Seminar on Cybersecurity Testing, Hong Kong 2018

Development and applications of the Common Criteria for IT security evaluation

Hongsong Shi

China Information Technology Security Evaluation Center

Hong Kong

2018.7

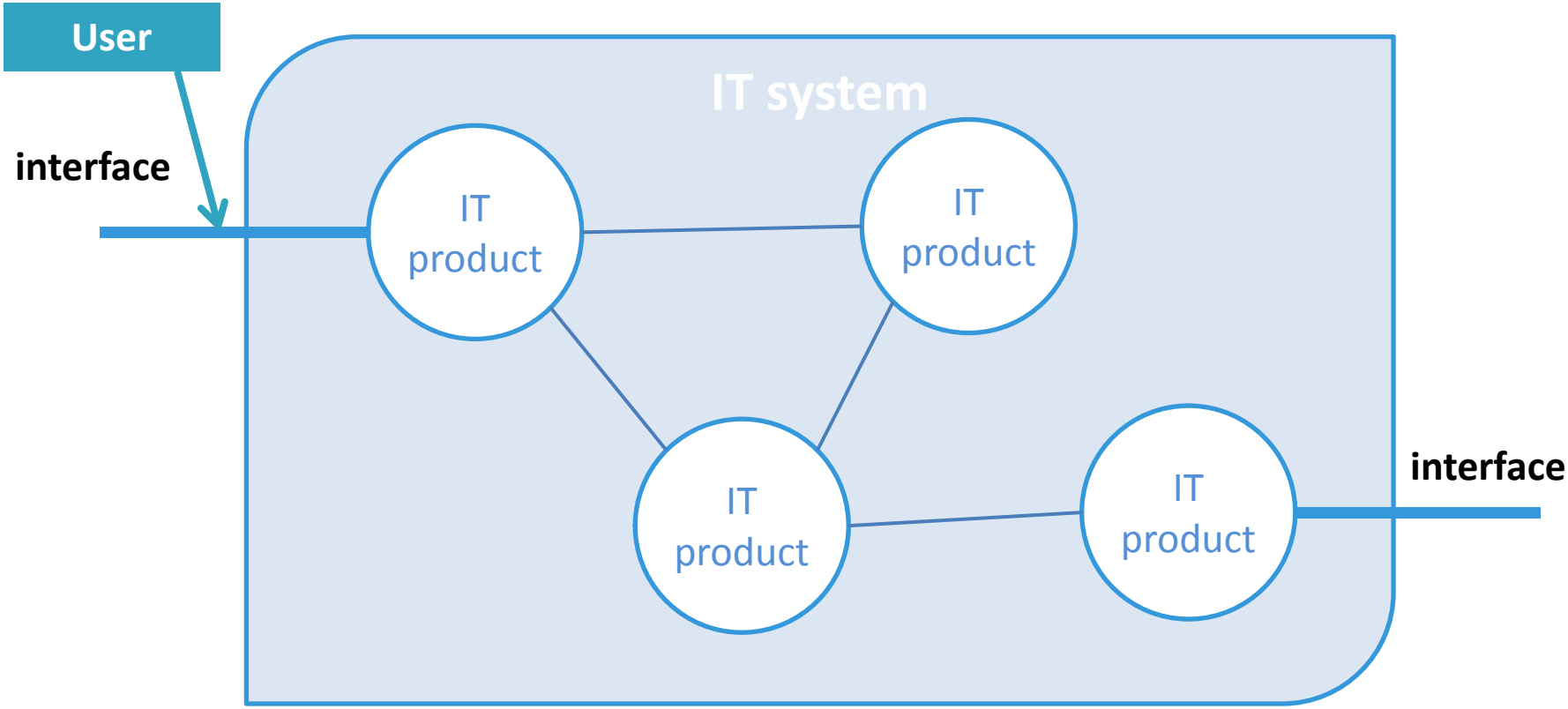
Outline

- Why we need security evaluation?
- What is the Common Criteria?
- How well does it work?
- Is it still in progress?

Outline

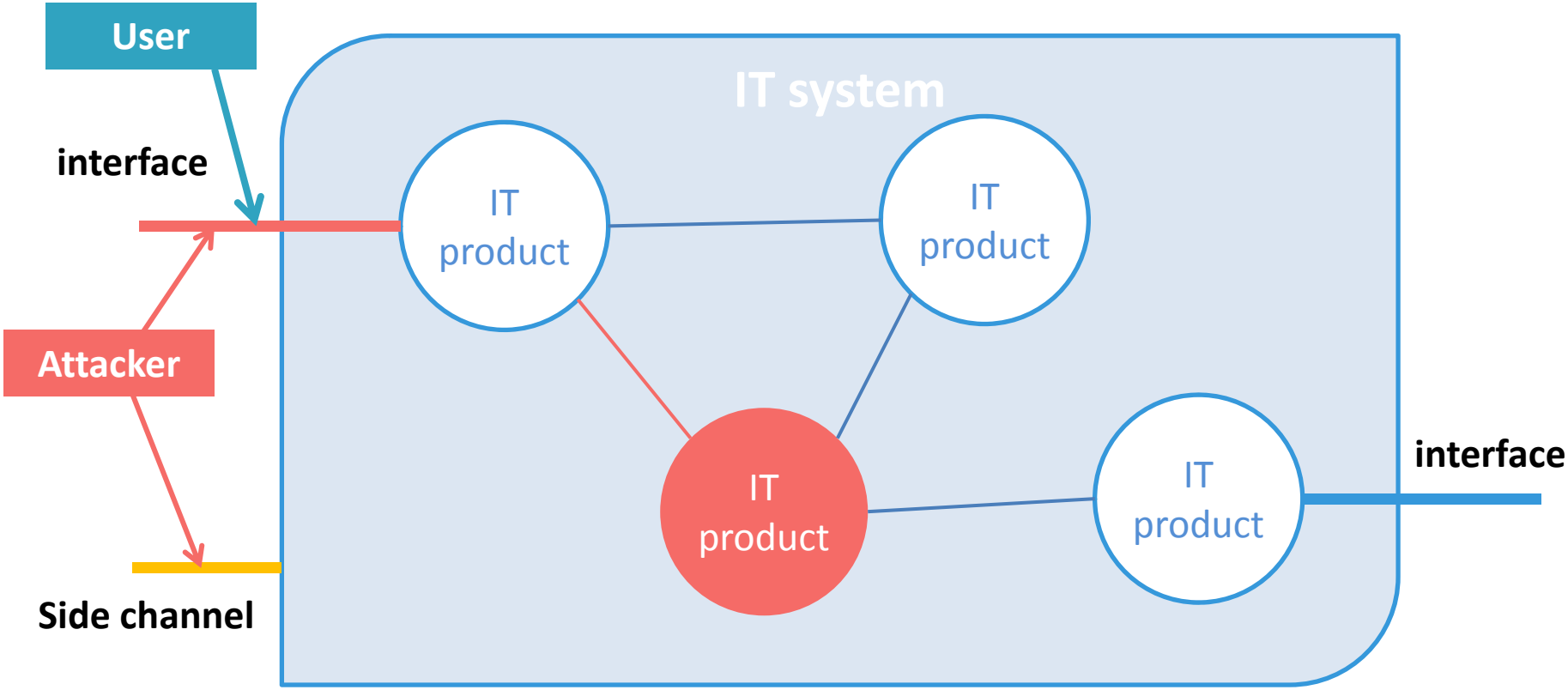
- Why we need security evaluation?
- What is the Common Criteria?
- How well does it work?
- Is it still in progress?

Attacks are ubiquitous



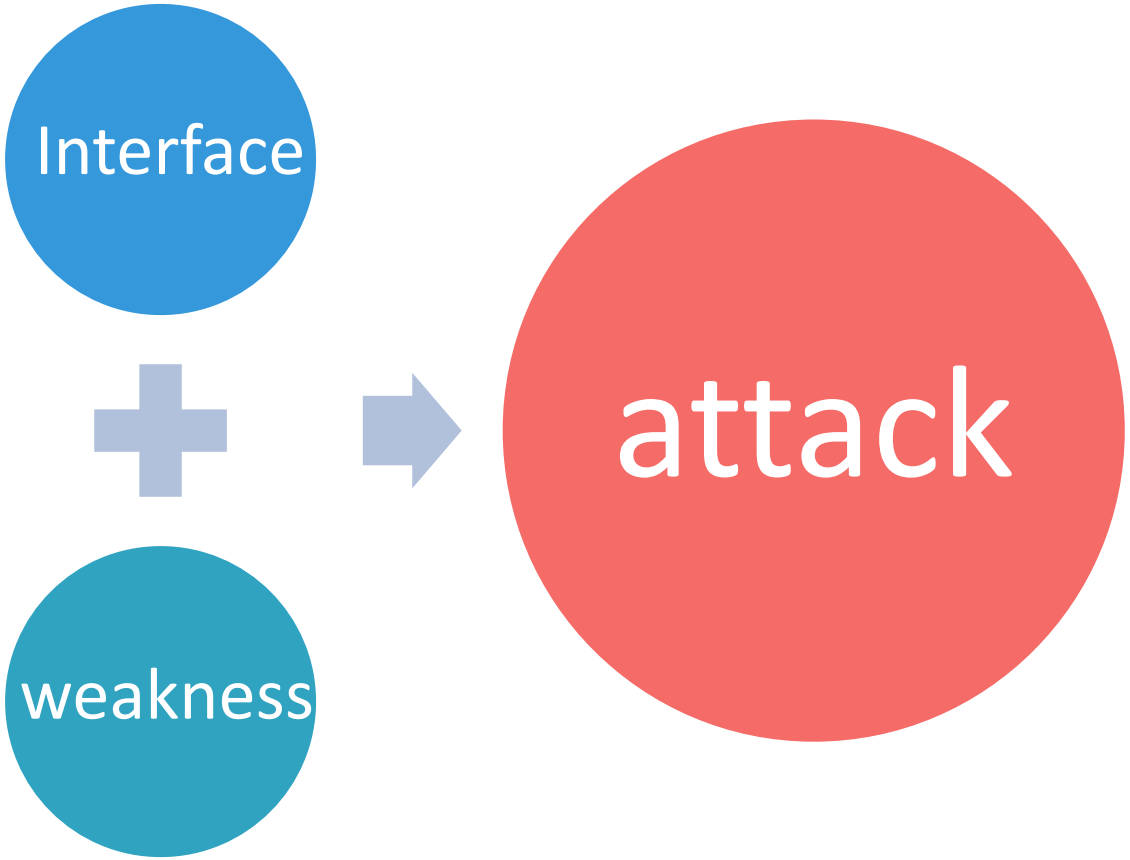
- Various IT products are integrated into an system to realize specific functions

Attacks are ubiquitous



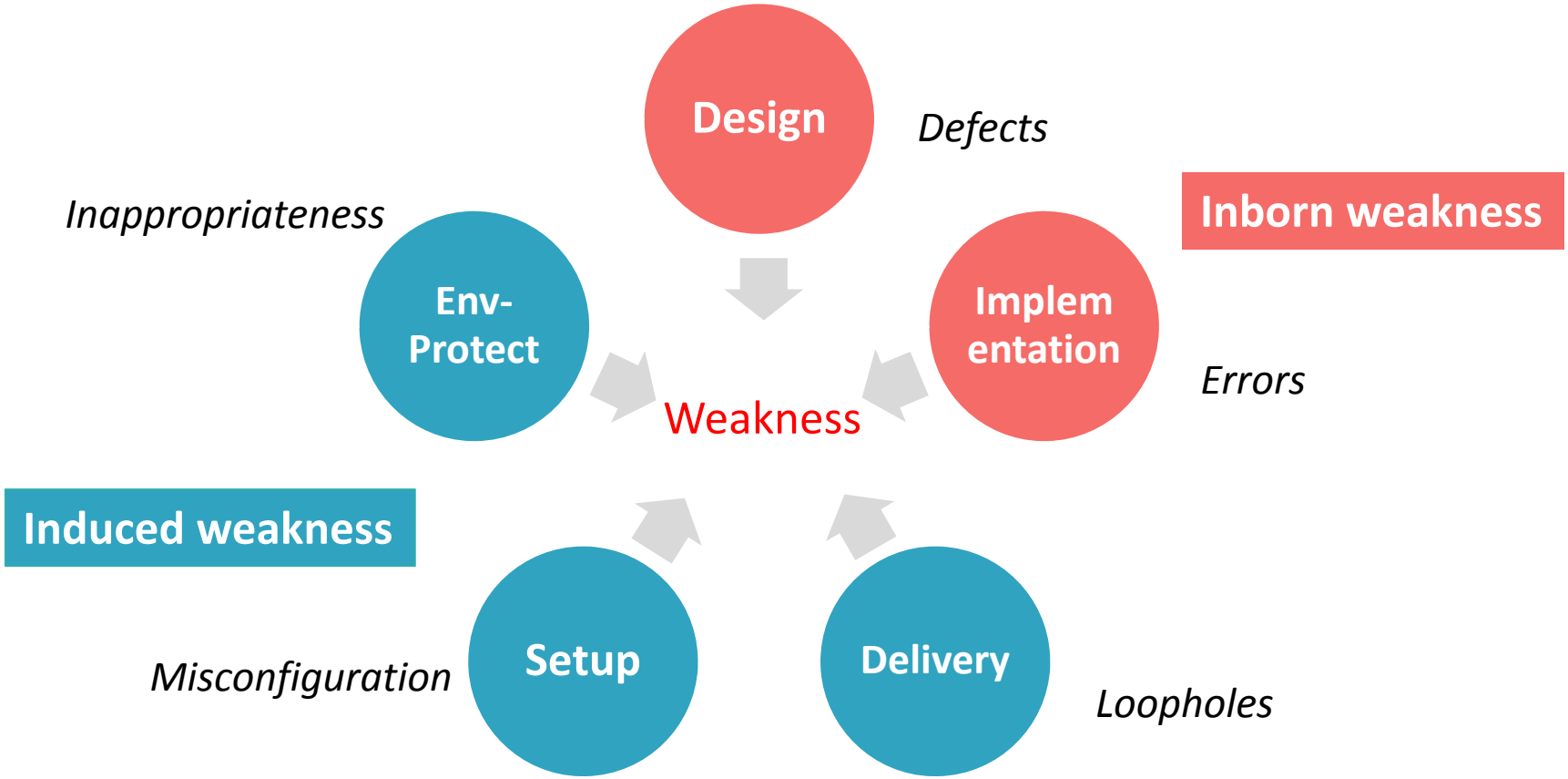
- Various IT products are integrated into an system to realize specific functions
- IT system may include something that attracts the attacker to conduct actions
- The interface and side channel can be the entry points of the attacks

Attacks are ubiquitous



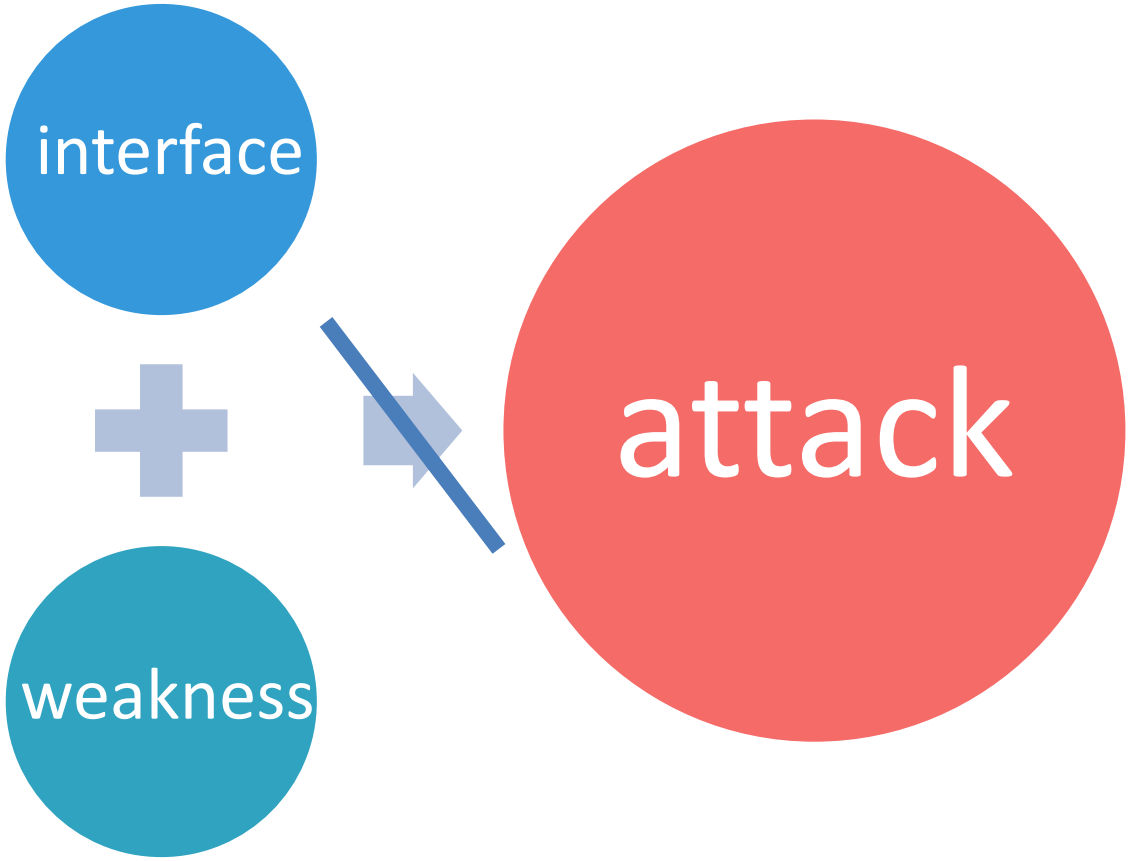
- Availability of interfaces and the existence of weakness would induce attack

Weakness in IT products



How to resist attacks

Reduce the availability of it to the attacker

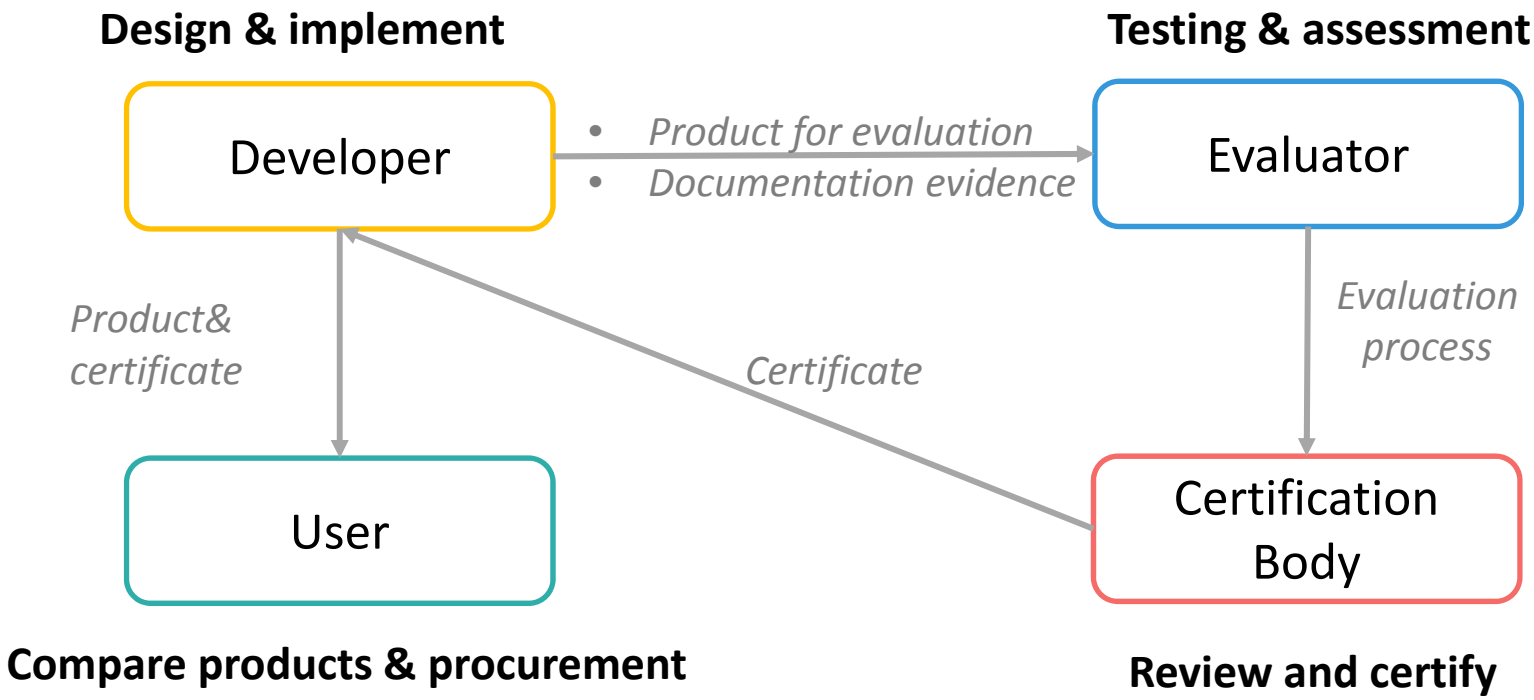


Remove or patch it as possible as we can

The role of security evaluation

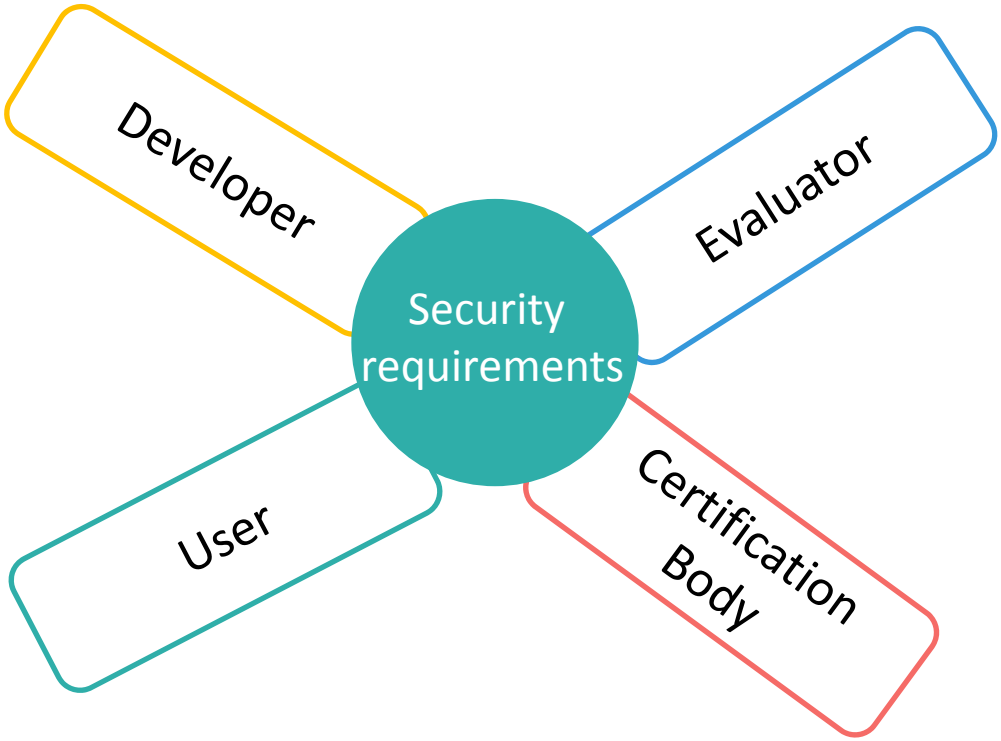
- Remove weakness as possible as we can
  - Examine the design and implementation documents
  - Test the correctness of security functionality
  - Assess the risks induced by potential vulnerabilities
- Recommend the developer/user to adopt appropriate technical and administrative countermeasures
  - Follow the examined guidance and procedure to develop, deliver, install and operate the product
  - To reduce the interface availability to the adversary
    - Remove unnecessary interfaces and make them compact
    - Adopt strict access control measures in the environment
    - Reduce or randomize the leakage of side channels

General framework for security evaluation



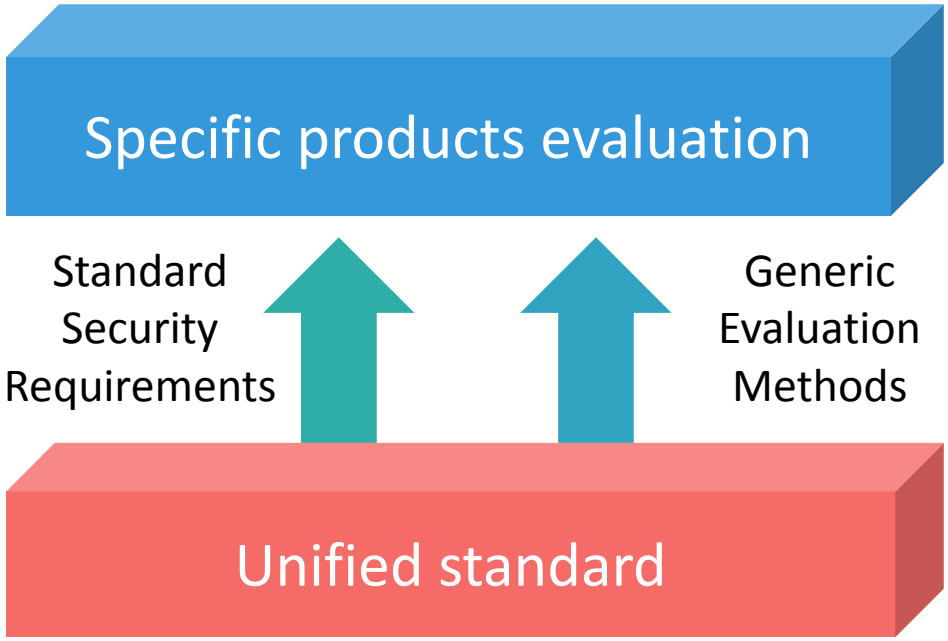
- Why the involved parties can trust each other?
  - Who define the security requirement?
  - What standards or specifications should be relied on?

Who define the security requirements



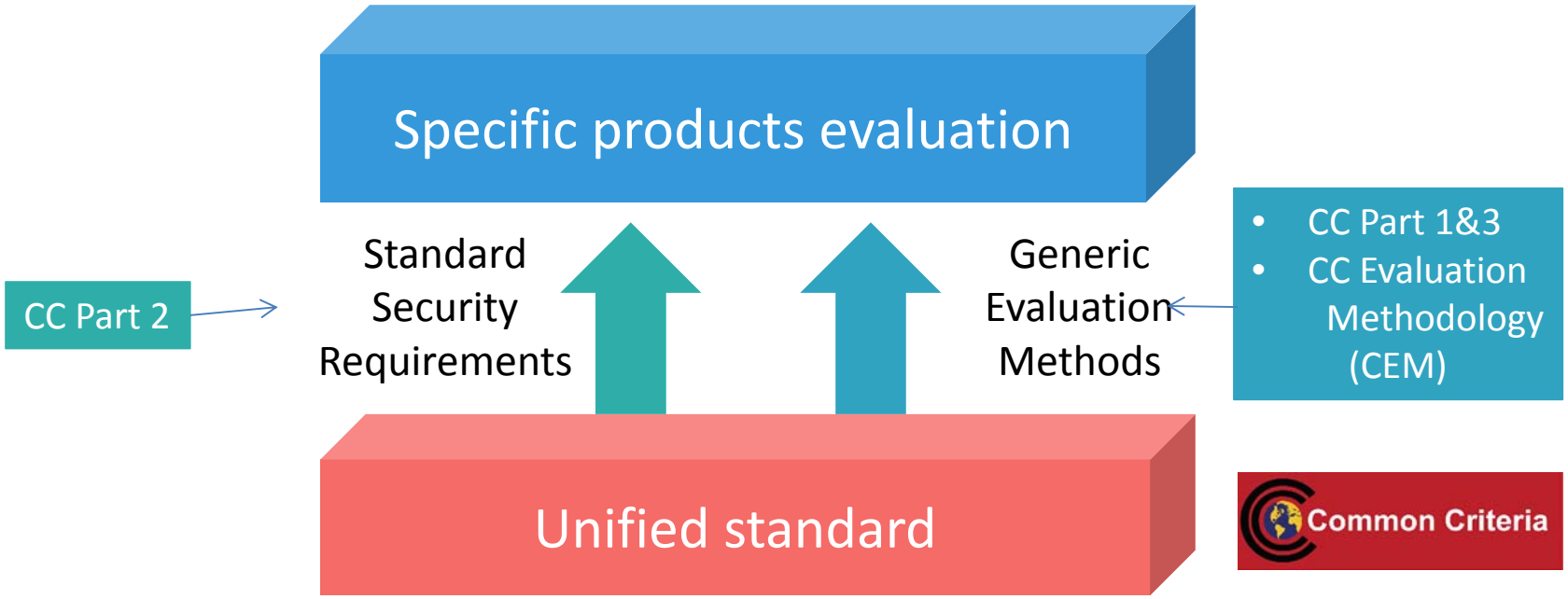
- All the parties collaborate to formulate the requirements
  - User can clarify what they want and care for
  - Developer can know the exact meaning of the requirements
  - Evaluator can verify the satisfiability of the requirements
  - CB can check the validity of the evaluation process based on the requirements

What standards should be relied on?



- Unified standard is the ground for mutual trust and recognition
  - Expressing requirements in a standard way can reduce ambiguity
  - Generic evaluation methodology can treat all kinds of products evaluation in a simple and uniform way
  - Community recognized methodology is helpful to remove uncertainty about the evaluation process

What standards should be relied on?

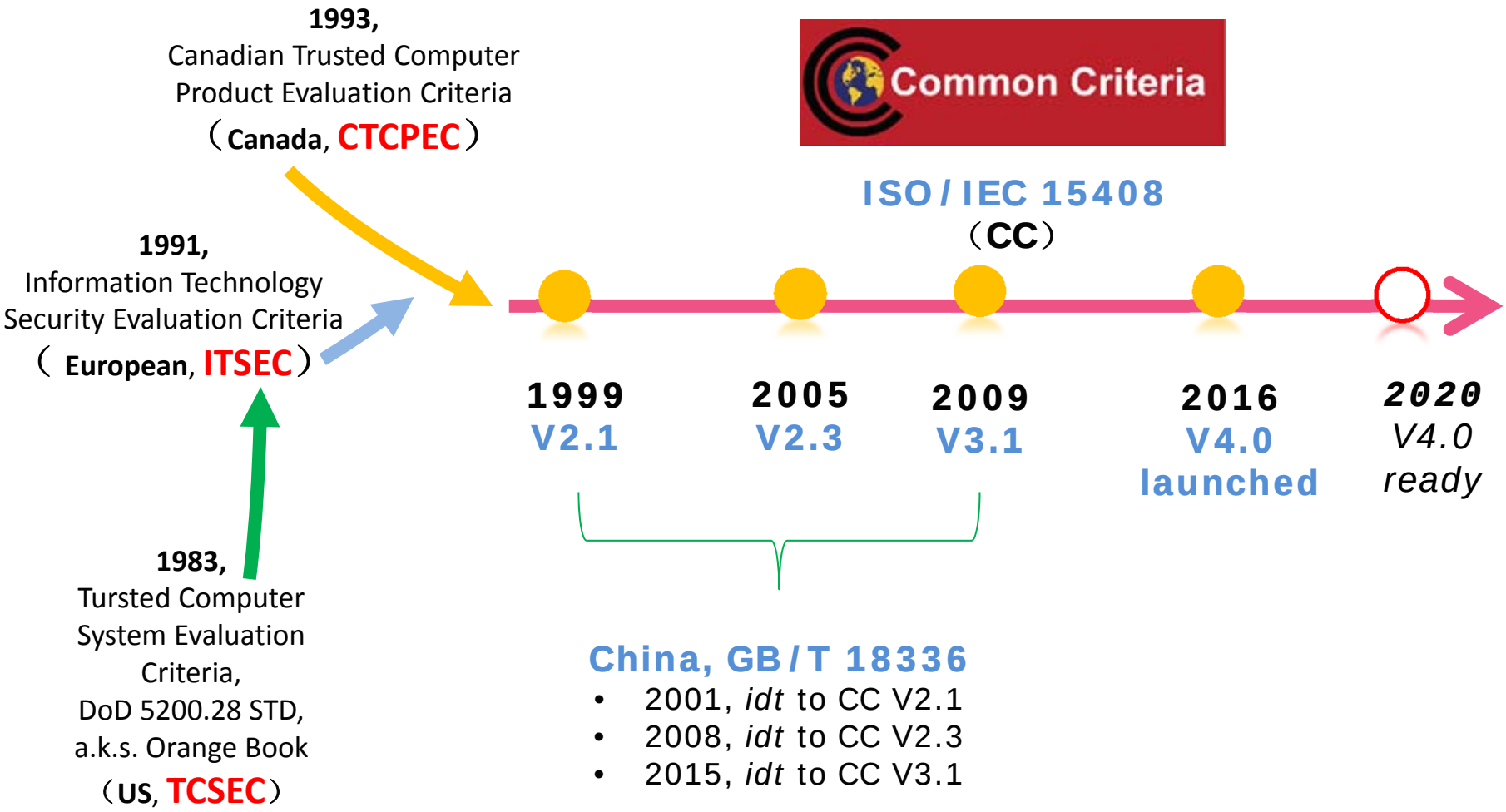


- Unified standard is the basis to achieve mutual recognition
  - Expressing requirements in a standard way can reduce ambiguity
  - Community recognized methodology is helpful to remove uncertainty about the evaluation process
  - Generic evaluation methodology can treat all kinds of products evaluation in a simple and uniform way

Outline

- Why we need security evaluation?
- What is the Common Criteria?
- How well does it work?
- Is it still in progress?

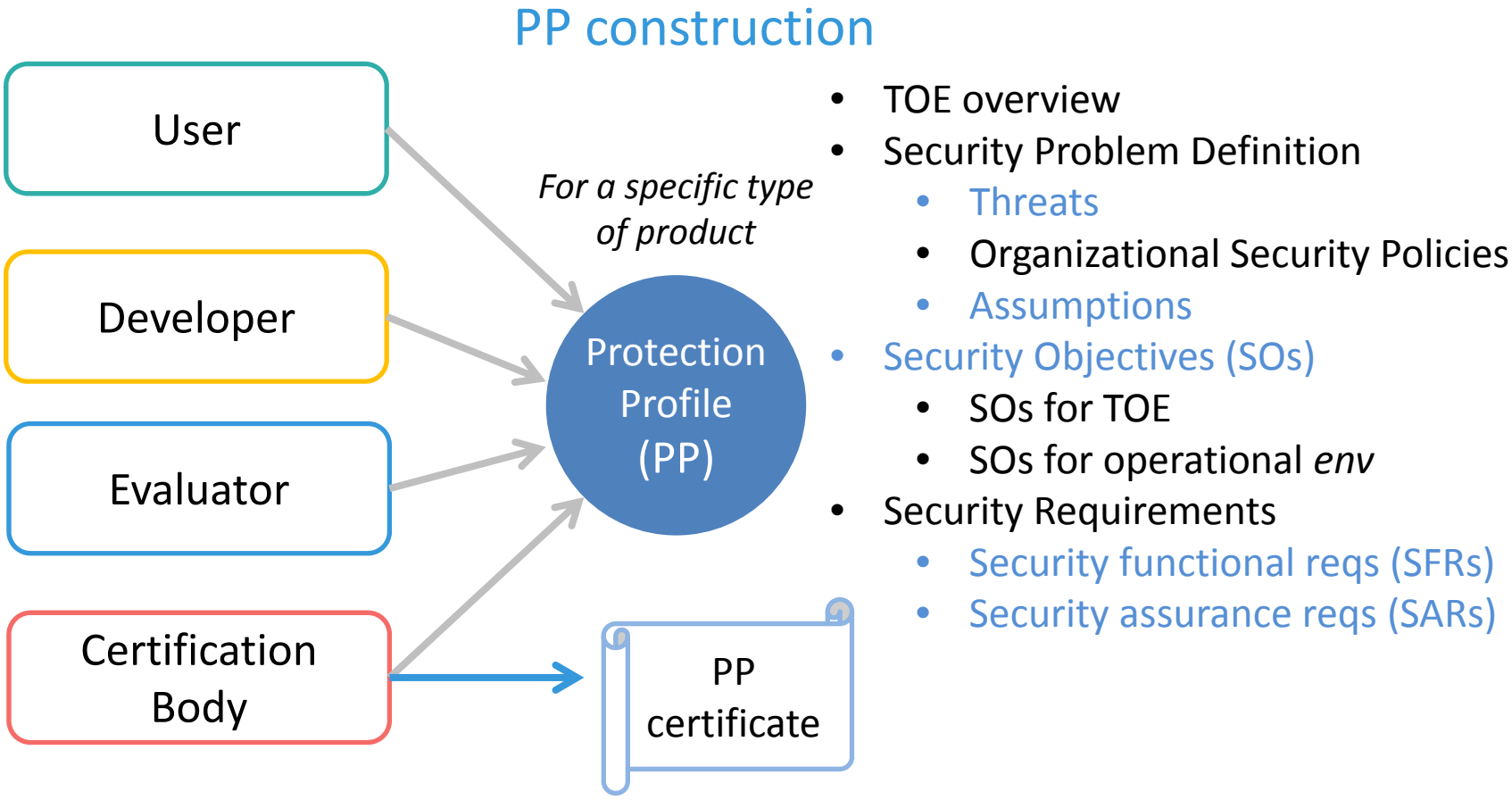
Brief history of CC



The Common Criteria

- CC is a fundamental standard for security evaluation
  - ISO/IEC 15408-2009
  - **The general model** for security evaluation(Part I)
  - **Security functional components** can be chosen to express requirements in a standard way (Part II)
    - 11 security functional classes are specified, and the users can extend them to characterize more specific requirements
  - **Security assurance components** can be used to express evaluation requirements in a generic way (Part III)
    - 7 security assurance classes and 7 predefined assurance packages
- A companion standard
  - ISO/IEC 18045-2009
  - **The evaluation methodology** describes the general methods in performing evaluation activities (CEM)

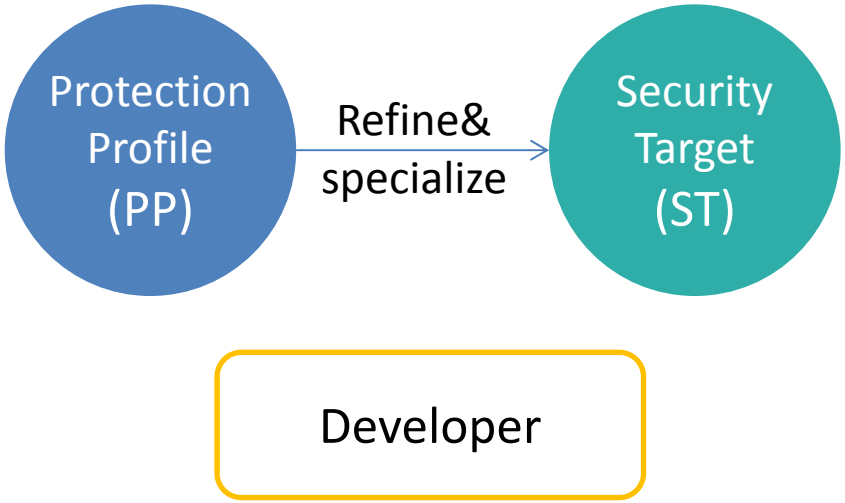
General model of CC evaluation



- PP is a security requirement specification for a specific type of product
- The logic correspondence between the assumptions, threats, security objectives and security requirements should be analyzed

General model of CC evaluation

ST construction

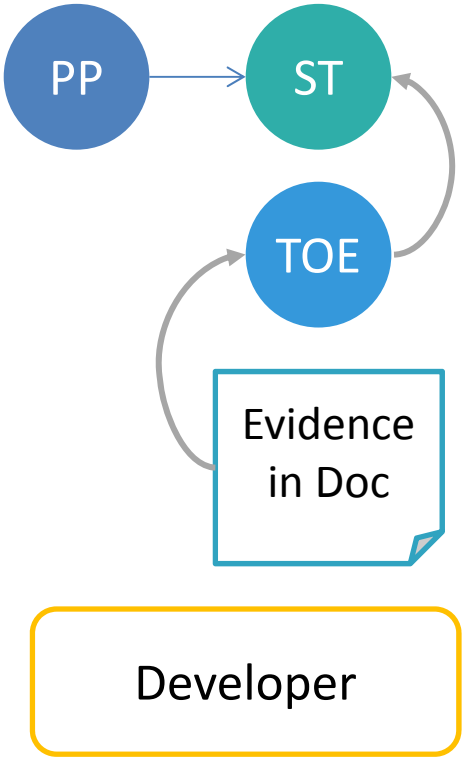


- TOE description
- Security Problem Definition
  - Threats
  - Organizational Security Policies
  - Assumptions
- Security Objectives (SOs)
  - SOs for TOE
  - SOs for operational *env*
- Security Requirements
  - Security functional reqs (SFRs) with refinement
  - Security assurance reqs (SARs) with refinement

- ST is the specialization of PP, which specifies the exact security requirements of a specific product

General model of CC evaluation

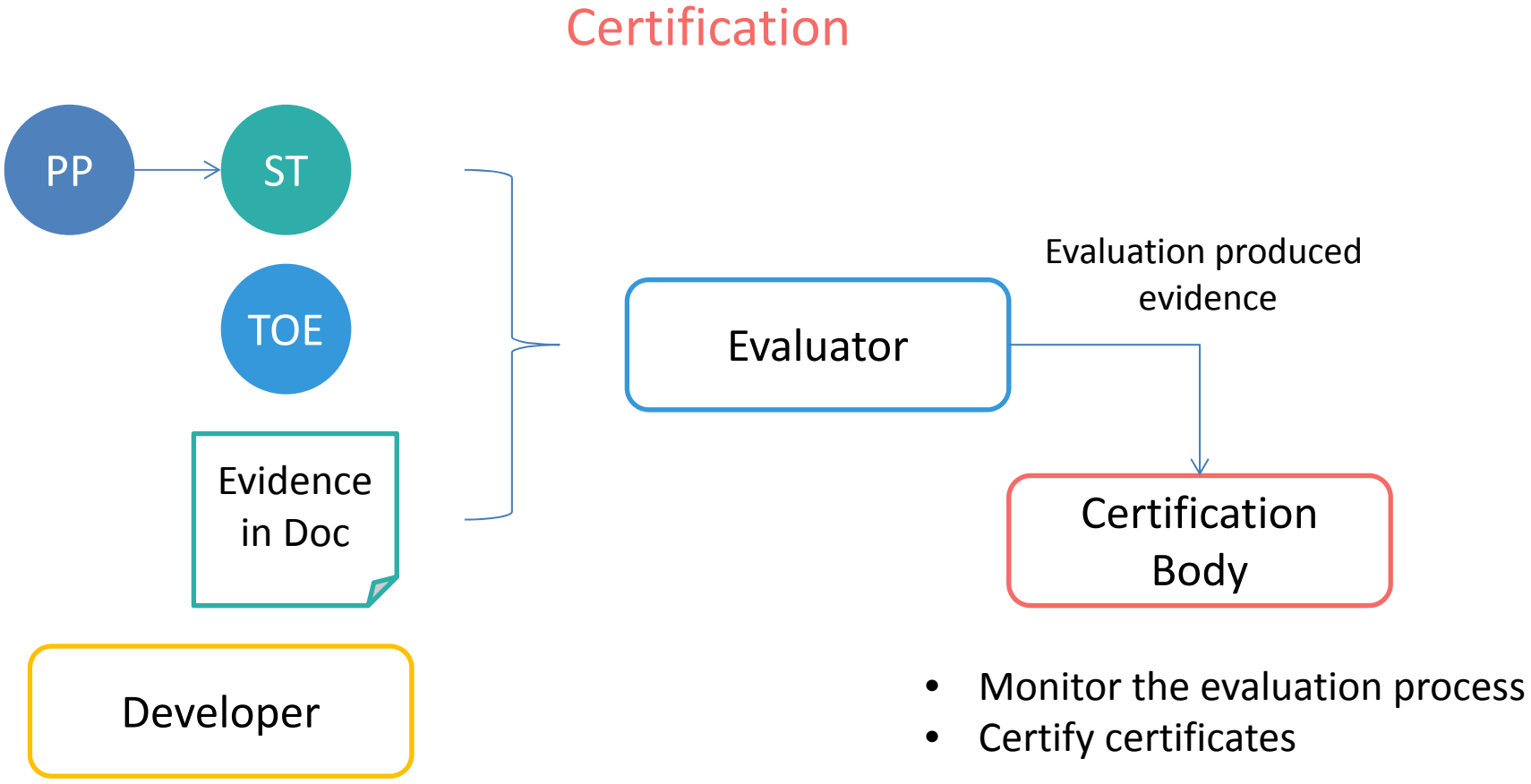
TOE evaluation



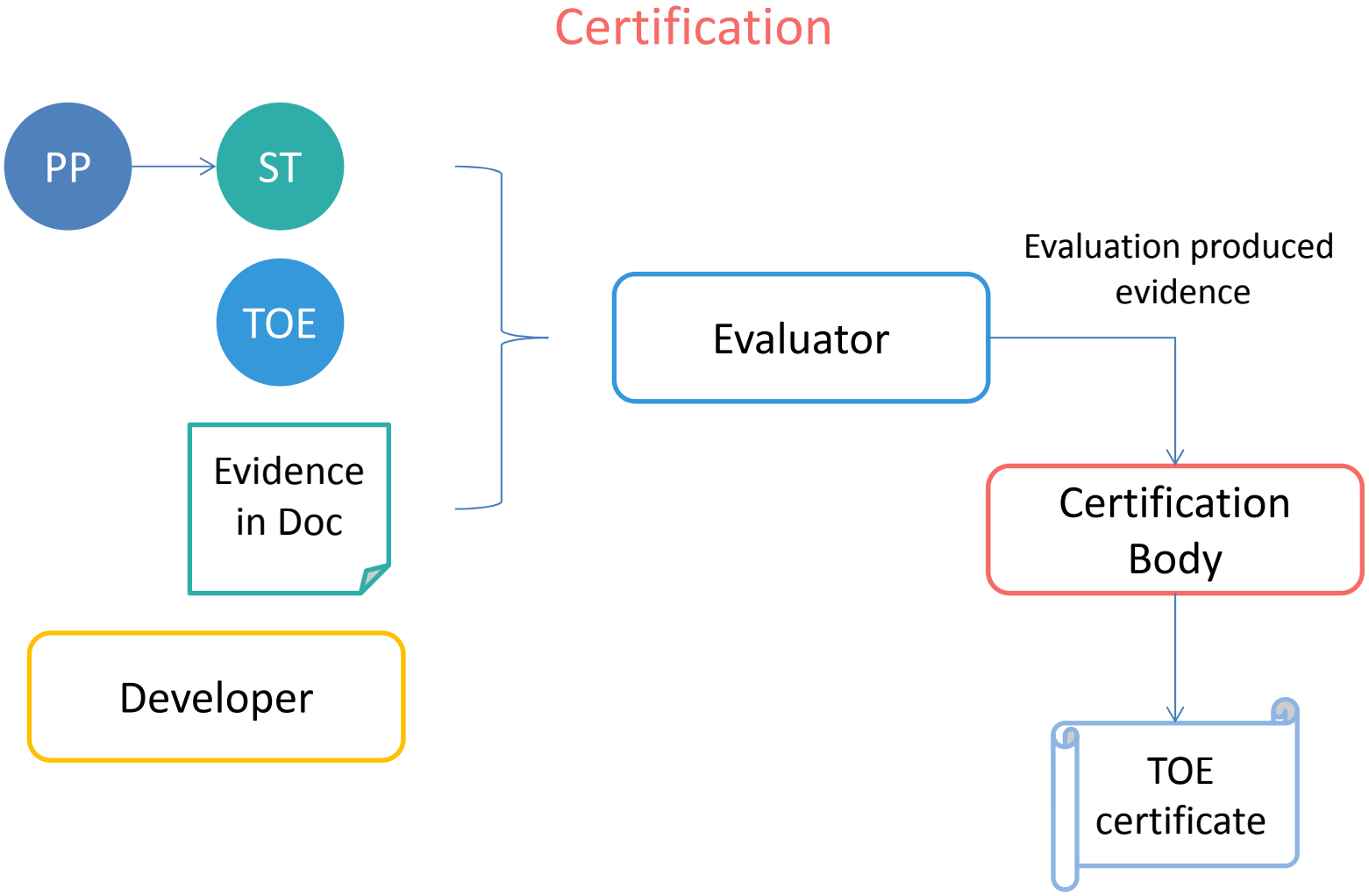
Evaluator

- Examine the documentation to confirm the countermeasures can resist all the know threats in principle (i.e., Sufficiency of the countermeasures)
- Validate the countermeasures are correctly implemented (i.e., Correctness of the countermeasures)

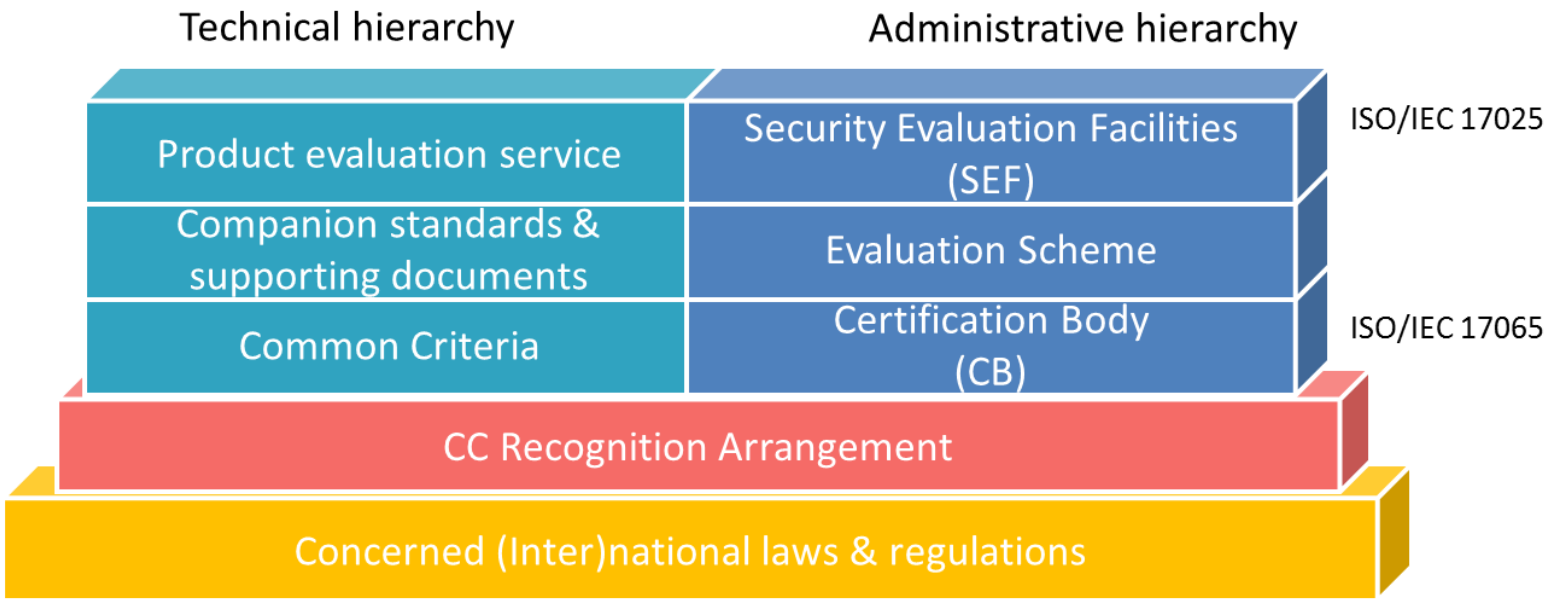
General model of CC evaluation



General model of CC evaluation

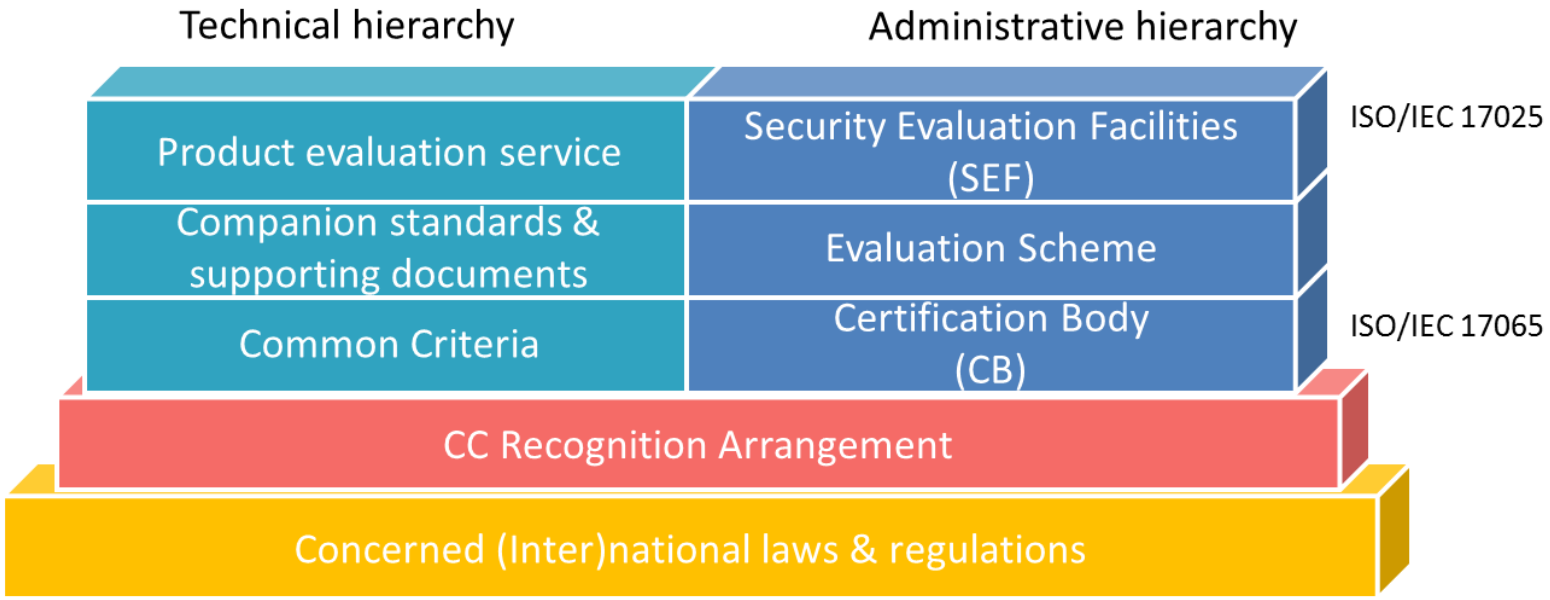


CC application framework



- If to recognize a certificate is not consistent with the applicable laws, acts or regulations, the certificate may be declined to be accepted
- CCRA provides the ground to requires CBs issuing CC certificates should meet high and consistent standards

CC application framework



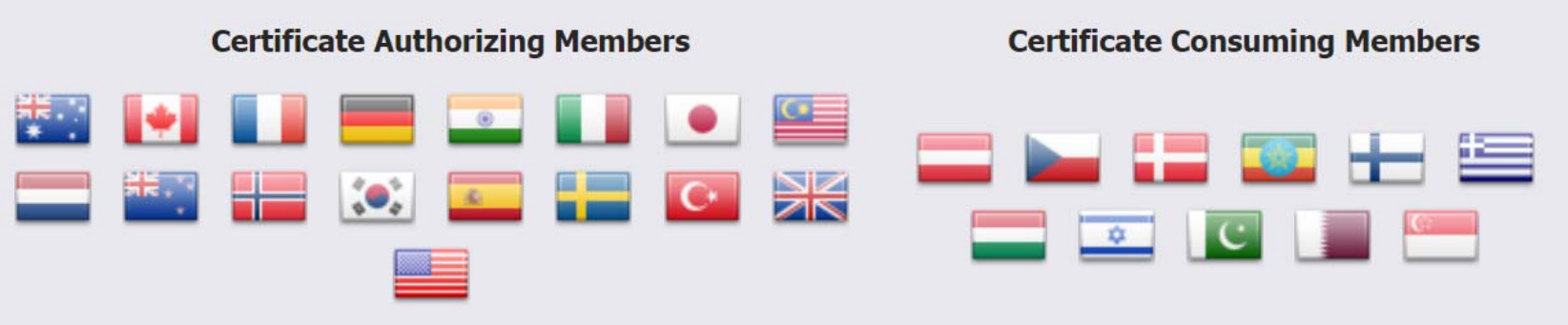
- Scheme managed by CB is to ensure, through the systematic organisation and management of the functions of Evaluation and Certification/Validation, that high standards of competence and impartiality are maintained and that consistency is achieved
- SEFs should be accredited by Accreditation Body and approved by CB, who monitors SEF's evaluation activities such that the certificate can be issued impartially

CC Recognition Arrangement

- Eligibility of participation
  - Participants in this Arrangement are government organizations or government agencies, representing their country or countries
- Participant type
  - Certificate authorizing member
    - Operating in their own country and issue certificates
  - Certificate consuming member
    - Promise to recognize certified IT Products and PPs, but cannot issue
- Membership evolution
  - 1998, 5 countries signed the original CCRA file
  - 2000, 14 countries signed
  - 2018, 28 countries signed the revised CCRA file

CC recognition arrangement

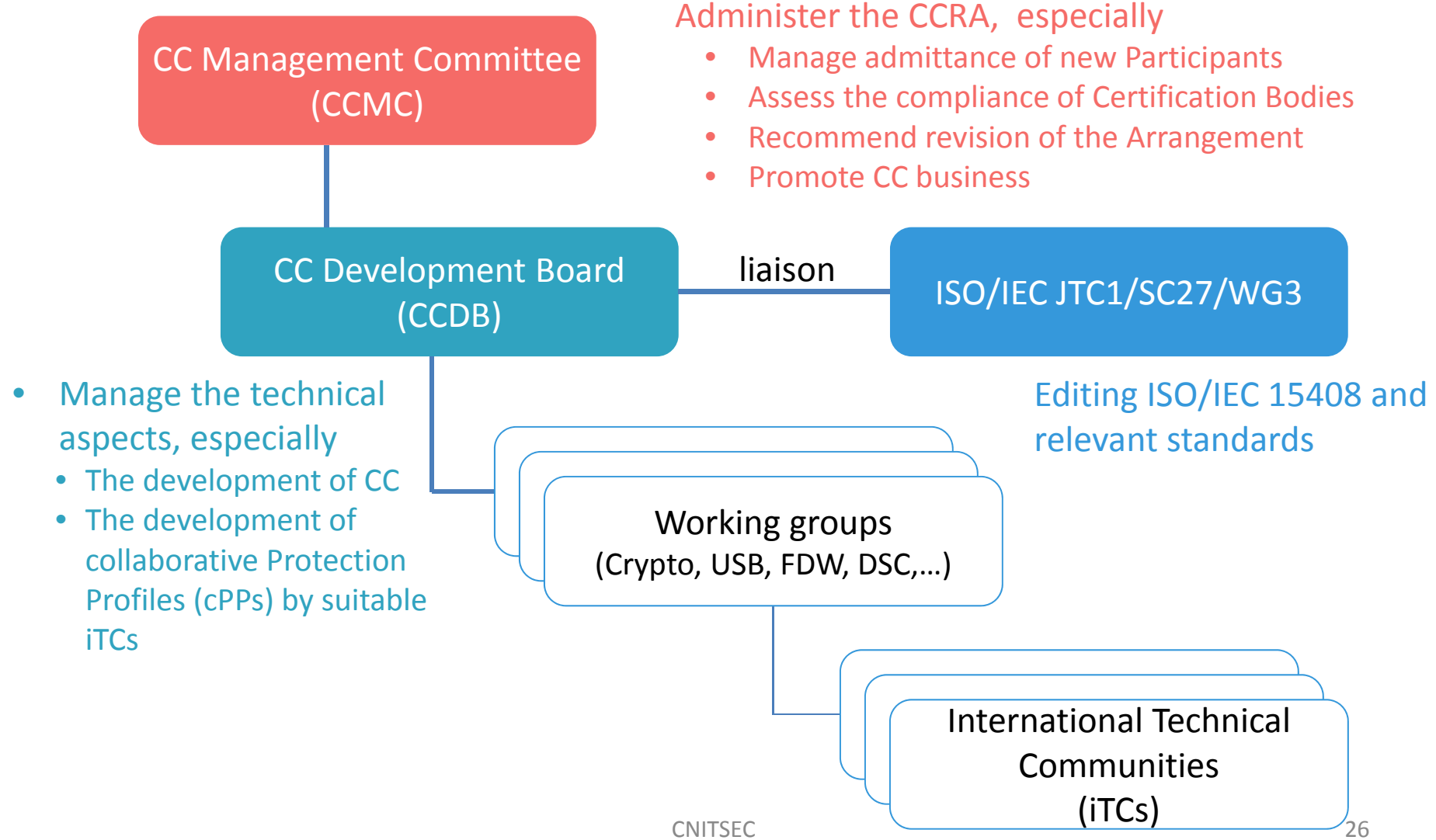
- 28 members of CCRA



Certificate Authorizing members (17)	Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, South Korea, Span, Switzerland, Turkey, UK, US
Certificate Consuming members (11)	Austria, Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Israel, Pakistan, Qatar, Singapore

Data from https://www.commoncriteriaportal.org, 2018.7

Management structure of CC

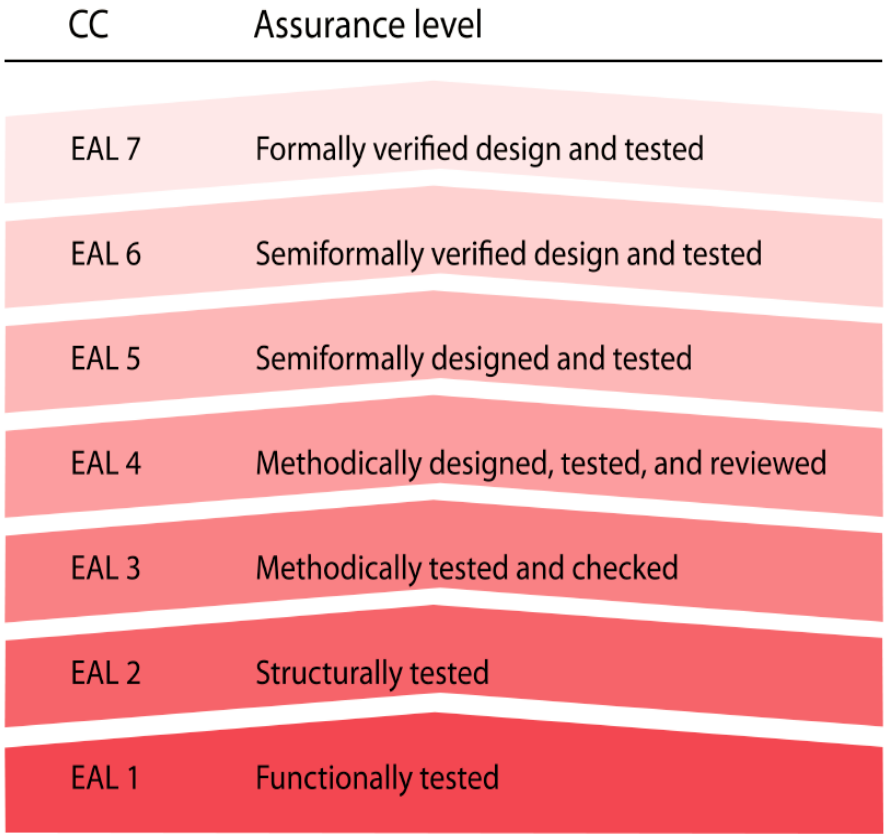


Outline

- Why we need security evaluation?
- What is the Common Criteria?
- How well does it work?
- Is it still in progress?

Hierarchical view of CC evaluation

- 7 Predefined Evaluation Assurance Levels (EALs)



- The increase of users' confidence about the security of the product (the ability that the IT product can resist more complicated attacks)
- The increase of levels increases the evaluation rigor and depth
- Thus, the higher of the level, the higher of the cost

The application of CC

- PP certification

363 Protection Profiles by Category *		
Category	**PPs**	**Archived**
Access Control Devices and Systems	10	7
Biometric Systems and Devices	7	5
Boundary Protection Devices and Systems	38	25
Data Protection	19	4
Databases	10	7
Detection Devices and Systems	17	17
ICs, Smart Cards and Smart Card-Related Devices and Systems	91	20
Key Management Systems	15	11
Mobility	9	5
Multi-Function Devices	5	3
Network and Network-Related Devices and Systems	37	23
Operating Systems	17	15
Other Devices and Systems	67	18
Products for Digital Signatures	21	2
Trusted Computing	10	4
Totals:	**373**	**166**
Grand Total:		**539**

** A Protection Profile may have multiple Categories associated with it.*

Diagram from https://www.commoncriteriaportal.org, 2018.7

The application of CC

- PP certification

Protection Profiles by Scheme and Assurance Level																		
Scheme	**EAL1**	**EAL1+**	**EAL2**	**EAL2+**	**EAL3**	**EAL3+**	**EAL4**	**EAL4+**	**EAL5**	**EAL5+**	**EAL6**	**EAL6+**	**EAL7**	**EAL7+**	**B**	**M**	**S**	**N**	**Total**
Australia	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Canada	0	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	4
Germany	6	0	2	10	3	7	3	62	0	0	0	0	0	0	0	0	0	0	93
Spain	2	0	2	1	2	0	4	0	0	0	0	0	0	0	0	0	0	0	11
France	0	1	0	8	0	11	0	34	1	1	0	0	0	0	0	0	0	6	62
India	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Italy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Japan	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	1	6
Republic of Korea	0	2	0	0	0	0	2	5	0	0	0	0	0	0	0	0	0	0	9
Malaysia	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Netherlands	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	3
Norway	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	0	0	0	3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	4
Turkey	0	0	6	2	0	0	0	3	0	0	0	0	0	0	0	0	0	0	11
United Kingdom	0	0	1	0	5	0	3	3	0	0	0	0	0	0	0	0	0	0	12
United States	18	1	15	21	2	7	2	11	0	0	1	0	0	0	12	26	0	32	148
Totals:	**26**	**5**	**26**	**45**	**14**	**26**	**15**	**125**	**1**	**1**	**1**	**0**	**0**	**0**	**12**	**26**	**0**	**40**	**363**

Diagram from https://www.commoncriteriaportal.org, 2018.7

The application of CC

- Product certification

2378 Certified Products by Category *		
Category	**Products**	**Archived**
Access Control Devices and Systems	68	58
Biometric Systems and Devices	3	0
Boundary Protection Devices and Systems	80	120
Data Protection	69	90
Databases	33	53
Detection Devices and Systems	11	57
ICs, Smart Cards and Smart Card-Related Devices and Systems	1134	25
Key Management Systems	23	27
Mobility	26	18
Multi-Function Devices	185	175
Network and Network-Related Devices and Systems	237	234
Operating Systems	101	74
Other Devices and Systems	277	313
Products for Digital Signatures	99	8
Trusted Computing	32	0
Totals:	**2378**	**1252**
Grand Total:		**3630**

** A Product may have multiple Categories associated with it.*

Diagram from https://www.commoncriteriaportal.org, 2018.7

The application of CC

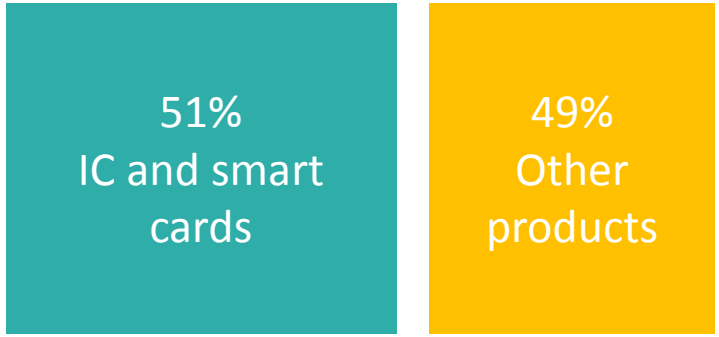
- Product certification

Certified Products by Assurance Level and Certification Date																				
EAL	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**Total**
EAL1	0	0	0	0	0	0	1	1	6	3	1	0	1	10	2	2	3	3	8	1	42
EAL1+	1	0	0	0	0	0	0	0	17	0	2	11	2	0	1	2	1	0	0	1	38
EAL2	0	0	0	0	0	0	1	0	8	1	7	2	3	1	10	12	18	15	22	6	106
EAL2+	0	0	0	1	1	1	2	2	8	8	8	4	5	10	16	27	59	76	66	21	315
EAL3	0	0	0	0	0	0	0	0	10	3	1	9	5	1	9	12	9	2	3	0	64
EAL3+	0	0	0	0	0	2	1	1	37	10	12	11	12	19	12	23	17	19	10	4	190
EAL4	0	1	0	1	0	0	0	0	28	5	9	4	6	2	7	2	0	5	2	5	77
EAL4+	0	1	1	2	2	3	3	2	142	58	67	56	60	87	63	51	58	56	52	15	779
EAL5	0	0	0	0	0	0	0	0	6	3	2	0	1	0	0	0	0	3	1	0	16
EAL5+	0	0	0	0	0	0	3	0	50	27	31	43	35	27	56	53	43	69	65	7	509
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL6+	0	0	0	0	0	0	0	0	0	0	2	3	0	4	6	6	12	8	13	11	65
EAL7	0	0	0	0	0	0	0	0	0	0	1	0	0	0	4	0	0	0	0	0	5
EAL7+	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
Basic	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	8	13	22	78	46	171
Totals:	**1**	**2**	**1**	**4**	**3**	**6**	**11**	**6**	**312**	**118**	**143**	**144**	**130**	**161**	**190**	**198**	**233**	**278**	**320**	**117**	**2378**

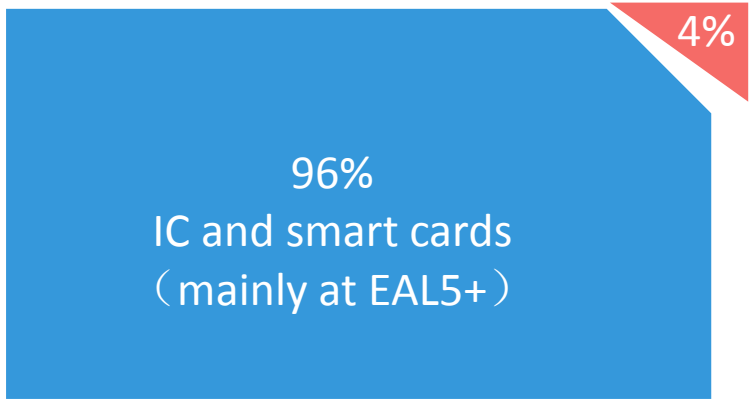
Diagram from https://www.commoncriteriaportal.org, 2018.7

Statistics of product evaluation

EAL4 and above
（over 58%）



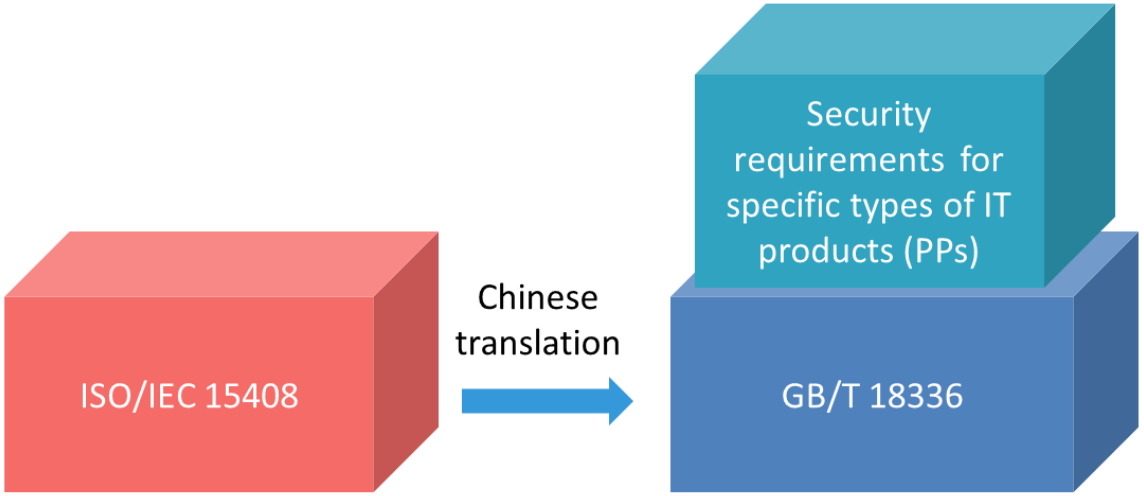
EAL5 and above
（over 30%）



IBM specialized OS,
hardware data diode,
Optical switch
…

CC applications in China

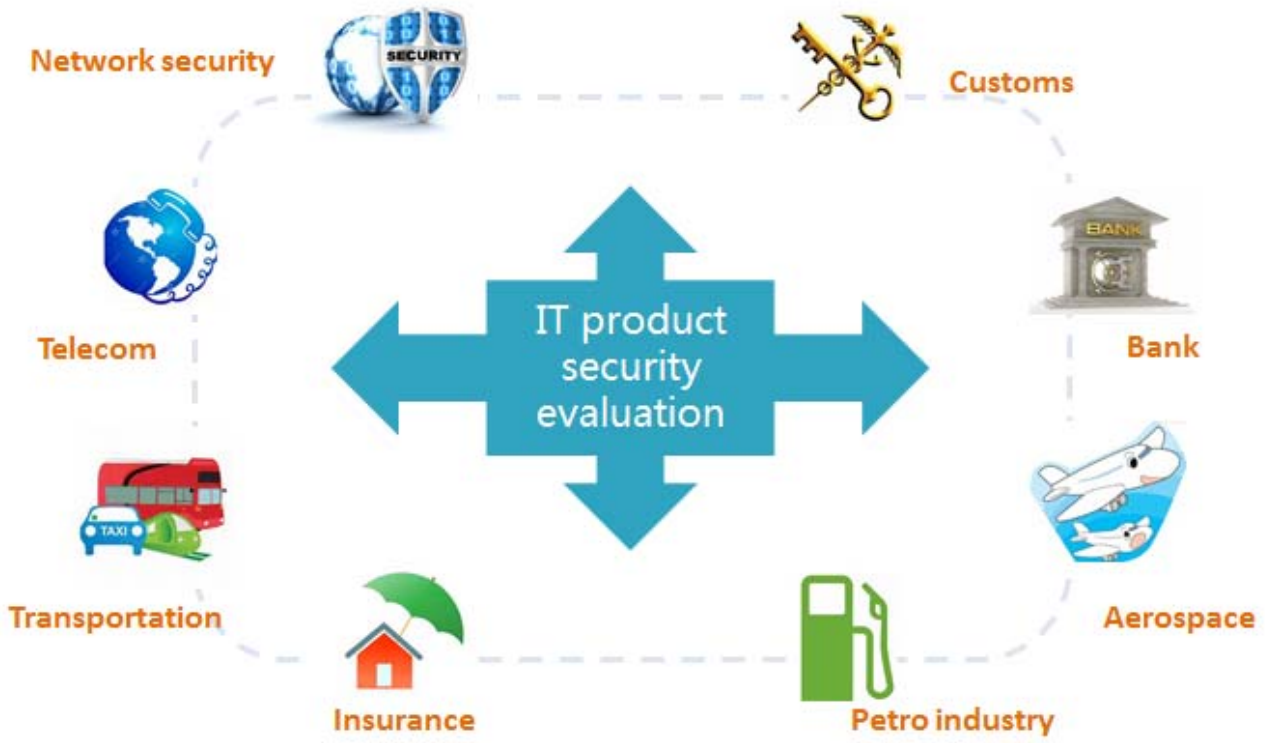
- PPs as national standards
  - 10+ have been published



GB/T 20276: IC embeded software
GB/T 22186: IC chip
GB/T 18018: Router
GB/T 21028: Server

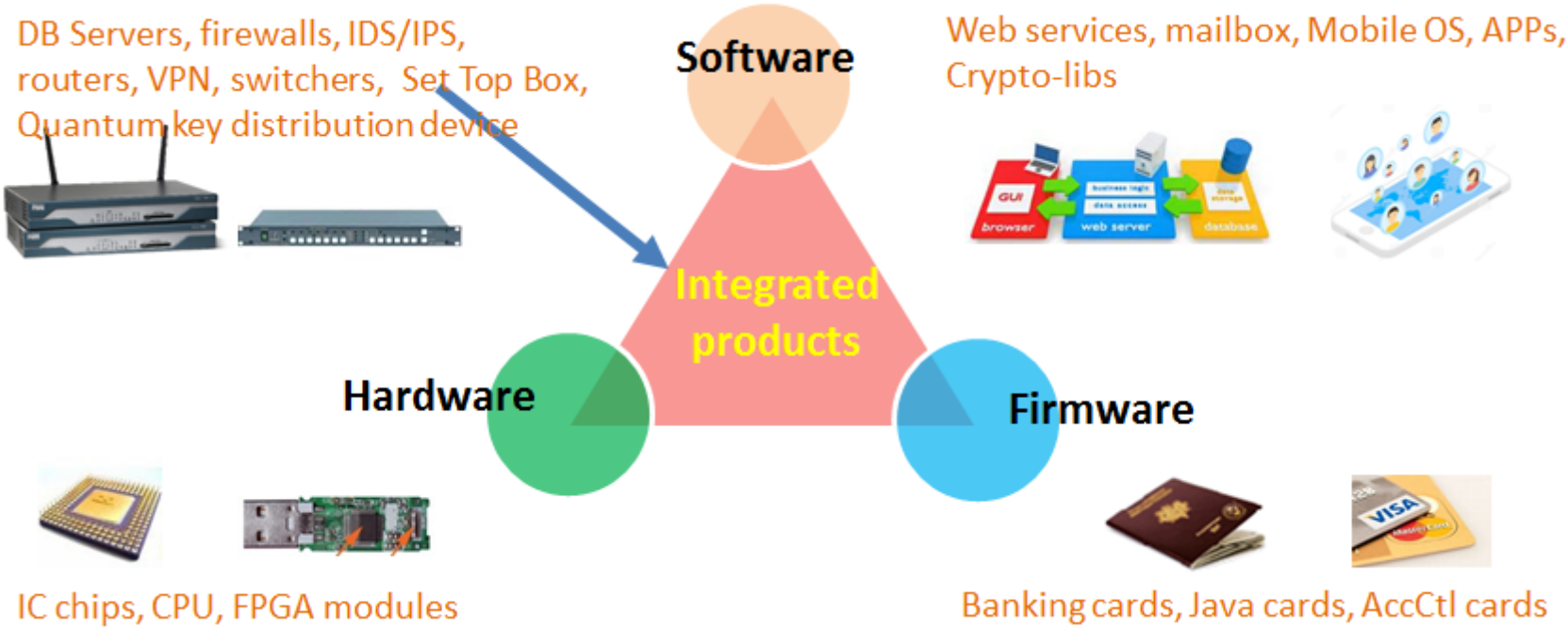
GB/T 21050: Network switcher
GB/T 20279: Network filter
GB/T 33565: Wireless access network
GB/T 33563: Wireless access client

CC applications in China



- During the last 10 years, many governmental departments or industrial sectors, especially those provide fundamental facilities have been involved into CC evaluation business
- CC evaluation is mainly driven by the industry or the users

CC applications in China



- Include a variety of IT products with the forms of hardware, software, firmware as well as their integration
- Since 2001, more than 1500 products have been evaluated in China, mainly at EAL 3 to EAL 5+, including some international vendors' products

Outline

- Why we need security evaluation?
- What is the Common Criteria?
- How well does it work?
- Is it still in progress?

CC is far from perfect

Evaluation is usually a costly process	• An IC hardware evaluation at EAL5+ level may cost more than 1 Million dollars
Evaluation is usually a time-consuming process	• The effort and time necessary to prepare evaluation evidence and other evaluation-related documentation is so cumbersome • An IC hardware evaluation at EAL5+ level may require more than 1 year to finish
Evaluation results may not provide comparable basis for procurement	• Evaluations could be based on different Protection Profiles even for the same type of products • Capability discrepancies among different evaluation facilities are unavoidable thus affects the result
Evaluation may not provide beneficial suggestions to improve design	• For some evaluation schemes, evaluation focuses primarily on assessing the evaluation documentation, not on the actual security, technical correctness or merits of the product itself

The revision of CCRA

- The CCRA in new version was signed in July, 2014
  - Evaluations should be done against cPPs if possible which can be recognized up to EAL 4 (+ ALC_FLR), otherwise mutual recognition would be limited up to EAL2
    - CCMC will endorse suitable iTCs to develop collaborative PPs (cPPs) for each specific technical fields (with the cooperation of users, vendors, SEFs, CBs and any other stakeholders)
    - cPP is a special type of PP, which defines the minimum set of common security functional requirements
    - cPP shall only include assurance components to a maximum of EAL2, except where the iTC can demonstrate a rationale that activities up to and including EAL4 can be reproduced between schemes
  - Approved cPPs are expected to be the basis for producing reasonable, comparable, reproducible and cost-effective evaluation results, and promote fair competition

The revision of CCRA

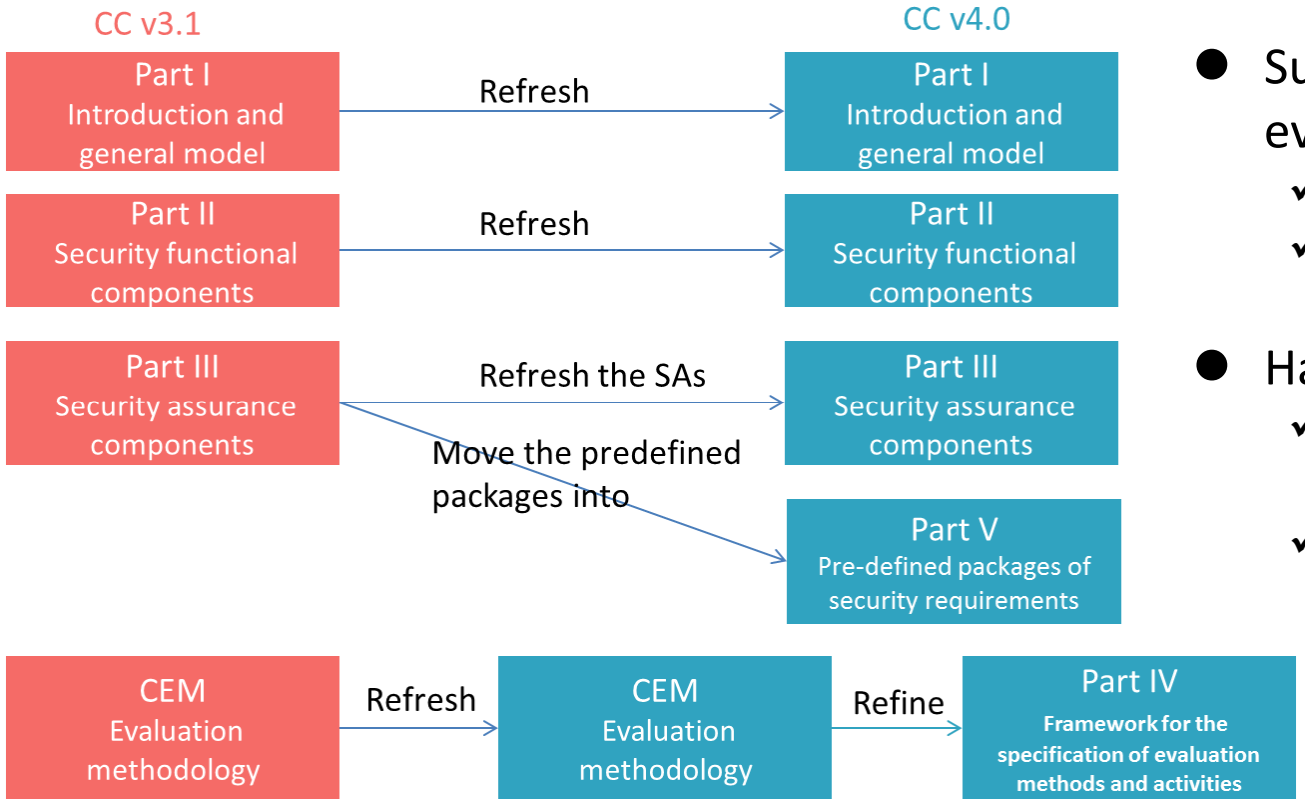
- 6 iTCs have been established

Full Drive Encryption	USB Portable Storage Device	Network Fundamentals and Firewalls
Application Software	Biometric Security	Dedicated Secure Components

- 9 cPPs have been published since then
  - collaborative Protection Profile Module for Full Drive Encryption – Enterprise Management v2.0
  - collaborative Protection Profile for Full Drive Encryption - Encryption Engine v2.0
  - collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition v2.0
  - collaborative Protection Profile for Stateful Traffic Filter Firewalls v2.0 + Errata 20180314
  - collaborative Protection Profile for Network Devices v2.0 + Errata 20180314
  - 4 old versions of those cPPs

The renewal process of CC

- CC has to be revised to support the changes of CCRA



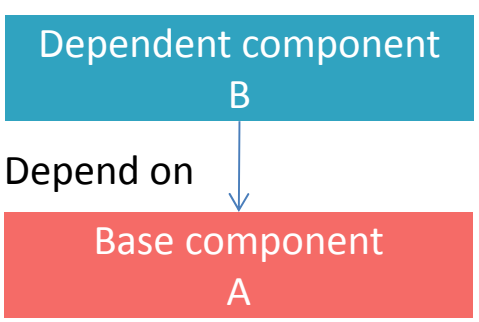
- Support more flexible evaluation methods
  - ✓ Attack-based approach
  - ✓ Requirement-based approach
- Handle complex product
  - ✓ Composite product evaluation
  - ✓ Modular PP

Two kinds of evaluation methods

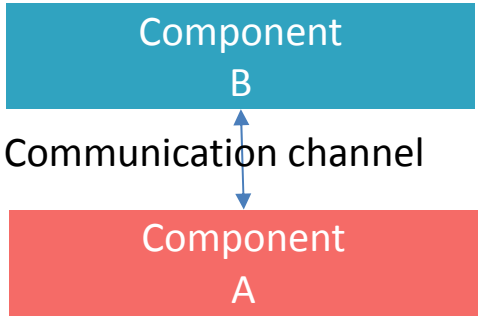
Attack-based approach (traditional investigative approach)	Requirement-based approach (cPP based approach)
The security requirements are not so clear before actual evaluation. This is the common use case for **new technologies**, since they are not so mature and stationary when they emerge.	The expected security requirements are well known before actual evaluation. This is the use case for **common technologies** since they are mature enough after a long time development.
PP may not be necessary for an evaluation. Specific details about the security requirements may not be known in writing PP, so a corresponding ST should refine and specialize the open-ended assignment options.	PP as the requirement specification is necessary for an evaluation. Details about the security requirements and the evaluation activities are well defined in PP, and ST should be in exact conformance with the PP.
Tests are not defined in advance and will depend on the expected EAL scale. The evaluator are allowed to introduce reasoned analysis depend on the TOE for flaw assessment.	Tests are defined exactly in advance, and EALs are not used. The evaluation is to enumerate the already defined tests.
Penetration testing is required, in order to check the attack potential in a real execution circumstance.	Penetration testing is not required, since the security problems are known well before the evaluation, but the PP should be updated frequently to reflect the state-of-the-art.

Handle complex products

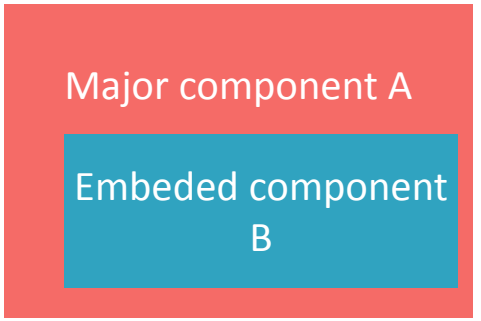
- CC can be used to handle complex system
  - CC is not limited on evaluating simple structured products
- Products composition



OS & Applications



Network systems

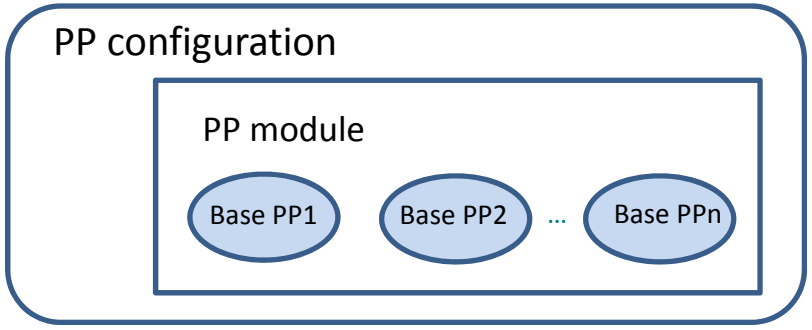


Host+Secure libraries

  - ACO(+CAP) approach
    - only reflects the CAP level, not the EAL scale of the final composition products
  - Composite TOE evaluation
    - Give a verdict on the whole EAL scale of the composite TOE

Handle complex products

- Modularity within a TOE
  - Divide security requirements of complex product into modules, and then combine them to improve reusability of requirement specifications
  - Requirement bundling
    - Bundle dependent SFRs for easy reuse
  - Requirement package
    - Bundle requirements to achieve specific and explicit logical objective
    - Assurance packages (i.e., predefined EALs)
    - Optional functional package to achieve specific security objective
  - Modular PP
    - Base PP
    - PP module
    - PP configuration



- *"The complexity of information systems is such that even the most carefully written security Evaluation criteria and Evaluation methodology cannot cover every eventuality"- from CCRA document*
- *The Common Criteria is not perfect, but on the road to be perfect*

Thank you

中国信息安全测评中心
China Information Technology Security Evaluation Center

1st building, No.8 Yard, Shangdi west road,
Haidian district
Beijing, China
Tel: +86-010-82341110