Rump session, WEIS2010

Product-Validation Systems and the Economics of Information Security

Kanta Matsuura

(The University of Tokyo)

This talk includes results from projects supported by NEDO (New Energy and Industrial Technology Development Organization) of Japan, and JST (Japan Science and Technology Agency).

Economics of information security: Analysis, Analysis, & Analysis.

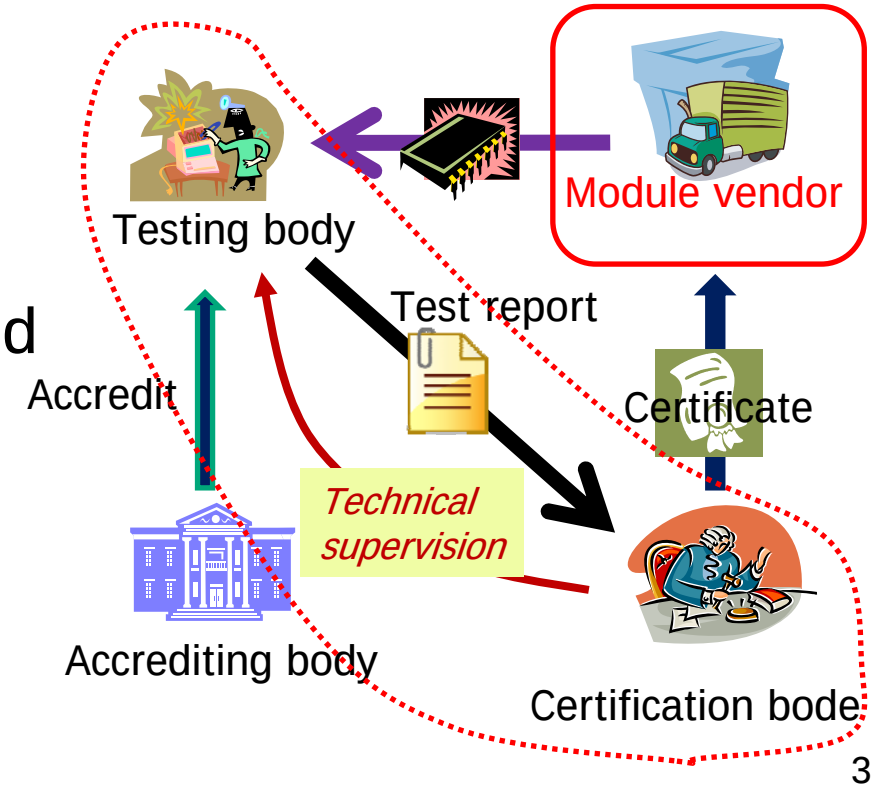
- We *understand* problems and mechanisms behind them
  - By Theories,
  - By Empirical studies,
  - And by analyzing policies.

Can we try more development-oriented works (syntheses) ?

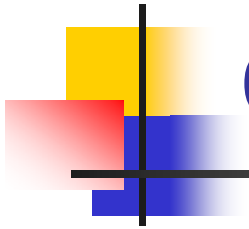
Recently, I experienced an interesting governmental project in this respect.

In the project, we *developed* a guideline for product-validation systems.

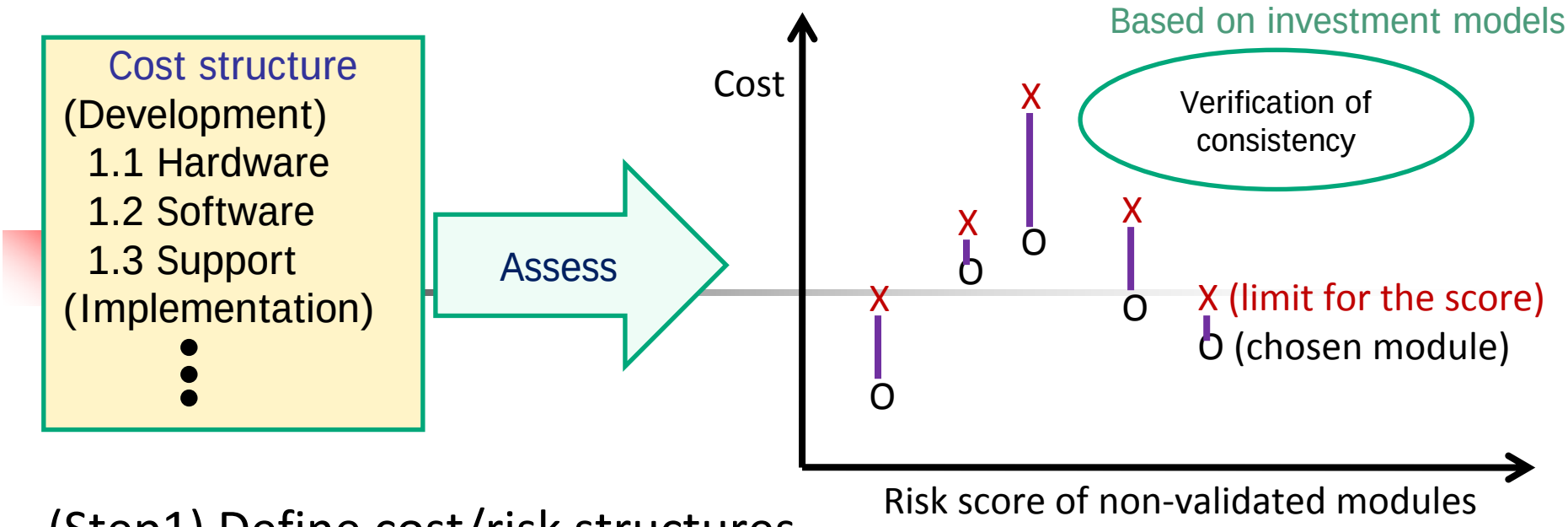
- An example: JCMVP (Japan Cryptographic Module Validation Program):
  - Full operation started in April 2007.
  - Level of a module: level1, 2, 3, or 4.
- Architecture of JCMVP



System vendors want to choose appropriate modules.



- Obviously, the higher level, the higher security. However, there are problems of cost, complicated restrictions, and so on.
- A governmental view: JCMVP pays attention to small vendors which need help when they make choices.
- Thus, we started to *develop* a guideline, based on best practices and security economics/engineering.



(Step1) Define cost/risk structures.
(Step2) Assess parameters for alternatives.
(Step3) Choose a module.
<Do Steps1-3 for all the building blocks in the system/project.>
(Step4) Trust the results so far, and plot them.
(Step5) Verify the consistency of the choices, and get suggestions for the current/next PDCA cycles.

Assess

Risk structure
(Risk factor)
1.1 Algorithm
1.2 Validation levels (1-4)
(Failure rates)
2.1 Real data
2.2 Lower-bound

The guideline was released on 20 May, 2010 (Sorry, only in Japanese).

- Available at http://kmlab.iis.u-tokyo.ac.jp/resources/guideline_1_0.pdf
- Not exclusively for JCMVP; we use a generalized description (so that we can consider other validation systems in the future).
- Current version (not an official guideline but a reference document) is a *minimal* set; it does not use many (potentially applicable) theories.
- Further development and case studies will come.