The gray zone issue

2013.08.15

ECSEC.TRA

Yasusyoshi Uemura

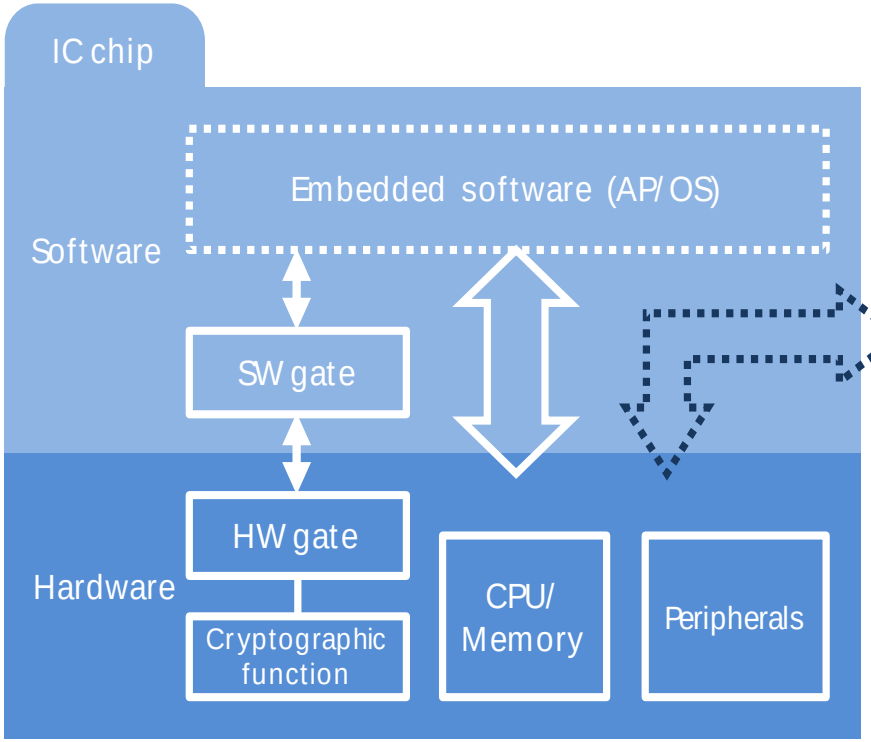
Japan's Protection Profile
Secure IC Chip for Embedded Devices
(Draft)

Edited by ICSS JC

1. This PP draft is developed by Japanese local technical community, with support from Japanese governmental budget.
2. The PP will be certified by the Japanese scheme during 2013 fiscal year in traditional CC manner.
3. TOE is the chip (hardware layer) with minimum software, being used for the module (the module will be combination of TOE and application software) which will be implemented to the device, such as mobile terminals, medical devices, smart meters, cars and so on.
4. At least the device should have “machine to machine authentication” function as the part of its application.
5. Main difference between TOE and the chip for smartcard is only one interface.
6. TOE has the interface for emulator, but smartcard has not.

7. TOE should have protection against attack from the interface for the emulation.
8. Assurance level is tentatively set as EAL4 because it will be implemented to the module in the embedded device.
9. Perhaps if the TOE is implemented to module such as SIM card, the developer may be required to let the EAL higher to similar as smartcard in their ST.
10. At this moment we are imaging to co-operating with European society, we are discussing EAL4 or higher. But we know it will be a problem if we are going to let the PP draft to international cPP.
11. Anyway, it is easy to manage the PP assurance level in future revision, the real problem is the *supporting document*.
12. On supporting document, we think almost 90% of the existing supporting document for smartcard may be reused for this PP.
13. Just a part for “the attack from the interface for the emulation” shall be newly developed.

TOE scope



Solid line Rectangle :
TOE elements

Arrow: TSFI
Note: "Cryptographic function" has no TSFI

TOE field is very near to “smartcard and similar devices”.
However it is still in “the gray zone” not yet determined how to manage this field in international CC activities.

Define the gray zone

Vision statement

There was some kind of conflict between two groups before the vision statement.
And the vision statement may be the result of a compromise between those two groups.
Success? has come just before the 13th ICCC.

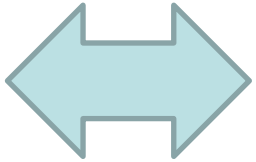
Old Eastern proverb says “Sleeping in same bed, but dreaming different”.

One will manage software products in the new manner.
Another will keep their own manner for smartcard and similar devices.

However there is a gray zone exists between two groups.

The gray zone is the frontier of CC market.
Or let us say “extension of smartcard and similar devices”.

Smartcard &
similar devices
Exceptional field

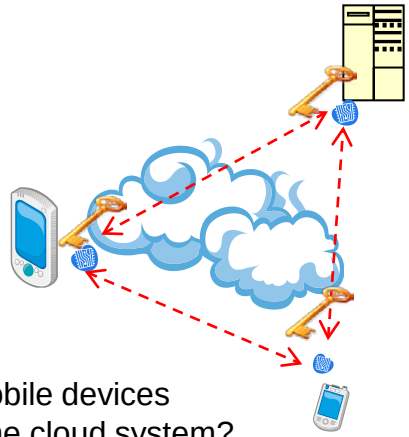


Software field
International
Technical Community

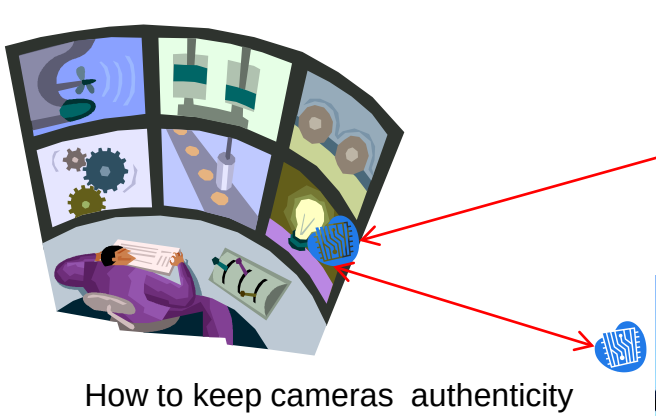
Here exists the gray zone !

Chips for the “M to M authentication”

The financial terminal implementing smart chip is the “similar device” managed by JTEMS, then how about the device implementing smart chip for another purpose?
Smart meters, medical machines connected to net work, home security devices, etc.
In Japan, this zone is called such as the “embedded device or embedded product”.



How to keep mobile devices authenticity in the cloud system?

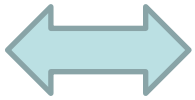


How to keep cameras authenticity in the security system?

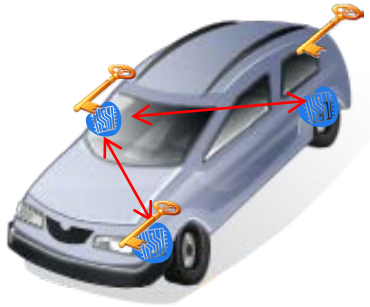
	Smartcard & similar devices	Embedded devices	Software
	HW+SW	HW+SW	SW
Attacks	Physical attack +Logical attack	Physical attack +Logical attack	Logical attack
Resistance	High level	High or medium level	Low level?*
Evaluation	Composite	Composite	Simple
Supporting documents	Already issued	Main part will be re-used. New part should be added.	Not yet developed.

*If EAL is related to resistance level.

Another issue

Commercial market  Government procurement

“A couple of embedded software and the smart chip which implements micro computer” might be a rough definition of that field.
In Japan, that kind of product has been managed as “hardware”.
Then, which group will take advantage in the gray zone?
Which CC manner will meet to this kind of products?



Frontier of CC market; Car devices
Hardware controlled by embedded chip and software.

Exceptional hardware?
Multiple functional printer (MFP) has been managed as the “software” in Japanese certification scheme.

Historical problem of CC

The historical problem in the CC theory is still exists after the vision statement.

- “Assurance level” is not “Security level”
- However CC evaluation is not just paper examination to assure all security functions stated in PP/ST are implemented
- “Were above functions securely implemented to TOE or not” or “Has TOE enough security level comparing to the product usage or not” shall be examined by third party evaluator through vulnerability analysis.
- Then how to evaluate the “security level”?
- Is there any method?

Two streams to resolve the problem

- One group intends to resolve it by cPP supporting document keeping CC evaluation to lower EAL.
- Another group intends to resolve it by vulnerability analysis related to the assurance level as described in smartcard supporting document.

Attack potential

CC version 3.1, 8.4 Evaluation assurance level 2 (EAL2) – structurally tested, paragraph 102 states as following.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential

Recommended resolution

- According to the vision statement, since cPP has to state lower EAL, every cPP product only resists to attackers with a basic attack potential.
- Even supposed product is one of COTS, many governmental IT systems shall resist to attackers with a high or moderate attack potential.
- CC part3 should be revised and separate EALs from levels of attack potential if to keep cPPs to lower EAL.

Supporting document

Which tells the truth?

The cPP way goes…

EAL will have no meaning in the future.
CEM will still be exist, however main security issues will be replaced to many supporting documents for each cPP product field.
In the supporting document, vulnerability analysis method for each cPP product field will be described such as in exist supporting documents for smartcard and similar devices.
"High assurance of security" will be guaranteed not by higher assurance level of CC evaluation but substantially guaranteed by advanced vulnerability analysis technique described in each supporting document.

The way hardware field goes…

CC and CEM structure will of course be exist in the future.
However CC maintenance for higher assurance level will substantially be done by local or regional community for hardware field products.
The field “smartcard and similar devices” should be extended to financial terminals, and may be somewhat more for hardware product which needs same kind of evaluation methodology.
In these product fields, “assurance level” may still be related to vulnerability analysis technique such as described in exist supporting documents for smartcard and similar devices.

Gray zone product again

Definition
A couple of embedded software and the smart chip which implements micro computer

The TOE field is very near to “smartcard and similar devices”.
Exist supporting documents for “smartcard and similar devices” are very convenient to re-use for this field.

Smartcard's wisdom

VAN	Vulnerability testing X point
5	X
4	X-α
3	X-β

In each vulnerability testing, points are determined according to VAN level.

High point=high VAN level, means highly resistant to the attack potential.

Above means one supporting document can cover rather deep product field. (Not wide but)

Not related to specific PP, but can cover higher resistant product to lower.

It's a kind of wisdom.

It’s a wisdom for private market

Commercial market  Government procurement

Since there will be many applications for one product field in the private market,
One application needs highest resistance to the attack potential.
Another needs not highest, but should be resistant against moderate or lower attack potential.

Recommended resolution

- “Relate with EAL or not” is not the matter.
- However “Relate with attack potential level” is still needed for the private market.
- If we want to manage “embedded device” field by CC manner, re-use of existing supporting documents for the “smartcard and similar devices” is very convenient.

Conclusion

A political issue concerning the gray zone

Let the exceptional “smartcard and similar devices” field expand to all “embedded device”.

Let the vision statement proceed to all hardware product except the “smartcard and similar devices”.

Not saying political issue directly however..

At least
If we want to manage “embedded device” field by CC manner, re-use of existing supporting documents for the “smartcard and similar devices is very convenient.

“It’s better to respect the wisdom and experience of smartcard field” is the conclusion.

International technical community

Following is just concern

To create the cPP with supporting document, at least several times, hopefully 5 to 10 of face to face discussion shall be needed.
If CCRA intends to succeed to create cPPs for many product fields at once, almost all discussions will be held in one or two continents by small size of members.
It will be difficult for Asian stakeholders to attend every discussion held at western continents.
Even though we are watching CCUF website, however we could catch very small news how CC is going after the vision statement for this one year.
If CCRA intends to be fair, at least ISO manner to set the meeting shall be traced, however it will increase the cost for creating cPP, decrease the speed to the goal.

Thank you!

Contact: uemura@ecsec.org

ELECTRONIC COMMERCE SECURITY TECHNOLOGY RESEARCH ASSOCIATION