

KOREA Domestic IT Security Evaluation Scheme

– Devise a Fast Evaluation Scheme

2010. 9. 22
KISA
HyeonMee Pak

11th ICC 2010



Index

1. Introduction of domestic CC evaluation scheme
2. Performing domestic CC evaluation
3. Conclusions



1. Introduction of domestic CC evaluation scheme

1. History of Domestic CC Evaluation Scheme



1. Introduction of Domestic CC Evaluation Scheme

- a. Start from March, 2007
- b. Increase of demand of domestic evaluation
 - evaluation scheme : Introduction standard for all information security products
 - Increase of demand of domestic evaluation
- c. Increase of maintenance costs & evaluation of Manufacturer
 - Most of domestic manufacturers are small and medium-sized businesses
 - Increase of costs by evaluation of private evaluation agencies
 - Increase of evaluation products by changes and integrations of product types
 - Increase of maintenance costs by many attack threats

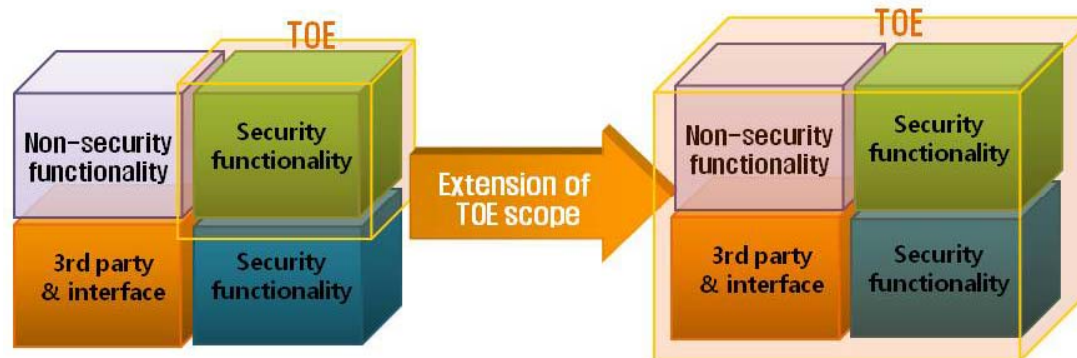
2. Alteration of Domestic CC Evaluation Scheme

- a. Start from April, 2010
- b. Losing confidence by increasing attack threats
- c. Increase of attack threats outside TOE boundary

2. Domestic CC Evaluation Method of Evaluation Scheme-1

1. Domestic CC Evaluation method

a. Scope of TOE is Extended to all functions of products



b. Performing evaluation focused on tests for product and vulnerability analysis

c. Simplifying evaluation deliverables

- Allowing deliverables of self-development document type to be applied for evaluation
- Simplifying evaluation deliverables

| Comparison | EAL1 | EAL2 | EAL3 | EAL4 |
|--------------------|------|------|------|------|
| Before Improvement | 4 | 8 | 10 | 12 |
| After Improvement | 5 | 10 | 13 | 15 |

2. Domestic CC Evaluation Method of Evaluation Scheme-2

2. Evaluation content of domestic CC evaluation by components

| Phase | Component | Evaluation content | |
|-------|---|--------------------|--|
| | | International | Domestic |
| ST | ASE_INT, ASE_CCL ASE_SPD, ASE_OBJ ASE_REQ, ASE_ECD ASE_TSS | All | All ※ Reflecting TOE scope that extended to product |
| AGD | AGD_OPE, AGD_PRE | All | All |
| ADV | ADV_ARC, ADV_FSP ADV_TDS | All | - Using as reference for functionality/vulnerability evaluation - Allowing deliverables of self-development document type |
| ALC | ALC_CMC, ALC_CMS ALC_DEL, ALC_DVS ALC_LCD, ALC_TAT | All | - Replacing with Site Visits - Minimizing detailed evaluation activities |
| ATE | ATE_COV, ATE_FUN ATE_IND | All | - Performing evaluation focused on functional test - Functional test reflecting extended TOE scope |
| AVA | AVA_VAN | All | - Strengthen evaluator's vulnerability analysis - Evaluation of developer's vulnerability analysis document - Vulnerability evaluation reflecting extended TOE scope |

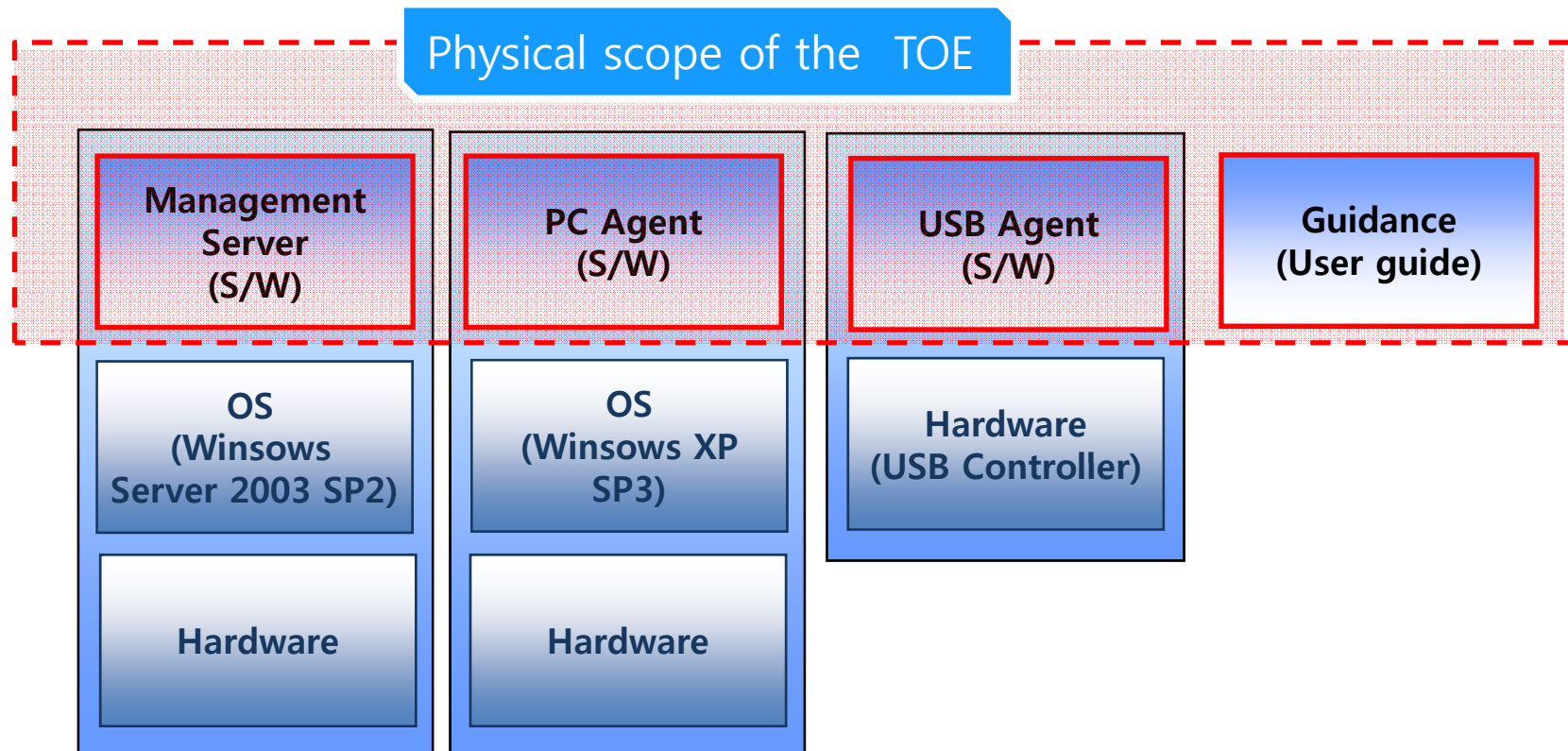
2. Performing domestic CC evaluation

1. Performing domestic CC evaluation



1. Extended Scope of Evaluation

- a. Scope of TOE is Extended to all functions of products that companies implemented
- b. Applicable practice : USB Management system



1. Performing domestic CC evaluation

c. Operational Environment of TOE



: TOE
 : TOE
 : TOE
 : TOE (Non security functionality)
 : Non-TOE (Extended TOE)

1. Performing domestic CC evaluation



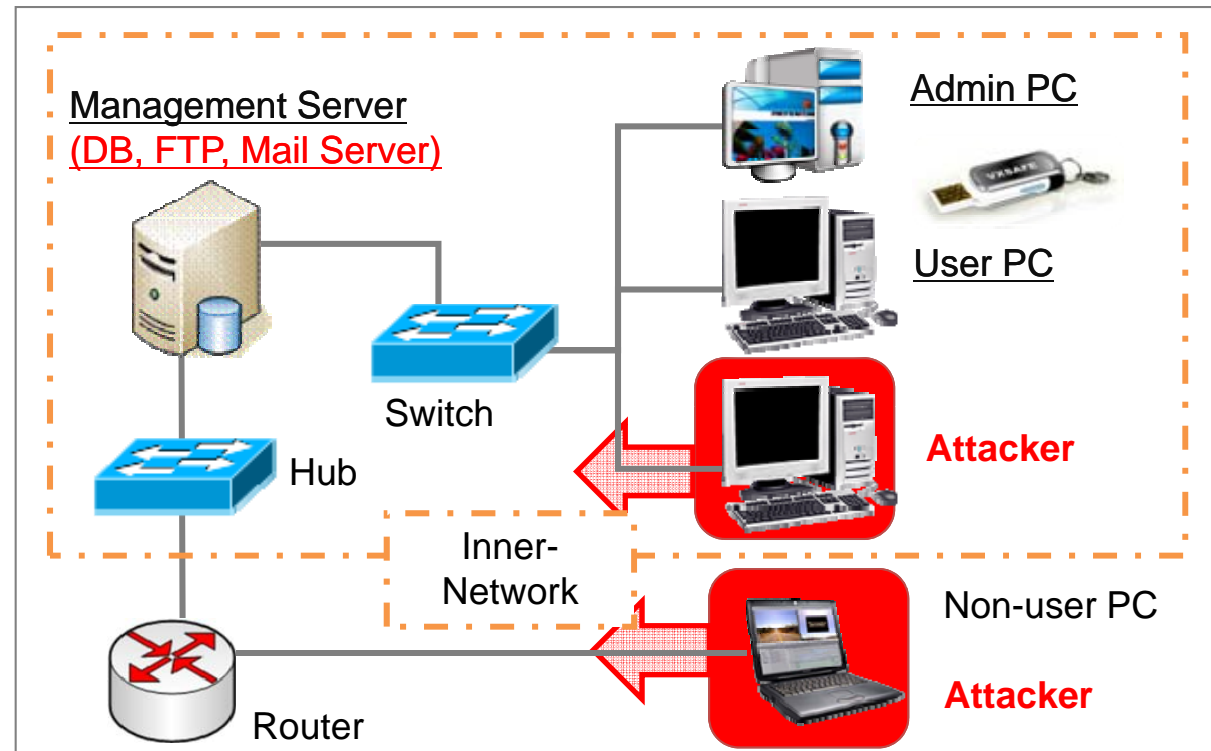
2. Evaluation focused on test and vulnerability Analysis–1

- a. Deliverables : Test Document
 - Performing functional test for external interface
 - Performing service integrated test for subsystem/interaction between subsystems
 - Performing module test(EAL4) for module/interaction between modules(internal interface)
- b. Performing Test evaluation
 - Performing all-set test of developer(function/integration, module test)
 - Performing independent functional(module) test for all functions of product
- c. Deliverables : submission of Developer's Vulnerability Analysis Document
 - Vulnerability analysis for security architecture(self protection/domain separation/non bypassability/secure initialization)
 - Identification and analysis for public domain vulnerability of functions that are used
 - Description of results of vulnerability analysis based on potential vulnerability that developer devised

1. Performing domestic CC evaluation

d. Performing vulnerability analysis evaluation

- Reenacting vulnerability analysis test that developer devised
- Identification and analysis public domain vulnerabilities of functions that are used
- Vulnerability analysis for security architecture (self protection/domain separation/non bypassability/secure initialization)
- Penetration test for all implemented functions (including non security functions)



1. Performing domestic CC evaluation



3. Simplifying evaluation deliverables and outputs

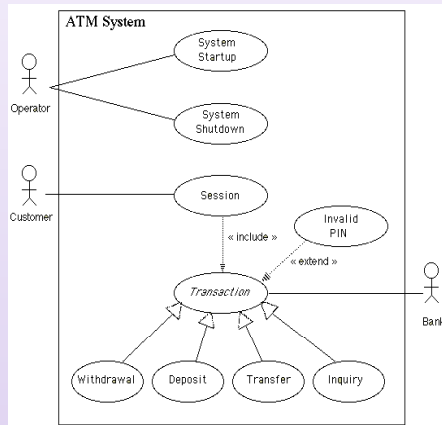
- a. Non submission of overlapped deliverable -> Replacing with existing documents
 - Security Architecture(ADV_ARC) -> Developer's Vulnerability Analysis Document(AVA)
 - Functional Specification(ADV_FSP) -> ST(ASE), Guidance documents (AGD)
 - Test document(ATE_COV, ATE_DPT) -> Test document (ATE_FUN)
- b. Simplifying evaluation and evaluation deliverables
 - Evaluating security functions and external interface by using ST and guidance document
 - Evaluating Life-cycle support(ALC_CMC/CMS/DEL/DVS) in performing Site Visits
 - Evaluator analyzes coverage and depth of test document in performing functional/module test
- c. Submission of developer's vulnerability analysis document
 - Enhancing level of vulnerability analysis

1. Performing domestic CC evaluation

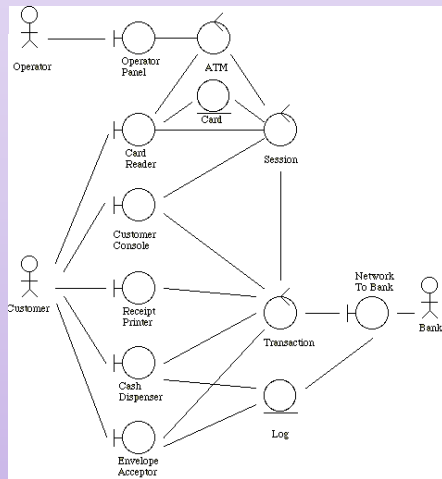
d. Development Document-Using deliverable of self-development document

ex) object-oriented analysis design

Analysis

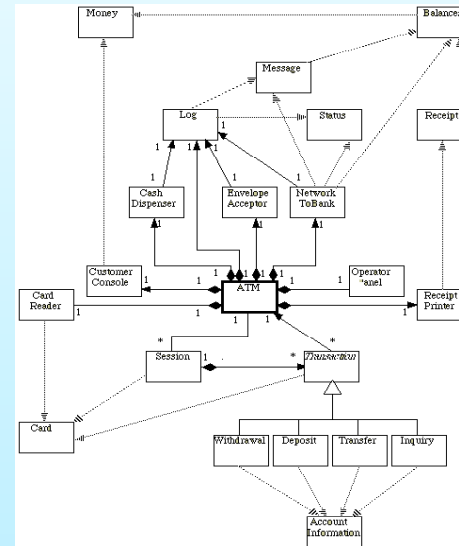


Use Case

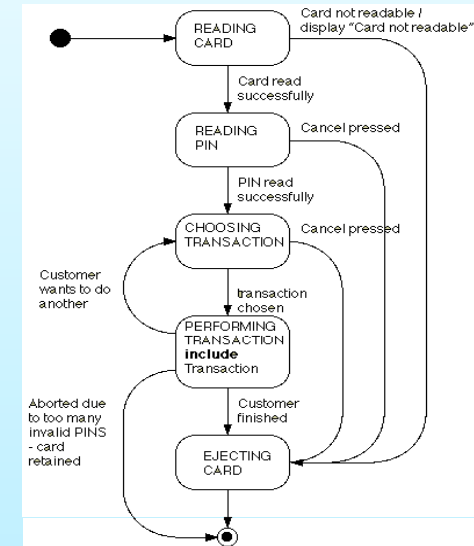


Analysis Classes

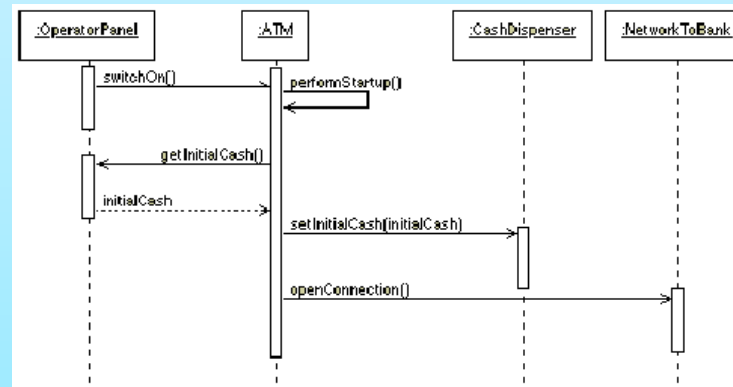
Design



Class Diagram



State Chart



Interaction Diagram

3. Conclusions

1. Conclusions



1. Effect of Domestic CC Evaluation Scheme

- a. Enhancing level of security/confidence assurance of product
 - Enhancing level of evaluation of security functionality and vulnerability analysis
 - Agency that introduced domestic CC evaluation scheme can prevent breaches by increasing security of assets

- b. Reducing costs of Manufacturers
 - Reducing maintenance costs by increasing security/confidence of product
 - Shortening period of preparation and evaluation
 - Reducing effort to generate deliverables by allowing self-development document

Thank You !!!

Question?

hmpark@kisa.or.kr

Korea Internet & Security Agency



1. Comparison of Domestic Average Period by Level

<Before Improvement>

| Level | EAL1 | EAL2 | EAL3 | EAL4 |
|-------------------------------------|--------|--------|---------|---------|
| Evaluation Period | 40days | 84days | 102days | 137days |
| Test/Vulnerability Evaluation Ratio | 25% | 37% | 38% | 37% |

<After Improvement>

| Level | EAL1 | EAL2 | EAL3 | EAL4 |
|-------------------------------------|--------|--------|---------|---------|
| Evaluation Period | 40days | 60days | 102days | 137days |
| Test/Vulnerability Evaluation Ratio | 65% | 65% | 65% | 65% |

Attachment. 1

2. Assurance Method

| ST | TOE Scope | SFR | Assurance Method |
|----|--|----------------|--|
| | Implemented security functionality | SFR Derivation | Document Assurance, Test/Vulnerability |
| | Implemented Non-security functionality | X | Test/Vulnerability |
| | Open Source Library | X | Test/Vulnerability |
| | 3rd party | X | Test/Vulnerability |

| TOE Design | TOE Design | EAL2 | EAL3 | EAL4 |
|------------|---------------------|--|--|--|
| | Summary | Non-security functionality Open Source Library 3rd party | Open Source Library 3rd party | Open Source Library 3rd party |
| | Subsystem | Security Functionality | Security Functionality Non-security functionality | Summary(Security/Non-Security Functionality) Module and Mapping |
| | Subsystem Interface | X | X | X |
| | Module | N/A | N/A | Security functionality Non-security Functionality |
| | Module Interface | N/A | N/A | TSFI (AGD Mapping) Interface between modules 3rd party and Interface |

Attachment. 2

