UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Always A Pioneer, Always Ahead

UTeM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MyUTeM

BITS 2523
Cyberlaw & Security Policy
Lecture 14

By

Mohd Fairuz Iskandar Othman, Phd

mohdfairuz@utem.edu.my

Trusted Network

Topics covered:

- Security Architecture requirements
- Systems Evaluation
- Common Criteria
- Malaysian Common Criteria Evaluation and Certification (MyCC)
- Incident
- Incident response policy, plan and procedure

Security Architecture requirements

- In the 1970s, the US government needed to ensure that all of the systems that it was purchasing and implementing were properly protecting its most secret of secrets.
- The government had various levels of classified data (secret, top secret) and users with different clearance levels (secret, top secret).
- It needed to come up with a way to instruct vendors on how to build computer systems to meet their security needs and in turn a way to test the products these vendors developed based upon those same security needs.
- In 1972, the US government release a report that outlined basic and foundational security requirements of computer systems that it would deem acceptable for purchase and deployment.
- These requirements were further defined and built upon, which resulted in the Trusterd Computer Systems Evaluation Criteria, which shaped the security architecture of almost all of the systems in use today.

Systems evaluation

- An assurance evaluation examines the security-relevant parts of a system, meaning the Trusted Computing Base (TCB), access control mechanisms, reference monitor, kernel, and protection mechanisms.
- The relationship and interaction between these components are also evaluated in order to determine the level of protection required and provided by the system.
- How do we show/know that something is secure? – by using Security Evaluation criteria
- Security Evaluation Criteria are usually presented as a set of parameter thresholds that must be met for a system to be evaluated and deemed acceptable. These criteria are established based on a Threat Assessment to establish the extent of the data sensitivity, the security policy*, and the system characteristics.

Examples:

- US Trusted Computer System Evaluation Criteria – TCSEC (Orange Book) 1983
- European Information Technology Security Evaluation Criteria (ITSEC)
- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
- Common Criteria - CC

* In this context, “security policy” refers to the rules of configuration for a system rather than a managerial guidance document.

TCSEC, ITSEC and CTCPEC

- **Trusted Computer System Evaluation Criteria (TCSEC):** This is a standard set by DoD (United States Government Department of Defense) regarding basic needs to assess the effectiveness of security controls of companies, which are built into computer systems. It was used for evaluation, classification, and selection of computer systems which were considered to process, store and retrieve classified or sensitive data. It is often referred as the Orange Book and was issued initially in 1983 by NCSC (National Computer Security Center). TCSEC was first updated in 1985.
- **Information Technology Security Evaluation Criteria (ITSEC):** This is a structured criterion set to evaluate the security of computer systems as well as related products. It was established for the first time in May 1990 based on the work done in the UK, Netherlands, Germany, and France. Consequently, it was started first in these countries. In June 1991, an extensive international review was published (Version 1.2) for operational use in certification and evaluation systems of the Commission of the European Communities. ITSEC evaluation validity has been recognized by many European countries since 1990.

TCSEC, ITSEC and CTCPEC (cont...)

- **Canadian Trusted Computer Product Evaluation Criteria (CTCPEC):** This standard of computer security was published by the Communications Security Establishment in 1993 to offer an evaluation criterion to different IT products. It can be regarded as a combination of the TCSEC and ITSEC.
- All the above three evaluation systems are to some extent obsolete or outdated and currently replaced by a more modern approach known as the Common Criteria model, which offers similarly-defined evaluation levels, implementation of evaluation concept target, as well as the document of Security Target.

Common Criteria for Information Technology Security Evaluation (Common Criteria)

- Common Criteria or CC was prepared predominantly by unifying the above-mentioned pre-existing standards (TCSEC, ITSEC, and CTCPEC) to make sure that companies selling computer-related products for government departments (particularly for use in Defense and Intelligence) may have a standard set to be evaluated against.
- The development of CC was done jointly by the governments of the UK, the U.S., the Netherlands, Germany, France, and Canada. It is taken as the international standard (ISO/IEC 15408) regarding computer security certification and currently running the revision 4 of version 3.1.
- CC is more of a framework where users of the computer systems can state their requirements related to security functions and assurances, i.e. SFRs and SARs respectively by using the Protection Profiles or (PPs).
- Through PPs the vendors can actually make claims and/or implementations regarding their products' security attributes.

Common Criteria for Information Technology Security Evaluation (Common Criteria)

- Moreover, evaluation of the products can be done through testing laboratories to determine whether the products are truly meeting the claims.
- In a real sense, CC provides the assurance that the specification process, its implementation, and evaluation of the products related to computer security have been carried out through rigorous and standard protocols in a repeatable way at a level corresponding or analogous to the target environment for actual use.

The Concept of CC

- CC evaluations are done solely on computer security systems and products. The CC evaluation has the following key concepts:
- ***TOE or the Target of Evaluation:*** This refers to the system or product that is to be evaluated or subject to evaluation. The evaluation process is meant to validate the claims made regarding the target system or product. This can be achieved through:
  - ***PP or Protection Profile:*** It is a document, produced typically by a single user or a user community that identifies the security needs for any security device class (such as network firewalls or the smart cards used for digital signatures), which is applicable to that user for any definite purpose. The product vendors have the option to choose and implement products complying with one or more PPs. They can then evaluate their products against those chosen PPs. PP will serve as a template for the ST or Security Target of the product in such cases. The ST's authors may also at least make sure that every requirement also appears in relevant PP's targeted ST document. Thus, customers wanting particular product types can focus on products those are certified against the PP meeting their needs.
  - ***ST or Security Target:*** This is the document to identify the target's security properties for evaluation and it may claim one or more PP's confirmation. The evaluation of the TOE is done against the Security Functional Requirements or SFRs, which are established in its ST. No more or less evaluation is carried out. Thus, vendors are allowed to tailor the process of evaluation for accurate matching of the proposed capabilities of the products. Moreover, it means that network firewalls do not need to meet the similar functional needs as the database management system. This facilitates various firewalls to be evaluated against entirely different lists of requirements. Usually, the ST is published, allowing potential customers to decide on the specific security features certified through the evaluation.
  - ***SFRs or Security Functional Requirements:*** This specifies security functions for individuals that any product may provide. For such functions, a standard catalog is usually presented by the CC. For instance, how a user will act in any specific role that may be authenticated will be stated in the SFR. Even if there are two targets representing the same product type, the SFRs list can vary widely from one evaluation to the next. Even though SFRs are not prescribed by CC, it is still included in the ST as it helps to identify dependencies in cases when the right operation of one function (the ability to limit access as per roles) is dependent on another (the ability to identify roles of individuals).
-

The Concept of CC (cont...)

- The process of evaluation attempts to establish the confidence level which may be placed on the security features of the product by different processes of quality assurance:
  - ***SARs or Security Assurance Requirements:*** This is the descriptions or detailing of the measures taken while developing and evaluating the product to ensure its compliance with the security functionality claimed. For instance, in an evaluation, it may be required that full functional testing is done, or every source code to be kept in a change management system. A catalog for these aspects is provided by the CC where the needs may vary between different evaluation processes. All the requirements for any specific product or target are respectively documented in the PP and ST.
  - ***EAL or Evaluation Assurance Level:*** This is a numerical rating that describes the rigor of an evaluation process. Every EAL comprises of security assurance requirement (SARs) packages to cover the total process of a product development, with a given strictness level. There are seven levels listed in CC, the most basic being the EAL 1. It is also the cheapest level to implement and evaluate any product. Likewise, the EAL 7 is the most stringent and costliest level to implement. In general, authors of ST or PP do not individually select assurance requirements. Instead, they choose one for the whole package, perhaps 'augmenting' the needs of a few areas with that from a higher level. It is important to note that higher EALs not always necessarily imply "better security". Higher levels only signify that the claimed TOE security assurance has been verified more extensively.
- To date, most of the PPs and evaluated, certified products or STs are related to IT components (such as smart cards, operating systems or firewalls). CC certification is therefore often specified under IT procurement. There are however other product standards, including user training, system management, supplement CCs and interoperation.

The Concept of CC (cont…)

- CC is regarded as the foundation for certification schemes driven by governments, and evaluations are typically conducted to be utilized by the agencies of the Federal Government and other critical infrastructures.
- Moreover, CC allows comparison between independent security evaluation results by offering a common set of requirements related to IT product's security functionality. It also provides assurance measures concerning these IT products at the time of security evaluation. The IT products can be implemented in software, firmware or hardware.

Malaysian Common Criteria Evaluation and Certification (MyCC)

- Malaysia is one of the main manufacturers for information, communication and technology (ICT) products for local and international market. To be accepted globally, these products need to fulfil certain requirements from other countries especially when these products need to be implemented in critical sectors.
- Nowadays, the consumers are looking for an assurance that the security functions of the product are functioning as claimed by the developer. This can be achieved if the product is evaluated by an independent evaluation facility and certified by an independent certification body using the recognise standards.
- Recognising the importance of security assurance of ICT products and systems, measures will be undertaken to provide security evaluation and certification programme based on international standards.

Malaysian Common Criteria Evaluation and Certification (MyCC) (cont...)

- The 9th Malaysian Plan (2006-2010) provides a clear mandate for the establishment of a national ICT security evaluation capability.
- As extracted from paragraph 5.75 of the 9th Malaysian Plan:

  Recognising the importance of security assurance of ICT products and solutions measures will be undertaken to provide information security assessment based on international standards and certification. For this purpose, a number of evaluation laboratory facilities will be established to undertake risk assessment and security evaluation of local products with a view to facilitating market entry and consumer acceptance.

- The MyCC Scheme is one measure intended to satisfy the 9th Malaysian plan and derives its funding from Malaysian Government approval of this plan.

Malaysian Common Criteria Evaluation and Certification (MyCC) (cont...)

- National Cyber Security Policy In response to the 9th Malaysian Plan, CyberSecurity Malaysia implemented the National Cyber Security Policy (NCSP) to accumulate the national effort for enhancing the security of Malaysia's Critical National Information Infrastructure (CNII). The guiding vision for the NCSP is:

    a. *Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well-being and wealth creation*.

- The NCSP identifies eight policy thrusts:

    1) Effective Governance; 2) Legislative and Regulatory Framework; 3) Cyber Security Technology Framework; 4) Culture of Security and Capacity Building; 5) Research and Development Towards Self-Reliance; 6) Compliance Enforcement; 7) Cyber Security Emergency Readiness; 8)International Co-operation.

- The MyCC scheme is a key program within the Cyber Security Technology Framework of the NCSP that will fulfil the implementation of an evaluation and certification programme for ICT security products and systems.

Malaysian Common Criteria Evaluation and Certification (MyCC) (cont...)

- Common Criteria (CC) or ISO/IEC 15408 has been identified as a recognise standard for information technology security evaluation. While Common Evaluation Methodology (CEM) or ISO/IEC 18045 has been identified as recognise common methodology for information technology security evaluation.
- Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme is a systematic process for evaluating and certifying the security functionality of ICT products against defined criteria or standards. It is important to have a scheme to ensure high standards of competence and impartiality are maintained, and that consistency is achieved.
- MyCC Scheme evaluates and certifies the security functionality within ICT products against ISO/IEC 15408 standard which is known as Common Criteria (CC). The methodology use in the evaluation is also a recognised standard known as Common Evaluation Methodology (CEM) or ISO/IEC 18045.
- Based on the Common Criteria Recognition Arrangement (CCRA) requirement, a scheme is managed by a sole Certification Body (CB). The Certification Body for the MyCC Scheme is known as Malaysian Common Criteria Certification Body (MyCB), a department within CyberSecurity Malaysia. MyCB is responsible for carrying out certification and overseeing the day-to-day management and operation of the scheme. MyCB is independent from the Evaluation Facilities.

Malaysian Common Criteria Evaluation and Certification (MyCC) (cont...)

- This scheme also consists of an Evaluation Facility, besides the CB. The main responsibility is to carry out security evaluations against agreed standards in an independently accredited environment. The Evaluation Facility for the MyCC Scheme is known as Malaysian Security Evaluation Facility (MySEF). Currently there are three Security Evaluation Facility (SEF) licensed under MyCC Scheme that has been accredited with MS ISO/IEC 17025.
- Further information on MyCC can be obtained from:

  https://www.cybersecurity.my/mycc/about.html

What is an incident?

- An information security incident is an adverse event that threatens business security and/or disrupts service.
- Information security incident is related to loss of confidentiality, integrity or availability (CIA).
- Examples of incidents include exposure of or modification of legally protected data, unauthorized access to intellectual property, or disruption of internal or external services.
- The starting point of incident management is to create an organization-specific definition of the term *incident* so that the scope of the term is clear.
- The definition and criteria should be codified in policy.

What is an incident?

In Practice

Incident Definition Policy

Synopsis: To define organizational criteria pertaining to an information security incident.

Policy Statement:

- An information security incident is an event that has the potential to adversely impact the company, our clients, our business partners, and/or the public-at-large.
- An information security incident is defined as:
  - Actual or suspected unauthorized access to, compromise of, acquisition of, or modification of protected client or employee data, including but not limited to:
    - personal identification numbers, such as social security numbers (SSNs), passport numbers, driver's license numbers
    - financial account or credit card information, including account numbers, card numbers, expiration dates, cardholder name, and service codes
    - healthcare/medical information
  - Actual or suspected event that has the capacity to disrupt the services provided to our clients.
  - Actual or suspected unauthorized access to, compromise of, acquisition of, or modification of company intellectual property.
  - Actual or suspected event that has the capacity to disrupt the company's ability to provide internal computing and network services.
  - Actual or suspected event that is in violation of legal or statutory requirements.
  - Actual or suspected event not defined above that warrants incident classification as determined by management.
- All employees, contractors, consultants, vendors, and business partners are required to report known or suspected information security incidents.
- This policy applies equally to internal and third-party incidents.

Incident Response

- When an unauthorized incident occurs, such as an unauthorized employee copying sensitive material, a response is required.
- Incident response may be defined as the components required to identify, analyze, and contain an incident.
- Incident handling is the planning, coordination, and communications functions that are needed to resolve an incident in an efficient manner.
- Incident management can be defined as the “framework” and functions required to enable incident response and incident handling within an organization.
- The objective or goal of incident response and management is to restore normal operations as quickly as possible with the least possible impact on either the business or the users. Post-incident analysis should take place, as necessary, to identify the source of the incident.

Incident Response Capability

Benefits of having a practiced incident response capability:

- Calm and systematic response
- Minimization of loss or damage
- Protection of affected parties
- Compliance with laws and regulations
- Preservation of evidence
- Integration of lessons learned
- Lower future risk and exposure

Incident Response Policy

- The incident response policy is the foundation of the incident response program. It defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items.
- This section discusses policies, plans, and procedures related to incident response, with an emphasis on interactions with outside parties.
- We will be referring to the following document: NIST's Computer Security Incident Handling Guide

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Incident Response Policy (cont...)

Policy elements:

- Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements:
  - Statement of management commitment
  - Purpose and objectives of the policy
  - Scope of the policy (to whom and what it applies and under what circumstances)
  - Definition of computer security incidents and related terms
  - Organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process
  - Prioritization or severity ratings of incidents
  - Performance measures
  - Reporting and contact forms

Incident severity Levels

- Not all incidents are equal in severity. Included in the incident definition should be severity levels/ratings based on the operational, reputational, and legal impact to the organization.
- Corresponding to the level should be required response times as well as minimum standards for internal notification.

TABLE 11.1 Incident Severity Level Matrix

An information security incident is any adverse event whereby some aspect of an information system or information itself is threatened. Incidents are classified by severity relative to the impact they have on an organization. Each level has a maximum response time and minimum internal notification requirements.	
Severity Level = 1	
Explanation	Level I incidents are defined as those that could cause significant harm to the business, customers, or the public and/or are in violation of corporate law, regulation, or contractual obligation.
Required Response Time	Immediate.
Required Internal Notification	Chief Executive Officer. Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Compromise or suspected compromise of protected customer information. Theft or loss of any device or media on any device that contains legally protected information. A denial of service attack. Identified connection to "command and control" sites. Compromise or suspected compromise of any company website or web presence. Notification by a business partner or vendor of a compromise or potential compromise of a customer or customer-related information. Any act that is in direct violation of local, state, or federal law or regulation.

Incident severity Levels

Severity Level = 2	
Explanation	Level 2 incidents are defined as compromise of or unauthorized access to noncritical systems or information; detection of a precursor to a focused attack; a believed threat of an imminent attack; or any act that is a potential violation of law, regulation, or contractual obligation.
Required Response Time	Within four hours.
Required Internal Notification	Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Inappropriate access to legally protected or proprietary information. Malware detected on multiple systems. Warning signs and/or reconnaissance detected related to a potential exploit. Notification from a third party of an imminent attack.
Severity Level = 3	
Explanation	Level 3 incidents are defined as situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel. There is no evidence or suspicion of harm to customer or proprietary information, processes, or services.
Required Response Time	Within 24 hours.
Required Internal Notification	Chief Information Security Officer. Designated incident handler.
Examples	Malware detected and/or suspected on a workstation or device, with no external connections identified. User access to content or sites restricted by policy. User's excessive use of bandwidth or resources.

Incident Response Plan

- An incident response plan provides a roadmap for implementing an incident response program based on the organization's policy.
- The plan indicates both short- and long-term goals for the program, including metrics for measuring the program.
- The incident response plan should also indicate how often incident handlers should be trained and the requirements for incident handlers.

Incident Response Plan (cont…)

Plan elements:

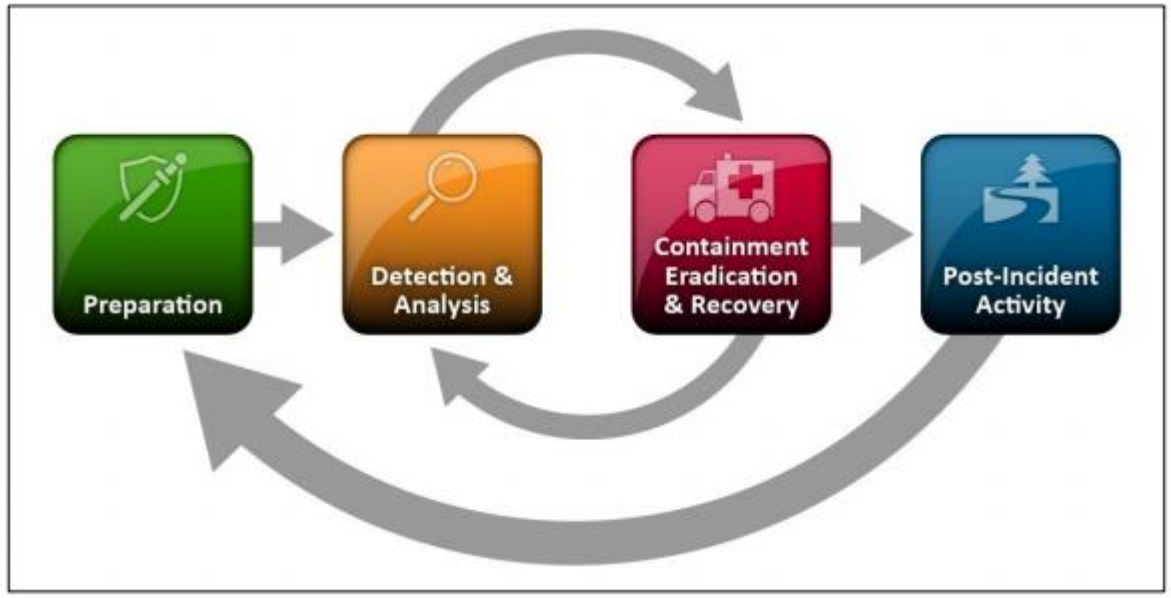
- Organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements:
  - Mission
  - Strategies and goals
  - Senior management approval
  - Organizational approach to incident response
  - How the incident response team will communicate with the rest of the organization and with other organizations
  - Metrics for measuring the incident response capability and its effectiveness
  - Roadmap for maturing the incident response capability
  - How the program fits into the overall organization.

Incident Response Plan (cont...)

- The organization's mission, strategies, and goals for incident response should help in determining the structure of its incident response capability. The incident response program structure should also be discussed within the plan.
- Once an organization develops a plan and gains management approval, the organization should implement the plan and review it at least annually to ensure the organization is following the roadmap for maturing the capability and fulfilling their goals for incident response.

Incident Response Procedure

- The incident response procedures provide detailed steps for responding to an incident. The procedures should cover all the phases of the incident response process. The procedures should be based on the incident response policy and plan.
- The incident response life cycle shows the major phases of the incident response process—preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.



Incident Response Procedure

- **Preparation**: The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented.
- **Detection and analysis**: Detection of security breaches is thus necessary to alert the organization whenever incidents occur.
- **Containment eradication and recovery**: In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident.
- **Post-incident activity**: After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents. This section describes the major phases of the incident response process—preparation, detection and analysis, containment, eradication and recovery, and post-incident activity—in detail.

Incident Response Procedure (cont…)

Procedure elements:

- Procedures should be based on the incident response policy and plan. Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations.
- In addition, following standardized responses should minimize errors, particularly those that might be caused by stressful incident handling situations.
- SOPs should be tested to validate their accuracy and usefulness, then distributed to all team members. Training should be provided for SOP users; the SOP documents can be used as an instructional tool.
- Detailed examples of various incident response procedures, please refer to:

https://www.cynet.com/incident-response/incident-response-plan-template/

Thank You

MyUTeM

www.utem.edu.my