INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Trusted Labs

Thinking up your security

High Level CC Certification in Japan

Toru Hashimoto

IT Security Center (ISEC)

Information-technology Promotion Agency, JAPAN (IPA)

Boutheina Chetali

Innovative services & R&D programs

Trusted Labs

Contents

1. Introduction of Japan’s Scheme
2. Previous Effort for Hardware Certification
3. Going for EAL6
4. Going Further for EAL7

Contents

1. **Introduction of Japan’s Scheme**
2. Previous Effort for Hardware Certification
3. Going for EAL6
4. Going Further for EAL7

Japan’s Common Criteria Scheme

- JISEC: Japan IT Security Evaluation and Certification Scheme
- IPA: The Certification Body of JISEC
- JISEC has been established in 2001, certifying software-related products only.

Beginning of Hardware Certification

- Hardware evaluation was not in JISEC’s scope.
- Japanese chip vendors had to bring their products to Europe to obtain certification, which was very costly.
- JISEC started a project to establish hardware certification in 2009.

Contents

1. Introduction of Japan’s Scheme
2. **Previous Effort for Hardware Certification**
3. Going for EAL6
4. Going Further for EAL7

Previous Efforts

- Trial Evaluation
  - 2 pilot evaluation projects completed in 2012 and 2013.
- Test Vehicle for Vulnerability Analysis
  - Tool to assess evaluator candidates' ability necessary to carry out penetration testing.
  - Sponsored by IPA. Developed by Trusted Labs.
  - Used to accredit the first Japanese ITSEF to evaluate hardware products in 2012.

Test Vehicle (Native Smart Card)

- Developed in 2011.
- These attack methods are covered:
  - Physical Attacks
  - Perturbation Attacks
  - Side Channel Attacks
  - Fault Injection Attacks
  - Software Attacks

Test Vehicle (Java Card)

- Developed in 2012.
- This covers Java Card specific attack scenarios:
  - Global Platform
  - Byte Code Verifier / Defensive Virtual Machine
  - Java Card Firewall

Hardware Certification Scheme Successfully Established

- First ITSEF to evaluate hardware products was accredited in 2012.
- Certified products are added in the certified product list.

Contents

1. Introduction of Japan’s Scheme
2. Previous Effort for Hardware Certification
3. **Going for EAL6**
4. Going Further for EAL7

Next Step: EAL6

- High EAL (6 or higher) evaluation had also been uncovered area under JISEC.
- Market demand for high EAL certified products is growing...
- IPA is working on both sides: robustness and correctness.
- IPA decided to make it possible to evaluate at EAL6 within JISEC.

Differences between EAL5 and 6

- There are several gaps between EAL 5 and 6.
- Some of them are really challenging, especially semi-formal and formal methods evidence elements.

Assurance class	Assurance Family	EAL5	EAL6	EAL7
Development	ADV_FSP	5	5	6
	ADV_IMP	1	2	2
	ADV_INT	2	3	3
	ADV_SPM	-	1	1
	ADV_TDS	4	5	6
Life-cycle support	ALC_CMC	4	5	5
	ALC_DVS	1	2	2
	ALC_LCD	1	1	2
	ALC_TAT	2	3	3
Tests	ATE_COV	2	3	3
	ATE_DPT	3	3	4
	ATE_FUN	1	2	2
	ATE_IND	2	2	3
Vulnerability assessment	AVA_VAN	4	5	5

What Is the Matter for EAL6?

- What we need:
  - An Evaluation methodology
    - CEM defines evaluation methodology only up to EAL5.
    - Our scheme has to prepare a methodology by our own, for the Japanese Industry and beyond.
  - Skilled evaluators
    - Similar to hardware evaluations that require deep and state of the art expertise
    - Must be prepared and trained to evaluate the formal and semi-formal evidences

EAL6 Evaluation Methodology

- IPA has prepared EAL6 Evaluation Methodology for Smart Cards so that Japanese ITSEFs can use it for evaluation.
  - Sponsored by IPA.
  - Developed by Trusted Labs.
- The methodology must be both at the state of the art and concrete
  - Covers main approaches (deductive and model checking)
  - Enforced by test vehicles to practice

Test Vehicle for EAL6

- Tool to assess evaluators' ability for EAL6 evaluation.
- It can be used also for competencies and cultivation of human resources.
- Focused on ADV activities.
  - Formal Security Policy (ADV_SPM.1)
  - Semi-formal Models of the Design (ADV_FSP.5 and ADV_TDS.5)
  - Sample Source Code (ADV_IMP.2)
  - Semi-formal Mappings

Assurance class	Assurance Family	EAL5	EAL6	EAL7
Development	ADV_FSP	5	5	6
	ADV_IMP	1	2	2
	ADV_INT	2	3	3
	ADV_SPM	-	1	1
	ADV_TDS	4	5	6
Life-cycle support	ALC_CMC	4	5	5
	ALC_DVS	1	2	2
	ALC_LCD	1	1	2
	ALC_TAT	2	3	3
Tests	ATE_COV	2	3	3
	ATE_DPT	3	3	4
	ATE_FUN	1	2	2
	ATE_IND	2	2	3
Vulnerability assessment	AVA_VAN	4	5	5

Contents

1. Introduction of Japan’s Scheme

2. Previous Effort for Hardware Certification

3. Going for EAL6

4. **Going Further for EAL7**

EAL7

- JISEC is going to cover EAL7!
- EAL7 is even more challenging...
- Formal Assurance that what is described
  - Is correct (consistent)
  - Is correctly implemented in the product
- Strongly dependent on the state of the art, but
  - Must be security relevant

Assurance class	Assurance Family	EAL5	EAL6	EAL7
Development	ADV_FSP	5	5	6
	ADV_IMP	1	2	2
	ADV_INT	2	3	3
	ADV_SPM	-	1	1
	ADV_TDS	4	5	6
Life-cycle support	ALC_CMC	4	5	5
	ALC_DVS	1	2	2
	ALC_LCD	1	1	2
	ALC_TAT	2	3	3
Tests	ATE_COV	2	3	3
	ATE_DPT	3	3	4
	ATE_FUN	1	2	2
	ATE_IND	2	2	3
Vulnerability assessment	AVA_VAN	4	5	5

EAL7 Evaluation Methodology

- EAL7 is not covered by the CEM.
- IPA plans to prepare EAL7 evaluation methodology for smart cards.
- Some of evaluation activities are really challenging, especially formal method.
  - The use of formal theory is not sufficient.
  - The corresponding tools are not enough to ensure correctness.

Test Vehicle for EAL7

- Tool to assess evaluators’ ability for EAL7 evaluation.
- Includes challenges to demonstrate the feasibility and capabilities
- Customized to assess several level and the ramp up
- Focused on ADV activities:
  - A Formal Security Policy (ADV_SPM.1)
  - Formal models of the design and consistency proofs (ADV_FSP.6, ADV_TDS.6)
  - Formal proofs

Assurance class	Assurance Family	EAL5	EAL6	EAL7
Development	ADV_FSP	5	5	6
	ADV_IMP	1	2	2
	ADV_INT	2	3	3
	ADV_SPM	-	1	1
	ADV_TDS	4	5	6
Life-cycle support	ALC_CMC	4	5	5
	ALC_DVS	1	2	2
	ALC_LCD	1	1	2
	ALC_TAT	2	3	3
Tests	ATE_COV	2	3	3
	ATE_DPT	3	3	4
	ATE_FUN	1	2	2
	ATE_IND	2	2	3
Vulnerability assessment	AVA_VAN	4	5	5

Time Line

- EAL6 Evaluation Methodology

COMPLETED

- EAL6 Test Vehicle
- EAL7 Evaluation Methodology
- EAL7 Test Vehicle
  - Planned to complete in 1Q of 2014.

Conclusion

- IPA is paving the way for high level CC certification under JISEC by overcoming these obstacles:
  - Preparation of Evaluation Methodology
    - Development of evaluation methodology by IPA as the CB.
  - Training of evaluators
    - Development of Test Vehicle, which is usable for assessing the skill of evaluators and educational purpose.

Thank You for Your Attention!

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Trusted Labs

Thinking up your security

JISEC Information

English: https://www.ipa.go.jp/security/jisec/jisec_e/

Japanese: https://www.ipa.go.jp/security/jisec/

http://www.trusted-labs.com