# CC in China

Zhuohui Liu , CNCA ; Xiaohua Chen , ISCCC

Sept. 23rd, 2008

# Agenda

1. Following updates of CC

2. Translation of CC into Chinese

3. Practice of CC

4. Future of CC in China

# 1. Following updates of CC

# 1. Following updates of CC

- In China, the translation of CC1.0 was started since 1997.
- When CC2.1 became ISO/IEC 15408 in December 1999 , the translation of CC2.1 was combined with the above work.
- China officially issued GB/T 18336 (CC2.1) in 2001 and has been following updates of the CC development.

# 1. Following updates of CC

- The Chinese delegations have attended all ICCCs except for the fifth conference due to visa problems.

- Moreover, the information security evaluation agencies of China have sent delegations to visit the European information security evaluation agencies, such as Atsec, TÜViT, DCSSI, Syntegra, etc. The Chinese agencies also invited experts from CBs in other countries for technical training and communication.

# 1. Following updates of CC

| ICCC no. | Country | Host | Chinese attendance |
|---|---|---|---|
| 1 | US | NIST | √ |
| 2 | UK | CESG | √ |
| 3 | Canada | CSE | √ |
| 4 | Sweden | SWEDAC | √ |
| 5 | German | BSI | × |
| 6 | Japan | IPA | √ |
| 7 | Spain | CCN | √ |
| 8 | Italy | OCSI | √ |
| 9 | Korea | KISA | √ |

# 1. Following updates of CC

- Before July 2008: CNITSEC took charge of the voluntary certification of information security products based on CC.

- Nowadays: ISCCC takes charge of both voluntary and compulsory certification of information security products.

# 1. Following updates of CC - Designated Certification Body

## China Information Security Certification Center (ISCCC)

- According to China's current administrative status and demands, the government designates ISCCC to be responsible for the task of information security products compulsory certification.
- As an impartial and independent third-party CB, ISCCC carries out certification activities and services according to international/domestic standards, certification rules.
- Other certification activities: ISMS, IS Service,etc.

# 1. Following updates of CC - Designated Certification Body

- **Established by Law:**

  **Notification on the establishment of national certification and accreditation system for information security product**

  **(Regulation No.[2004]57, co-signed by 8 ministries)**

# 1. Following updates of CC - Designated Certification Body

## Administration and Coordination Departments:

- Information security products certification and accreditation system is under the unified management, supervision and coordination by CNCA, and is jointly implemented together with the relevant government departments and interest parties.

- Eight government authorities involved: Ministry of Public Security, Ministry of State Security, State Council Informatization Office, Ministry of Information Industry, State Cryptography Administration, National Administration for the Protection of State Secrets, AQSIQ, CNCA .

- National Information Security Products Certification Administration and the Executive Committees: established according to relevant rules, composed of representatives from relevant government departments, manufacturers, users, R&D or standards developers, etc.

# 2. Translation of CC into Chinese

# 2. Translation of CC into Chinese

**GB/T 18336 (Information technology – Security techniques – Evaluation criteria for IT security: Part 1-3) was officially issued in China in 2001, which is identical to ISO/IEC 15408: 1999 (CC 2.1).**

## 2. Translation of CC into Chinese

Additionally, the following standards were developed depending on the PPs issued publicly:

- GB/T 18019-1999 Information technology – Security requirements for packet filter firewalls (ref. Traffic Filter Firewall Protection Profile for Low Risk  Environments V1.0, Dec.1997)
- GB/T 18020-1999 Information technology – Security requirements for application level firewall (ref. Application Level Firewall Protection Profile for Low Risk  Environments V1.0, Dec.1997)

# 2. Translation of CC into Chinese

- GB/T 20276-2006 Information security technology – Security requirements for smartcard embedded software (EAL4+)
  (ref. Smartcard Embedded Software Protection Profile, Registered at the France Certification Body under the number PP/9810; Smart Card Security User Group Smart Card Protection Profile, Version 3.0)

- GB/Z 20283-2006 Guide for the Production of Protection Profile and Security Targets
  (NEQ ISO/IEC TR 15446:2004)

# 2. Translation of CC into Chinese

Depending on ISO/IEC 15408: 2005 (CC 2.3), GB/T 18336 is under revision, and this project was initiated in the national standard development programs of China information security standardization technical committee in 2007.

The project of transforming ISO/IEC 18045: 2005 (Methodology for IT security evaluation, i.e. CEM) into Chinese national standard is to be finished.

# 3. Practice of CC

# 3. Practice of CC – Certification Experience

- Since the publication of GB/T 18336 in 2001, 56 certificates of information security products based on CC have been issued.

- Meanwhile, the national standards, industry standards and laboratory regulations based on CC have also been used, and 639 more certificates (non-CC) have been issued.

- In summary, the CC certificates covered 8% of the information security products in China since 2002.

# 3. Practice of CC – Certification Experience

## Level of the certifications:

- 2 EAL1 certificates;
- 7 EAL2 certificates;
- 22 EAL3 certificates: mainly for firewalls and IDSs;
- 25 EAL4 certificates: mainly for telecommunication mobile smart-cards such as SIM card, UIM card and the related embedded software (COS).

# 3. Practice of CC – related standards developed

## Information security products standards based on CC:

- GB/T 20275-2006 Information security technology – Technical requirements and testing and evaluation methods for intrusion detection system
- GB/T 20278-2006 Information security technology – Technical requirements for network vulnerability scanners
- GB/T 20280-2006 Information security technology – Testing and evaluation methods for network vulnerability scanners
- GB/T 20945-2007 Information security technology – Technical requirements, testing and evaluation methods for information system security audit products
- GB/T 20281-2006 Information security technology – Technical requirements and testing and evaluation methods for firewall products
- Etc.

# 3. Practice of CC – Technical Requirements

## And PPs developed:

- ■ Application-level Firewall Protection Profile for Low Risk Environments (EAL2)
- ■ Application-level Firewall Protection Profile for Middle Risk Environments (EAL3+)
- ■ Application-level Firewall Protection Profile for Middle & High Risk Environments (EAL4)
- ■ Packet filter Firewall Protection Profile for Low Risk Environments (EAL2)
- ■ Packet filter Firewall Protection Profile for Middle Risk Environments (EAL3+)
- ■ Packet filter Protection Profile for Middle & High Risk Environments (EAL4)
- ■ Intrusion Detection System Protection Profile for Low Risk Environments (EAL2)
- ■ Intrusion Detection System Protection Profile for Middle & High Risk Environments (EAL4)

# 3. Practice of CC – Technical Requirements

## And PPs developed (Cont.):

- Certificate Issuing and Management Components Protection Profile
- Controlled Access Control Protection Profile
- Role-Based Access Control Protection Profile
- Security VPN Common Protection Profile
- Security Scanners Protection Profile for Low Risk
- Security Scanners Protection Profile for Middle & High Risk Environments (EAL4)

# 3. Practice of CC – Comments

## Comments on CC:

- ■ The assurance requirements are relatively abstract, poor to read. Most Chinese vendors say it is very hard to understand those assurance requirements.
- ■ It needs 2 to 3 years for an evaluator to understand CC and use it in practice. For instance, there are no operational guidelines for AVA class. When a new technology appears, there may be no proper PPs, no checklists. Henceforth, it would be very hard to analyze the technological implementation and determine the strength of security functions.
- ■ It would be hard to guarantee the compliance of the evaluation results from different labs.

# 4. Future of CC in China

# 4. Future of CC in China

- More technical trainings of evaluators
- Evaluator registration system
- Translating more PPs into Chinese
- Developing more PPs for new TOEs
- Considerations of participating CCRA

# 4. Future of CC in China

**Zhuohui Liu, Vice Administrator**
**Certification and Accreditation Administration of the PRC**
**Mail: liuzh@cnca.gov.cn**
**Http://www.cnca.gov.cn**

**Xiaohua Chen, Vice Director**
**China Information Security Certification Center**
**Mail: chenxh@isccc.gov.cn**
**Http://www.isccc.gov.cn**

Thanks for your attention.

Q's?