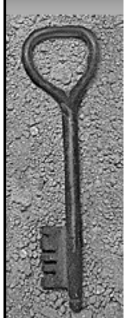
Development Process Assurance

- Role of Development Process Assurance
- Development Process Assurance in the CC
  - –Class ACM – Configuration Management
  - –Class ALC – Lifecycle Support
  - –Class AMA – Maintenance of Assurance

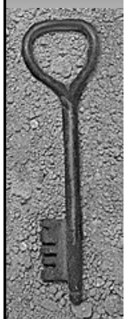
600.436 High-Assurance Systems Fall 01/Development Process Assurance 1



Role of Development Process Assurance

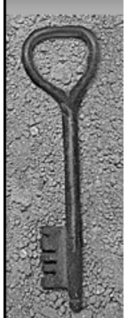
- Evidence is produced in the context of a development process
- The development process can limit the:
  - – Quality of the evidence
  - – Trustworthiness of the evidence
  - – Future reusability of the evidence

600.436 High-Assurance Systems Fall 01/Development Process Assurance 2



Development Process Assurance in the CC

- CC institutionalizes Development Process Assurance through 3 Assurance Classes containing 11 Assurance Families
  - Configuration Management (ACM)
    - Automation, Capabilities, Scope
  - Life Cycle Support (ALC)
    - Development Security, Flaw Remediation, Life Cycle Definition, Tools and Techniques
  - Maintenance of Assurance (AMA)
    - Assurance Maintenance Plan, Component Categorization Report, Evidence of Assurance Maintenance, Security Impact Analysis



Configuration Management (ACM)

- Goal of CM is to impose discipline and control on the processes for refining and modifying the TOE and its evidence
- The three Families in the Class are:
  - Configuration Management Automation (ACM_AUT)
  - Configuration Management Capabilities (ACM_CAP)
  - Configuration Management Scope (ACM_SCP)

Configuration Management Automation

- ♦ Focus is on increasing the effectiveness of the CM process
  - – Premise is that automated systems are less susceptible to human error or negligence
- ♦ Two Components, levelled on how much of TOE is subject to automated CM
  - – Partial CM Automation
  - – Complete CM Automation

Partial CM Automation

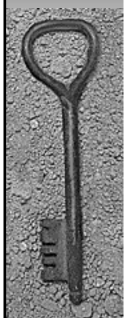
- ♦ **The developer shall use a CM system.**
  - – provides automated means by which only authorised changes are made to the TOE implementation representation.
  - – provides an automated means to support the generation of the TOE.
- ♦ **The developer shall provide a CM plan.**
  - – Describe the automated tools used in the CM system and how they are used.

Complete CM Automation

- **The developer shall use a CM system.**
  - provides automated means by which only authorised changes are made to the TOE implementation representation, **and to all other configuration items**.
  - provides an automated means to support the generation of the TOE.
  - **provides an automated means to ascertain the changes between the TOE and its preceding version.**
  - **provides an automated means to identify all other configuration items that are affected by the modification of a given configuration item.**
- **The developer shall provide a CM plan.**
  - Describe the automated tools used in the CM system and how they are used.

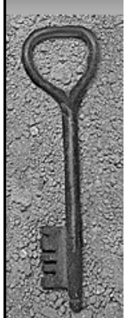
Configuration Management Capabilities

- Goals of CM capabilities are to:
  - ensure that the TOE is correct and complete before it is sent to the consumer;
  - ensure that no configuration items are missed during evaluation;
  - prevent unauthorised modification, addition, or deletion of TOE configuration items
- Five Components, levelled on capabilities, scope of CM documentation, and presence of developer justification that CM system meets its security requirements
  - Version Numbers
  - Configuration Items
  - Authorization Controls
  - Generation Support and Acceptance Procedures
  - Advanced Support



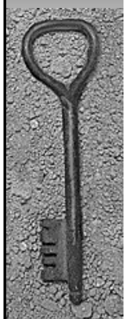
Version Numbers

- **The developer shall provide a reference for the TOE.**
  - **Unique TOE reference for each TOE version**
  - **TOE shall be labelled with its reference.**



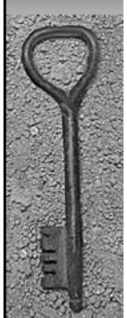
Configuration Items

- **Developer shall use a CM system**
  - **Shall uniquely identify all configuration items.**
- **Developer shall provide CM documentation.**
  - **Shall include a configuration list that describes the configuration items that comprise the TOE**
  - **Shall describe the method used to uniquely identify the configuration items**



Authorization Controls

- **Developer shall use a CM system**
  - **shall provide measures such that only authorised changes are made to the configuration items**
- **Developer shall provide CM documentation**
  - **Shall include a CM Plan that describes how the CM system is used**
  - **Shall include evidence that all configuration items have been and are being effectively maintained under the CM system and that demonstrates that the CM system is operating in accordance with the CM plan.**



Generation Support and Acceptance

- **Developer shall use a CM system**
  - **Shall support generation of the TOE**
- **Developer shall provide CM documentation**
  - **(In addition to configuration list and CM Plan) shall include an acceptance plan that describes the procedures used to accept modified or newly created configuration items as part of the TOE.**

Advanced Support

- **Developer shall use a CM system**
  - **That shall require that the person responsible for accepting a configuration item into CM is not the person who developed it.**
  - **That shall clearly identify the configuration items comprising TSF.**
  - **That shall support the audit of all modifications to the TOE, including as a minimum the originator, date, and time in the audit trail.**
  - **That shall be able to identify the master copy of all material used to generate the TOE.**
- **Developer shall provide CM documentation (that)**
  - **(In addition to configuration list, CM Plan, and acceptance plan) shall include integration procedures describing how the CM system is applied in the TOE manufacturing process**
  - **Shall demonstrate that**
    - **use of the CM system, together with the development security measures, allow only authorised changes to be made to the TOE**
    - **use of the integration procedures ensures that the generation of the TOE is correctly performed in an authorised manner**
    - **CM system is sufficient to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.**
  - **Shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.**

Configuration Management Scope

- Goal of CM Scope is to:
  - ensure that the TOE implementation representation is tracked;
  - ensure that all necessary documentation, including problem reports, are tracked during development and operation;
  - ensure that configuration options (e.g. compiler switches) are tracked; and
  - ensure that development tools are tracked.
- Three Components, levelled on the basis of what information is beingtracked by the CM system
  - TOE CM Coverage
  - Problem Tracking CM Coverage
  - Development Tools CM Coverage

TOE CM Coverage

- **Developer shall provide CM documentation that shall:**
  - **show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation**
  - **describe how configuration items are tracked by the CM system**

Problem Tracking CM Coverage

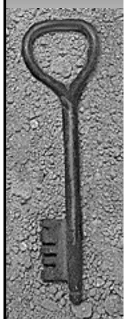
- **Developer shall provide CM documentation that shall:**
  - show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation**, and security flaws**
  - describe how configuration items are tracked by the CM system

Development Tools CM Coverage

- **Developer shall provide CM documentation that shall:**
  - show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation security flaws**, and development tools and related information**
  - describe how configuration items are tracked by the CM system

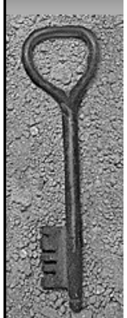
Life Cycle Support (ALC)

- Goal of life cycle support is to integrate and formalize security engineering and evidence production into the development process
- The four Families in the Class are:
  - Development Security (ALC_DVS)
  - Flaw Remediation (ALC_FLR)
  - Life Cycle Definition (ALC_LCD)
  - Tools and Techniques (ALC_TAT)



Development Security

- Goal of Development Security is to establish measures to remove or reduce threats that might exist at the developer's site
- Two Components, levelled on the basis of justification for sufficiency of security measures
  - Identification of Security Measures
  - Sufficiency of Security Measures



Identification of Security Measures

- **The developer shall produce development security documentation that shall**
  - **describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment**
  - **provide evidence that these security measures are followed during the development and maintenance of the TOE**

Sufficiency of Security Measures

- The developer shall produce development security documentation that shall
  - describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment
  - provide evidence that these security measures are followed during the development and maintenance of the TOE
    - **<u>the evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE</u>**

Flaw Remediation

- Goal of Flaw Remediation is to:
  - Ensure future maintenance and support for the TOE
  - Track, correct, and distribute flaw corrections
- Three Components, levelled on the increasing extent in scope of the flaw remediation procedures and the rigour of the flaw remediation policies
  - Basic Flaw Remediation
  - Flaw Reporting Procedures
  - Systematic Flaw Remediation

Basic Flaw Remediation

- **The developer shall document the flaw remediation procedures (in a way that shall):**
  - **describe the procedures used to track all reported security flaws in each release of the TOE**
  - **require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw**
  - **require that corrective actions be identified for each of the security flaws**
  - **describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users**

Flaw Reporting Procedures

- **The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws (in a way that shall):**
  - **ensure that any reported flaws are corrected and the correction issued to TOE users**
  - **provide safeguards that any corrections to these security flaws do not introduce any new flaws**

Systematic Flaw Remediation

- **The developer shall document the flaw remediation procedures (in a way that shall):**
  - **require timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw**
- **The developer shall designate one or more specific points of contact for user reports and inquiries about security issues involving the TOE**

Life Cycle Definition

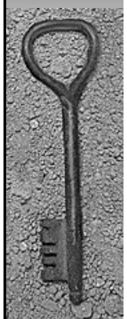
- Goal of Life Cycle Definition is to provide effective (management) control over the system engineering process used to develop the TOE
- Three Components, levelled on the basis of increasing requirements for standardisation and measurability of the life-cycle model, and for compliance with that model
  - Developer Defined Life-cycle Model
  - Standardized Life-cycle Model
  - Measurable Life-cycle Model

Developer Defined Life-cycle Model

- The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE (that shall):
  - provide for the necessary control over the development and maintenance of the TOE
- The developer shall provide life-cycle definition documentation (that shall):
  - describe the model used to develop and maintain the TOE

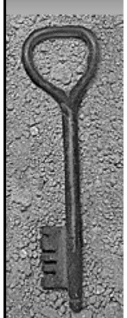
Standardized Life-cycle Model

- The developer shall use a standardised life-cycle model to develop and maintain the TOE
- The developer shall provide life-cycle definition documentation (that shall):
  - explain why the model was chosen
  - explain how the model is used to develop and maintain the TOE
  - demonstrate compliance with the standardised life-cycle model



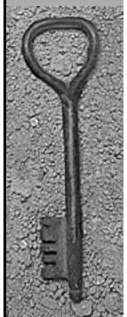
Measurable Life-cycle Model

- The developer shall use a standardised **<u>and measurable</u>** life-cycle model to develop and maintain the TOE
- **The developer shall measure the TOE development using the standardised and measurable life-cycle model**
- The developer shall provide life-cycle definition documentation (that shall):
  - describe the model used to develop and maintain the TOE, **<u>including the details of its arithmetic parameters and/or metrics used to measure the TOE development against the model</u>**
  - demonstrate compliance with the standardised **<u>and measurable</u>** life-cycle model
  - **<u>provide the results of the measurements of the TOE development using the standardised and measurable life-cycle model</u>**



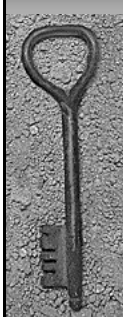
Tools and Techniques

- Goal of Tools and Techniques is to prevent ill-defined, inconsistent or incorrect development tools from being used to develop the TOE
- Three Components, levelled on the basis of increasing requirements on the description and scope of the implementation standards and the documentation of implementation-dependent options
  - Well-Defined Development Tools
  - Compliance With Implementation Standards
  - Compliance With Implementation Standards – All Parts



Well-Defined Development Tools

- **The developer shall identify the development tools being used for the TOE**
  - **All development tools used for implementation shall be well-defined**
- **The developer shall document the selected implementation-dependent options of the development tools**
  - (This documentation) **shall unambiguously define the meaning of all statements used in the implementation**
  - (This documentation) **shall unambiguously define the meaning of all implementation-dependent options**



Compliance With Implementation Standards

- **The developer shall describe the implementation standards to be applied**
  - At this level, the accountability is only for the implementation representations that the developer is actually developing

Compliance With Implementation Standards – All Parts

- The developer shall describe the implementation standards **for all parts of the TOE**
  - At this level, the accountability is extended to the implementation representations that are automatically incorporated by the tools that the developer is using (e.g., runtime libraries)

Maintenance of Assurance (AMA)

- Goal of Assurance Maintenance is to ensure that an evaluated and certified TOE still meets its ST requirements as the TOE or its environment changes
- The four Families in the Class are:
  - Assurance Maintenance Plan (AMA_AMP)
  - TOE Component Categorization Report (AMA_CAT)
  - Evidence of Assurance Maintenance (AMA_EVD)
  - Security Impact Analysis (AMA_SIA)

Assurance Maintenance Plan

- Goal of the Assurance Maintenance Plan is to identify the plans and procedures a developer must implement in order to ensure that the assurance that was established in the certified TOE is maintained as changes are made to the TOE or its environment.
  - The AM Plan is specific to the TOE, and is tailored to the developer's own practices and procedures
- One Component
  - Assurance Maintenance Plan

Assurance Maintenance Plan

- **The developer shall provide an AM Plan** (that shall)
  - **contain or reference a brief description of the TOE, including the security functionality it provides**
  - **identify the certified version of the TOE, and shall reference the evaluation results**
  - **reference the TOE component categorisation report for the certified version of the TOE**
  - **define the scope of changes to the TOE that are covered by the plan**
  - **describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact**
  - **describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date of the next re-evaluation of the TOE**

Assurance Maintenance Plan (cont)

- **The developer shall provide an AM Plan** (that shall)
  - **identify the individual(s) who will assume the role of developer security analyst for the TOE**
  - **describe how the developer security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed**
  - **describe how the developer security analyst role will ensure that all developer actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly**
  - **justify why the identified developer security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high-level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE**
  - **describe or reference the procedures to be applied to maintain the assurance in the TOE, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation**

TOE Component Categorization Report

- Goal of the TOE Component Categorization Report is to complement the AM Plan by providing a categorisation of the components of a TOE (e.g. TSF subsystems) according to their relevance to security
  - This categorisation acts as a focus for the developer's security impact analysis, and also for the subsequent re-evaluation of the TOE
- One Component
  - TOE Component Categorization Report

TOE Component Categorization Report

- **The developer shall provide a TOE component categorisation report for the certified version of the TOE (that shall):**
  - **categorise each component of the TOE,**
    - **in each TSF representation from the most abstract to the least abstract**
    - **according to security relevance– at least categorised as either TSP-enforcing or non-TSP-enforcing**
  - **describe the categorisation scheme used,**
    - **Know how to categorise new components**
    - **Know when to re-categorise existing TOE components following changes to the TOE or its security target**
  - **identify any tools used in the development environment that, if modified, will have an impact on the assurance that the TOE satisfies its security target**

Evidence of Assurance Maintenance

- Goal of Evidence of Assurance Maintenance is to establish confidence that the assurance in the TOE is being maintained by the developer, in accordance with the AM Plan
  - Developer produces evidence of security analysis and security process conformance
  - Evaluator audits evidence (to keep developer honest)
- One Component
  - Evidence of Maintenance Process

Evidence of Maintenance Process

- **The developer security analyst shall provide AM documentation for the current version of the TOE (that shall):**
  - **include a configuration list and a list of identified vulnerabilities in the TOE**
    - **The list of identified vulnerabilities in the current version of the TOE shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE**
  - **describe the configuration items that comprise the current version of the TOE**
  - **provide evidence that the procedures documented or referenced in the AM Plan are being followed**

Security Impact Analysis

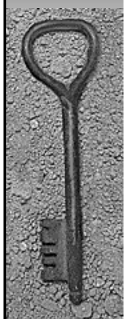
- Goal of Security Impact Analysis is to provide confidence that assurance has been maintained in the TOE
  - Relies on a developer analysis of the security impact of all changes affecting the TOE since it was certified
- Two Components, levelled according to the degree to which an evaluator validates the developer's security impact analysis
  - Sampling of Security Impact Analysis
  - Examination of Security Impact Analysis

Sampling of Security Impact Analysis

- **The developer security analyst shall, for the current version of the TOE, provide a security impact analysis that covers all changes affecting the TOE as compared with the certified version (which shall)**:
  - **identify the certified TOE from which the current version of the TOE was derived**
  - **identify all new and modified TOE components that are categorised as TSP-enforcing**
  - **for each change affecting the security target or TSF representations**
    - **briefly describe the change and any effects it has on lower representation levels**
    - **identify all IT security functions and all TOE components categorised as TSP-enforcing that are affected by the change**

Sampling of Security Impact Analysis

- **for each change which results in a modification of the implementation representation of the TSF or the IT environment, identify the test evidence that shows, to the required level of assurance, that the TSF continues to be correctly implemented following the change**
- **for each applicable assurance requirement in the configuration management (Class ACM Configuration management), life cycle support (Class ALC Life cycle support), delivery and operation (Class ADO Delivery and operation) and guidance documents (Class AGD Guidance documents) assurance classes, identify any evaluation deliverables that have changed, and provide a brief description of each change and its impact on assurance**
- **for each applicable assurance requirement in the vulnerability assessment (Class AVA Vulnerability assessment) assurance class, identify which evaluation deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable**



Examination of Security Impact Analysis

- No additional developer requirements
- Evaluator is required to do a complete check of the security impact analysis documentation to verify that **all** changes to the TOE have been analyzed and the conclusions documented

600.436 High-Assurance Systems Fall 01/Development Process Assurance 45