.



Information Security Group

## Delivery of course

- The course will be delivered as a series of eleven 3-hour lectures, mostly given by CJM.
- However, the lectures on topic C (Web applications) will be given by Allan Tomlinson (2 weeks) and John MacDonald (1 week).
- All lectures will be in MLT between 14:00 and 17:00 on Mondays (between 16/1/06 and 27/3/06, inclusive).

6

The course will be delivered as a series of eleven 3-hour lectures, mostly given by CJM. However, the lectures on topic C (Web applications) will be given by Allan Tomlinson (2 weeks) and John MacDonald (1 week).

All lectures will be in MLT between 14:00 and 17:00 on Mondays (between 16/1/06 and 27/3/06, inclusive).

Whilst the course notes are intended to be self-contained, every student is strongly encouraged to read around the subject. References to relevant books, standards and papers are made throughout these notes. Further details of all background resources mentioned are given at the end of these course notes.



## Examinations

- The examination will be of two hours duration, and will contain a total of five questions.
- Candidates will be permitted to answer at most three questions.
- Full marks will be obtained if a candidate answers three questions completely correctly.
- The breakdown of marks for each part of a question will be given on the examination paper.
- The provisional examination date is 22nd May 2006.

7

The examination will be of two hours duration, and will contain a total of five questions. Candidates will be permitted to answer at most three questions. Full marks will be obtained if a candidate answers three questions completely correctly. The breakdown of marks for each part of a question will be given on the examination paper.

The provisional examination date is 22nd May 2006.



## Coursework

- During the course, coursework sheets will be handed out (and also made available via the course web page).
- Students are expected to complete these pieces of coursework, and feedback will be provided.
- However, the coursework marks will not count towards the final course mark.


During the course, coursework sheets will be handed out (and also made available via the course web page). Students are expected to complete these pieces of coursework, and feedback will be provided. However, the coursework marks will not count towards the final course mark.



## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources

By starting the main part of this lecture with a discussion of security policy, there is an implication that everything starts from a security policy statement. Of course, at some high level everything stems from a business need, which gives rise to policy (either implicitly or explicitly). However, more detailed system-specific policies can only be completed when the form of the system is known, and almost all of the steps in the development lifecycle (see later) involve feedback to previous steps. Specifically, the relationship between policy expression and threat analysis is iterative.



Information Security Group

## What is a system?

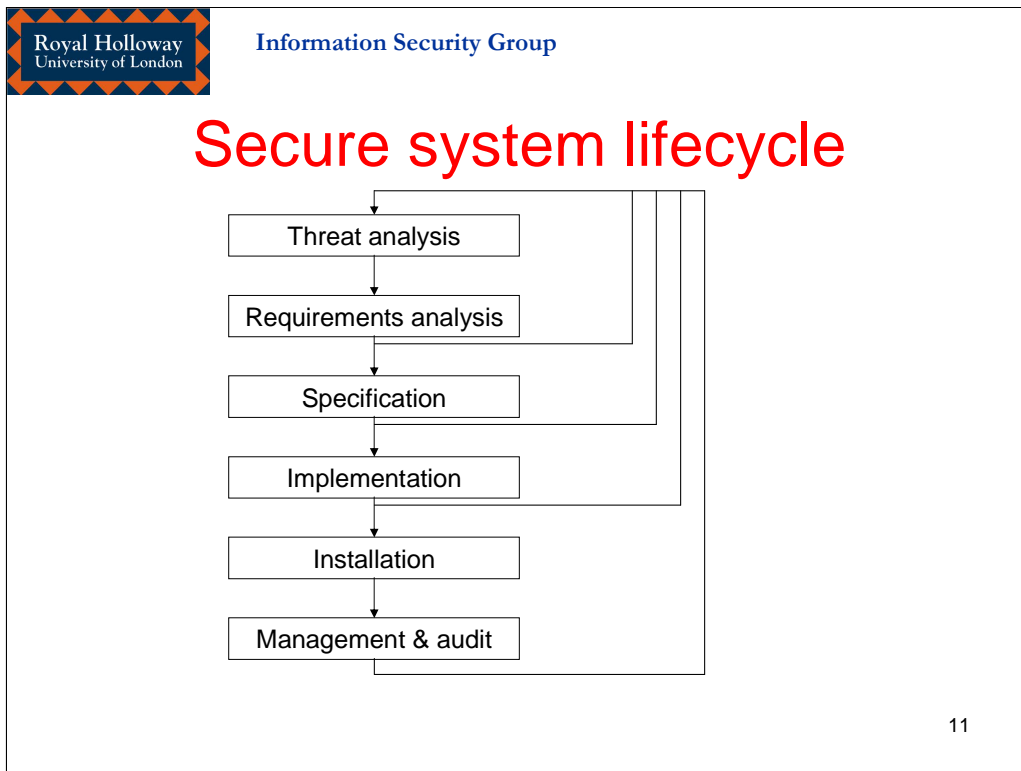
- This course is concerned with application systems.
- A system might be:
  - something designed to provide a business service (e.g. a system to support e-commerce), or
  - providing a security infrastructure for other systems (e.g. a PKI or a single sign-on system).
- Although network security protocols might be a necessary part of a system, this course is not primarily concerned with specific protocols.

10

This course is concerned with application systems. A system might be:

- something designed to provide a business service (e.g. a system to support e-commerce), or
- providing a security infrastructure for other systems (e.g. a PKI or a single sign-on system).

Although network security protocols might be a necessary part of a system, this course is not primarily concerned with specific protocols.



The main parts of the lifecycle of a secure system are as follows:


1. Threat analysis (which, for our purposes, includes the risk analysis step)
2. Security requirements analysis
3. System specification
4. System implementation
5. System installation
6. Ongoing management and audit

Whilst it is nice to think about these occurring in a neat and logical order, in practice almost every stage in the process affects previous stages. For example, when specifying safeguards to address identified security requirements, it is necessary to include these in a revised threat analysis, since the safeguards themselves may be subject to new threats. Moreover, ongoing use of the system may identify vulnerabilities which were missed in the original analysis, causing the need for a reassessment of the system and possible modifications to the implementation.

It could be argued that, as a result, threat/risk analysis should occur later in the cycle, since all the security measures need to be subjected to a threat analysis. However, it is surely right that some measure of threat/risk analysis occurs before developing the security requirements. Alternatively, one could ask for multiple threat analysis steps, occurring at various stages in the cycle – we instead opt here for the idea of multiple feedbacks to the threat analysis stage from other stages in the cycle.

Much more detail on system development lifecycles (SDLCs) and security system development lifecycles (SecSDLCs) is given (for instance) in:

- Whitman and Mattord's *Principles of Information Security* (chapter 1), and
- Swiderski and Snyder's *Threat Modeling* (chapter 1).



Information Security Group

## Scoping a system

- Before anything else, the scope of the system must be defined, i.e. a statement should be produced covering issues such as:
  - what the purpose of the system is,
  - the main entities that will use the system,
  - what data it should process,
  - what information will be transmitted between entities, and
  - what the main *assets* of the system are.

12

Before anything else, the scope of the system must be defined, i.e. a statement should be produced covering issues such as:

- what the purpose of the system is,
- the main entities that will use the system,
- what data it should process,
- what information will be transmitted between entities, and
- what the main *assets* of the system are.

Most important are the system assets – this is something we discuss again a little later.




## Defining the policy rules

- A *security policy* is a set of rules defining how assets are to be managed and protected.
- Policies can exist at many levels of detail – high-level policies will give general rules for handling sensitive data and resources; more detailed system-specific policies will describe rules for protection of system assets.
- A system security policy should provide overall guidance for the design process for a secure system.

13

A security policy is a set of rules defining how assets are to be managed and protected. Policies can exist at many levels of detail – high-level policies will give general rules for handling sensitive data and resources; more detailed system-specific policies will describe rules for protection of system assets. A system security policy should provide overall guidance for the design process for a secure system.

Discussions of security policies can be found in Whitman and Mattord, *Principles of Information Security* (chapter 6), and in clause 4 of ISO/IEC 13335-1: 2004.



Information Security Group

## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources

14

A much more detailed treatment of the topics considered here under ‘threat and vulnerability analyses’ can be found in ISO/IEC 13335-1: 2004 (*Management of information and communications technology security – Part 1: Concepts and models*).



## Assets

- *Assets* are the elements of a system that one might wish to protect.
- Assets typically include: data, hardware, software, procedures, and people.
- As part of the scoping of any secure system design, the assets must be identified and listed.

15

Assets are the elements of a system that one might wish to protect. Assets typically include: data, hardware, software, procedures, and people. As part of the scoping of any secure system design, the assets must be identified and listed.

In fact, asset identification is a fundamental part of risk analysis (see later).



Information Security Group

## Threats

- A *threat* is something that poses a danger to an asset's confidentiality, integrity or availability.
- Possible threats include:
  - Masquerade;
  - System penetration;
  - Authorisation violation;
  - Planting (e.g. Trojan horses, viruses, ...);
  - Communications monitoring (eavesdropping);
  - Modification of communicated data (passive attack);
  - Network spoofing (active attack);
  - Denial of Service (DoS);
  - Repudiation.

16

As defined in Ford and Baum's *Secure Electronic Commerce*:

A *threat* is a person, thing, event or idea which poses some danger to an asset in terms of that asset's confidentiality, integrity, availability or legitimate use. Threats may result from deliberate actions, such as hacker penetration, or accidental actions, such as a message sent in error to the wrong address.

There are many potential threats to systems, including the following (again see Ford and Baum's *Secure Electronic Commerce*):

- *Masquerade*, where an intruder pretends to be a legitimate user;
- *System penetration*, where an unauthorised person gains access to a system and modifies stored data, steals confidential data, or uses resources.
- *Authorisation violation*, where a person authorised to use a system for one purpose uses it for another, unauthorised purpose.
- *Planting*, where an intruder modifies a system by inserting a capability to perpetrate future attacks (e.g. a Trojan horse or a virus);
- *Communications monitoring*, where an intruder learns confidential information by (passively) reading data sent between system participants;
- *Modification of communicated data*, where an intruder (actively) modifies data sent between authorised system participants;
- *Network spoofing*, a type of masquerade in which one network system pretends to be another – includes server spoofing and DNS spoofing (where an intruder interferes with the operation of the Domain Name Server (DNS) system, part of the Internet routing infrastructure);
- *Denial of Service (DoS)*, where the availability of the system is threatened, e.g. by flooding a network entity with packets. A Distributed DoS (DoS) attack is where multiple sources flood a target.
- *Repudiation*, where a communicating party later denies having taken an action (e.g. making a purchase or signing a document).

Of course, the above list has obvious overlaps.

For a detailed discussion of threats and threat modelling (which, unfortunately, uses different terminology) see Swiderski and Snyder's *Threat Modeling*. Note also that there is a free software threat modelling tool that complements the book.



## Attacks

- An *attack* describes an implementation of a threat originating from deliberate actions.
- All the example threats given on the previous slide would, if implemented, be examples of attacks.
- However not all threats give rise to attacks (e.g. accidental loss of integrity or availability, e.g. due to storage errors, fire, accidental destruction, ...).

17

An attack is a term used to indicate a particular instance of a threat originating from deliberate actions. All the example threats given on the previous slide, if implemented, would give rise to attacks. However not all threats give rise to attacks (e.g. accidental loss of integrity or availability, e.g. due to storage errors, fire, accidental destruction, ...).

As defined in Ford and Baum's *Secure Electronic Commerce*:

An *attack* is an actual realisation of a threat. A passive attack involves unauthorised monitoring, but not alteration of data. An active attack involves deliberate alteration of information.



Information Security Group

## Safeguards

- *Safeguards* are mechanisms, procedures, ... used to protect assets against threats.
- In communications/computer security context, we have:
  - Authentication, including entity authentication and data origin authentication;
  - Access control;
  - Confidentiality;
  - Data integrity;
  - Non-repudiation.

18


As defined in Ford and Baum's *Secure Electronic Commerce*:

*Safeguards* are controls, mechanisms, policies and procedures that protect assets against threats.

In communications security and computer security contexts, safeguards are often referred to as *security services*. There are five main classes of security service:

- Authentication, including entity authentication and data origin authentication;
- Access control;
- Confidentiality;
- Data integrity;
- Non-repudiation.

This security service terminology originates in ISO 7498-2, dating back to the late 1980s.



Information Security Group

## Vulnerabilities

- *Vulnerabilities* are weaknesses in, or the absence of, safeguards, that can be exploited by one or more threats.
- Vulnerabilities include weaknesses in the system itself, its operation, and in the safeguards designed to protect a system.

19

As defined in Ford and Baum's *Secure Electronic Commerce*:

*Vulnerabilities* are weaknesses in, or the absence of, safeguards.

ISO/IEC 13335-1 defines vulnerability as:

A weakness of an asset or group of assets that can be exploited by one or more threats.

ISO/IEC 13335-1 goes on to say that:

Vulnerabilities associated with assets include weaknesses in physical layout, organisation, procedures, personnel, management, administration, hardware, software or information. A vulnerability in itself does not cause harm; a vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset.



Information Security Group

## Impact

- *Impact* refers to the degree of damage which could be caused by a threat.
- In some sense it therefore measures the seriousness of a threat.
- Measuring impact enables a balance to be made between the cost of safeguards and the cost of a realised threat.

20

Impact refers to the degree of damage which could be caused by a threat. In some sense it therefore measures the seriousness of a threat.

As described in ISO/IEC 13335-1:

Impact is the result of an information security incident, caused by a threat, which affects assets. The impact could be the destruction of certain assets, damage to the ICT system, and compromise of confidentiality, integrity, availability, non-repudiation, accountability, authenticity or reliability. Possible indirect impact includes financial losses, and the loss of market share or company image. The measurement of impact permits a balance to be made between the anticipated results of an incident and the cost of the safeguards to protect against the incident. The probability of occurrence of an incident needs to be taken into account.



## Risks

- Risk is an estimation of the seriousness of a threat, taking into account the impact and the probability of realisation.
- Hence high risk equates to high impact and high probability.
- Risk is never eliminated – risk needs to be managed (if the risk is low then spending large sums on safeguards may not be justifiable).

21

As defined in Ford and Baum's *Secure Electronic Commerce*:

*Risk* is an estimate of the cost of a vulnerability, taking into account the probability of a successful attack. Risk is highest when the value of a vulnerable asset is high and the probability of a successful attack is high. Conversely, risk is lowest when the value of the vulnerable asset is low and the probability of a successful attack is low.

As given in ISO/IEC 13335-1: 2004:

Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. Single or multiple threats may exploit single or multiple vulnerabilities.

Risk is never eliminated – instead risk needs to be managed (if the risk is low then spending large sums on safeguards may not be justifiable).



## Risk analysis and management

- This is a topic worthy of a course in itself!
- *Risk analysis* involves identifying risks and assessing them.
- *Risk management* is the totality of measures put in place to reduce/manage risks.

22

As defined in Ford and Baum's *Secure Electronic Commerce*:

*Risk analysis* is a process which gives a quantitative or qualitative assessment of whether expenditure on safeguards is warranted.

ISO/IEC 13335-1: 2004 gives the following definitions:

*Risk analysis*: the systematic process of estimating the magnitude of risks;

*Risk management*: the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect ICT system resources.

In a sense, risk management covers the entire process of secure system implementation and operation.

ISO/IEC 27005 (to appear) is purely concerned with risk management, and the current draft text (the Committee Draft (CD) of January 2006) runs to over 80 pages. Risk management is also the focus of chapters 4 and 5 of Whitman and Mattord's *Principles of Information Security*.



## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources



## Definition of security elements

- Following the threat, vulnerability and risk analyses, the next step is to define what security measures (*safeguards*) need to be put in place.
- This is what we mean by defining the *security requirements*.

Following the threat, vulnerability and risk analyses, the next step is to define what security measures, i.e. what safeguards, need to be put in place. This is what we mean by defining the *security requirements*.



Information Security Group

## Requirements terminology

- Typically requirements for assets (data and resources) will be phrased in terms of:
  - entity and origin authentication (in a communications context);
  - access control;
  - confidentiality;
  - integrity;
  - non-repudiation;
  - availability;
  - ...

25

Typically, security requirements for assets (data and resources) will be phrased in terms of:

- entity and origin authentication (in a communications context);
- access control;
- confidentiality;
- integrity;
- non-repudiation;
- availability;
- etc.

That is, the five security services we identified under the heading of safeguards, together with availability. We might also add accountability.

Note that integrity has two somewhat different meanings depending on the context:

- in a data storage context, integrity means preventing unauthorised change;
- In a data communications context, integrity means detecting unauthorised change.



## Refining the requirements

- The requirements analysis is typically performed as a series of refinements.
- That is, the first step would be to identify at a high-level the security measures, e.g.
  - confidentiality protection for communications link A,
  - access control functions for system B, etc.
- Communications link A may actually consist of series of network links, and hence the requirements for the entire link need to be refined to derive requirements for the constituent parts.
- System B may consist of a collection of subsystems, and requirements for its entirety can be refined to cover individual components.

26

The requirements analysis is typically performed as a series of refinements. That is, the first step would be to identify at a high-level the security measures, e.g.

- confidentiality protection for communications link A,
- access control functions for system B, etc.

Communications link A may actually consist of series of network links, and hence the requirements for the entire link need to be refined to derive requirements for the constituent parts.

System B may consist of a collection of subsystems, and requirements for its entirety can be refined to cover individual components.



## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources



## Specifying the system

- The overall structure of the system to be made secure will typically be determined by its main objectives, rather than by security requirements.
- Indeed, the details of the security requirements will typically derive from the structure of the system.
- Hence specifying security will typically consist of defining how certain components of the overall system operate with respect to security, and also to define specific security-relevant subsystems.

28

The overall structure of the system to be made secure will typically be determined by its main objectives, rather than by security requirements. Indeed, the details of the security requirements will typically derive from the structure of the system. Hence specifying security will typically consist of defining how certain components of the overall system operate with respect to security, and also to define specific security-relevant subsystems, rather than defining the overall architecture.




## Typical components

- Typical components of a secure system include:
  - cryptographic functions in software/hardware;
  - operating system security functions, e.g. access control, process isolation;
  - hardware security modules, including personal modules (e.g. smart cards) and PC resident subsystems;
  - physical security, e.g. secure rooms, tamper-resistant hardware.

29

Typical components of a secure system include:

- cryptographic functions in software/hardware;
- operating system security functions, e.g. access control, process isolation;
- hardware security modules, including personal modules (e.g. smart cards) and PC resident subsystems;
- physical security measures, e.g. secure rooms, tamper-resistant hardware.




Information Security Group

## Implementation

- Once the system has been specified, it will be necessary to implement it.
- This will typically involve procuring the necessary components, possible combined with bespoke implementation.
- This may involve putting out a tender for specific subsystems.

30

Once the system has been specified, it will be necessary to implement it. This will typically involve procuring the necessary components, possible combined with bespoke implementation. This may involve putting out a tender for specific subsystems.



Information Security Group

## Documentation

- A range of documentation must be created to accompany any system.
- This will typically include:
  - System specifications, defining what the system does;
  - System manuals, describing how to configure and operate system components (hardware and software);
  - Procedure definitions, describing how the system should be configured and operated.

31

A range of documentation must be created to accompany any system. This will typically include:

- System specifications, defining what the system does;
- System manuals, describing how to configure and operate system components (hardware and software);
- Procedure definitions, describing how the system should be configured and operated.

Note that it is important to distinguish system manuals from system procedures. Manuals will typically describe how the system can be operated, and will describe all the various features of a system. Such manuals will typically be generic documents, created by the provider of a system (or subsystem). Such manuals will not define in a stepwise manner how the system should be used within a particular organisation, and who should perform all the individual tasks – this is the role of procedures.



## Testing

- Once the system has been implemented, it is necessary to obtain confidence in its correct operation.
- This can be partially achieved through testing.
- Testing requires the design of a set of test cases which must be applied to the system.
- In the case of a subsystem provided by a third party, testing of that subsystem will typically be carried out by the supplier, although a review of the test cases used by the supplier would be advisable.

32

Once the system has been implemented, it is necessary to obtain confidence in its correct operation. This can be partially achieved through testing. Testing requires the design of a set of test cases which must be applied to the system. In the case of a subsystem provided by a third party, testing of that subsystem will typically be carried out by the supplier, although a review of the test cases used by the supplier would be advisable.



## Security evaluation

- Greater levels of confidence in the correctness of a system (or subsystem) can be obtained through a formal security evaluation.
- Licensed evaluation facilities will carry out evaluations in accordance with the Common Criteria (ISO/IEC 15408).
- Such an evaluation is to one of a series of levels defined in the Common Criteria.


33

Greater levels of confidence in the correctness of a system (or subsystem) can be obtained through a formal security evaluation. Licensed evaluation facilities will carry out evaluations in accordance with the Common Criteria (ISO/IEC 15408). In such a case, the evaluation takes place against one of a series of levels defined in the Common Criteria.



## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources



Information Security Group

## Preliminaries


- Each major component of the secure system will typically need to have a set of *Procedures*.
- These procedures will dictate how employees manage the operation of this system.
- The size and complexity of these procedures will vary immensely, depending in the degree to which human interaction is necessary.
- The procedures will need to cover initial configuration, as well as day to day operation.

35

Each major component of the secure system will typically need to have a set of *Procedures*. These procedures will dictate how employees manage the operation of this system.

The size and complexity of these procedures will vary immensely, depending in the degree to which human interaction is necessary. For example, if the component is a Certification Authority incorporating Registration Authority functions, then the procedures are likely to be rather complex, especially if each certification request needs to be manually authorised.

The procedures will need to cover initial configuration, as well as day to day operation.



Information Security Group

## Roles in procedures

- When defining procedures, it is normal to define the participants in terms of roles.
- For example, the procedures may involve roles with names such as:
  - Security manager;
  - Security officer;
  - Operator;
  - Auditor.


36

When defining procedures, it is normal to define the participants in terms of roles. For example, the procedures may involve roles with names such as:

- Security manager;
- Security officer;
- Operator;
- Auditor.

This enables staff to be re-assigned to different tasks in such a way that defining who does what remains unambiguous. Of course, this is consistent with the use of Role Based Access Control (RBAC) systems.

It is interesting to note that clause 5 of ISO/IEC 13335-1 actually defines recommended organisational roles for security personnel. This could be useful input when defining operational roles for a secure system.



Information Security Group

## Contents of procedures

- Codified procedures will typically cover the following subjects:
  - Role definition;
  - Assignment of roles to individuals (ongoing role management);
  - Installation and initial configuration;
  - Operational procedures;
  - Backup and restore, including disaster recovery.

37

Codified procedures will typically cover the following subjects:

- Role definition, that is the definition of a set of roles, where each procedure involves named role-holders;
- Assignment of roles to individuals (and ongoing role management, covering replacement of role holders), where in most cases no individual will be permitted to take on more than one role (helping to guarantee dual control and in line with the notion of separation of duty);
- Installation and initial configuration;
- Operational procedures, i.e. covering all the operations associated with normal day to day operation of the system;
- Backup and restore, including disaster recovery.



## Dual control


- When accessing and configuring security-sensitive systems, it is often required that no single individual has the power/authorisation to perform certain tasks, or have access to plaintext cryptographic keying material.
- This is in line with the notion of *Separation of duty*.

38

When accessing and configuring security-sensitive systems, it is often required that no single individual has the power/authorisation to perform certain tasks, or have access to plaintext cryptographic keying material. This is in line with the notion of *Separation of duty*.

As stated in Whitman and Mattord's *Principles of Information Security*:

Separation of duties is used to reduce the chance of an individual violating information security. The completion of a significant task that involves sensitive information should require two people. If one person has the authorisation to access particular information, then there may be nothing to prevent this individual from copying it and removing it from the premises.

Information Security Group

## Dual control mechanisms

- In the case of stored keys, dual control can involve splitting keys into two or more components.
- In the case of accessing physical systems, enforcing dual control can involve issuing role-holders with tokens, some number of which must be present before a device will complete certain tasks.

39

In the case of stored keys, dual control can involve splitting keys into two or more components. In the case of accessing physical systems, enforcing dual control can involve issuing role-holders with tokens, some number of which must be present before a device will complete certain tasks.

Splitting keys into components can be achieved in a number of ways. The simplest approach to dividing a  $k$ -bit key into  $n$  components is to randomly generate  $n-1$  components, each of  $k$  bits, and then compute the final  $n$ th component as the bit-wise exclusive-or (exor) of the key and the other  $n-1$  components. Because of the property of the exor operator, if the  $n$  components generated in this way are exored together, the result will be the key. However, knowledge of any  $n-1$  components yields no information whatever about the key.

This latter property is a crucial one. Each component must be at least as long as the key being constructed – for example, dividing a  $k$ -bit key into two  $k/2$  bit components and then reassembling the key by concatenating the components is an unacceptably weak approach, since knowledge of one component yields an enormous amount of information about the actual key. This is easy to see since, given knowledge of one component, performing an exhaustive search for the entire key would require only  $2^{k/2}$  operations, instead of  $2^k$ .

More sophisticated ways of dividing a key into  $n$  components so that the key can be reconstructed given any  $r$  of them (and such that knowledge of any  $r-1$  components yields no information about the key) can be devised, using so-called *threshold schemes*, a special class of *secret sharing schemes*.



## Auditing mechanisms

- A secure system will typically incorporate auditing subsystems which make records of security-relevant events.
- These records should be protected against tampering by those operating the system.
- This could be achieved by computing a MAC on records, using a key stored within a physically secure subsystem.

40

A secure system will typically incorporate auditing subsystems which make records of security-relevant events. These records should be protected against tampering by those operating the system. This could be achieved by computing a MAC on records, using a key stored within a physically secure subsystem.



## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources



## Security management

- Any secure system will require continuous management, to ensure that it operates correctly.
- Management will include upgrading the system to take on new functions, and to correct detected vulnerabilities.
- Auditing is one particularly important part of ongoing management.

42

Any secure system will require continuous management, to ensure that it operates correctly. Management will include upgrading the system to take on new functions, and to correct detected vulnerabilities. Auditing is one particularly important part of ongoing management.



Information Security Group

## Categories of management

- Security management can be divided into:
  - Fault management;
  - Configuration and change management;
  - Accounting and audit management;
  - Performance management;
  - Security programme management.

43

The five-layer security management model presented here is based on that given in Whitman and Mattord's *Principles of Information Security*. The five layers have the following scopes:


- *Fault management* – this covers the identification of faults in the application and in the way it is used – this includes penetration testing;
- *Configuration and change management* – this covers the administration of changes to the application;
- *Accounting and audit management* – covering audit (discussed later);
- *Performance management* – monitoring and evaluation of system performance;
- *Security programme management* – operational management of the system, in accordance with the defined procedures.



## Purpose of security auditing

- The main purpose of security auditing is to check that secure procedures have been carried out correctly, and to detect security breaches.
- Auditing procedures can also be used after a security breach to try to detect how it occurred (and who is responsible).

The main purpose of security auditing is to check that secure procedures have been carried out correctly, and to detect security breaches. Auditing procedures can also be used after a security breach to try to detect how it occurred (and who is responsible).




Information Security Group

## Roles and independence

- The auditing process should be carried out by role-holders completely independent of operational role-holders.
- That is, no auditor should also be permitted to act in an operational role.
- This ensures separation of duties.

45

The auditing process should be carried out by role-holders completely independent of operational role-holders. That is, no auditor should also be permitted to act in an operational role. This ensures separation of duty.




Information Security Group

## Procedural aspects

- A set of auditing procedures should be defined as part of the overall procedures.
- Thus auditors who may not be experts in system operation, can perform their functions correctly without relying on advice from the entities who they may be monitoring.

46

A set of auditing procedures should be defined as part of the overall procedures. Thus auditors who may not be experts in system operation, can perform their functions correctly without relying on advice from the entities who they may be monitoring.




Information Security Group

## Structure of lecture

1. Introduction
2. Security policy establishment
3. Threat and vulnerability analyses
4. Security requirements definition
5. System specification and implementation
6. Security procedure definition
7. Ongoing security management and audit
8. Further resources

47

We conclude this introductory lecture by listing a range of supporting resources.



Information Security Group

## Books

- Each part of the course uses material from a range of different books.
- Of particular relevance to this introductory lecture are:
  - W. Ford and M. S. Baum, *Secure Electronic Commerce*. Prentice Hall (2001), 2nd edition.
  - J. Sherwood, A. Clark and D. Lynas, *Enterprise Security Architecture: A Business-Driven Approach*. CMP Books (2005).
  - F. Swiderski and W. Snyder, *Threat modeling*. Microsoft Press (2004).
  - M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Thomson Course Technology (2003).
  - S. E. Pfleeger, *Software Engineering – Theory and Practice*. Prentice Hall (2001).

48

Each part of the course uses material from a range of different books. Of particular relevance to this introductory lecture are the following:

- W. Ford and M. S. Baum, *Secure Electronic Commerce*. Prentice Hall (2001), 2nd edition. [This book provides very helpful definitions of terms such as threats, safeguards, etc. It also contains a lot of other useful background material, including discussions of legal issues and a lot of material on PKIs].
- J. Sherwood, A. Clark and D. Lynas, *Enterprise Security Architecture: A Business-Driven Approach*. CMP Books (2005). [This book approaches security from rather a different angle to this course. The main focus is on security for an entire enterprise, rather than for single applications. However, it provides useful background on the authors approach to enterprise security].
- F. Swiderski and W. Snyder, *Threat modeling*. Microsoft Press (2004). [The main focus of this book is on developing software. However, many of the ideas in the book have more general application to the design of secure systems. There is an accompanying (free!) software tool for producing data-driven system models for threat analysis purposes].
- M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Thomson Course Technology (2003). [Covers almost all the topics in this introductory lecture].
- S. E. Pfleeger, *Software Engineering – Theory and Practice*. Prentice Hall (2001). [Provides useful background on security for the software development process].

There are a host of other books covering similar topics.



## Standards

- ISO/IEC 17779: *Code of practice for information security management.*
- ISO/IEC 13335-1: *Management of information and communications technology security.*
- ISO/IEC 27005: *Information Security Risk Management* (under development).
- ISO 7498-2: *OSI security architecture.*
- ISO/IEC 15408 (3 parts, all published in 2005): *Evaluation criteria for IT security.*

49

There are many standards governing some or all of the issues covered in this lecture. Some of them are discussed in further detail in other courses on this MSc (including IY5501: *Security management* and IY5602: *Standards and evaluation criteria*).

We note in particular four standards (or families of standards) of particular relevance:

- ISO/IEC 17799: 2005, *Information technology – Security techniques – Code of practice for information security management.*
- ISO/IEC 13335-1: 2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.* [Supersedes ISO/IEC TR 13335 Parts 1 and 2].
- ISO/IEC 27005 (to appear, currently at CD stage), *Information technology – Security techniques – Information security risk management.* [Will supersede ISO/IEC TR 13335 Parts 3 and 4].
- ISO 7498-2: 1989 (and the parallel ITU-T recommendation X.800), *Information processing systems - Open Systems Interconnection – Basic reference model – Part 2: Security architecture.*
- ISO/IEC 15408. This standard (which is freely available) contains three parts:
  - ISO/IEC 15408-1: 2005, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*
  - ISO/IEC 15408-2: 2005, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.*
  - ISO/IEC 15408-3: 2005, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.*



Information Security Group

## Online resources

- The following resources are relevant:
  - <http://www.isg.rhul.ac.uk/~cjm/IY5601/> [the course web page];
  - [http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf\\_Home/PubliclyAvailableStandards.htm](http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm) [freely available ISO standards];
  - <http://www.sans.org/rr/> [SANS InfoSec Reading Room];
  - <http://www.securityforum.org> [Information Security Forum].

50

The following resources are relevant to this part of the course:

- <http://www.isg.rhul.ac.uk/~cjm/IY5601/> [the course web page];
- [http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf\\_Home/PubliclyAvailableStandards.htm](http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm) [freely available ISO standards];
- <http://www.sans.org/rr/> [SANS InfoSec Reading Room];
- <http://www.securityforum.org> [Information Security Forum].