



Comparative Study Between the Chinese Standards and the Common Criteria

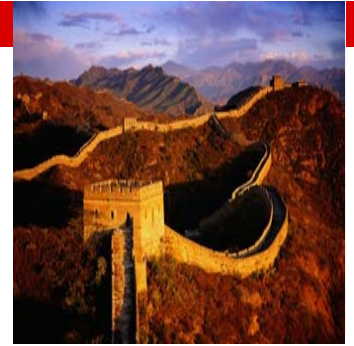
Yi Mao, Xiaohua Chen, and Yan Liu

Agenda



- Basic information security standards in China
- Product-specific standards in the Chinese Compulsory Certification (CCC) System
- Understanding the Chinese GB/T 20272 for a secure OS
- Understanding the Chinese GB/T 20273 for a secure DBMS
- Summary on the differences and connections between PPs under the CC framework and the Chinese standards
- Final Remarks

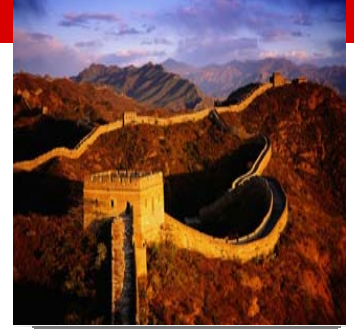
Basic Standards in China



The basic information security standards in China, which all of the product-specific standards rely upon, are:

- GB 17859 -1999, "Classified Criteria for Security Protection of Computer Information System"
- GB/T 20271-2006, "Information Security Technology - Common Security Technology Requirements for Information Systems"
- GB/T 18336.1-2008, GB/T 18336.2-2008, GB/T 18336.3-2008, which are the Chinese translations of CC V2.3 Part 1, Part 2, and Part 3

Chinese National Standard GB 17859-1999

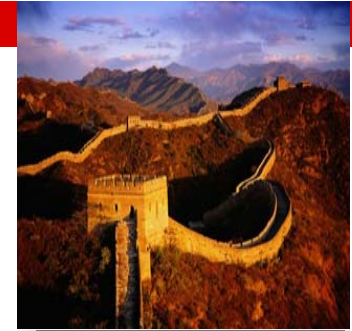


GB 17859 -1999 references:

- the DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)," and
- NCSC-TG-005 which extends the evaluation classes of the TCSEC to include trusted network systems and components.

Both DoD 5200.28-STD and NCSC-TG-005 are U.S. standards.

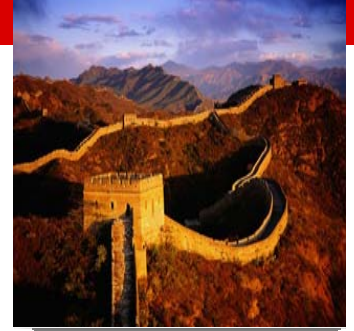
Security Protection Levels Classified in GB17859



GB 17859 -1999 classifies the security protection capability of Computer Information Systems into five levels:

- Level 1 - Discretionary Protection
- Level 2 - System Audit Protection
- Level 3 - Security Flag Protection
- Level 4 - Structure Protection
- Level 5 - Access Verification Protection

Security Functions in GB 17859-1999



GB 17859 -1999 outlines the incremental requirements for each security protection level from security functions in ten aspects:

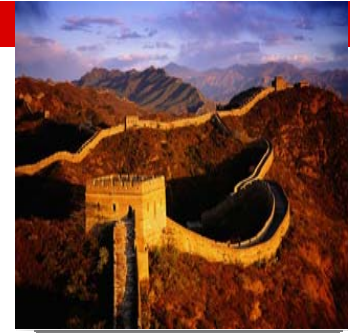
- Discretionary Access Control
- Mandatory Access Control
- Labels
- Identification and Authentication
- Object Reuse
- Audit
- Data Integrity
- Covert Channel
- Trusted Path
- Trusted Recovery

Correspondence of Security Functions and Security Levels in GB 17859-1999



Security Levels Security Functions	Discretionary Protection	System Audit Protection	Security Flag Protection	Structure Protection	Access Verification Protection
Discretionary Access Control	+	++	++	+++	+++
Mandatory Access Control			+	++	+++
Labels			+	++	++
Identification and Authentication	+	++	+++	+++	++++
Object Reuse		+	+	+	+
Audit		+	++	+++	++++
Data Integrity	+	++	+++	+++	++++
Covert Channel				+	+
Trusted Path				+	++
Trusted Recovery					+

Incremental Functional Requirements in GB 17859-1999



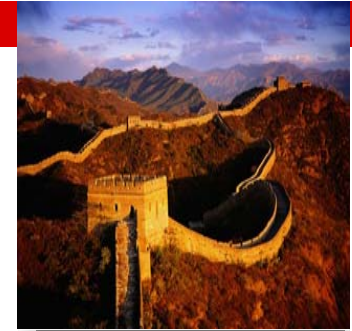
- The requirements for the same security function, for example DAC, are stronger from a lower security level to a higher one.
- The increasing number of "+" symbols in the corresponding table indicates the incremental requirements on the security functions.

Example:

The DAC at level 1 shall allow a user or user group to define and control the shared objects and shall prevent unauthorized read access to sensitive data.

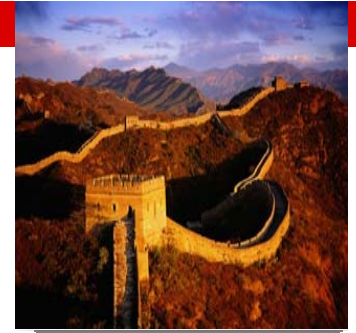
DAC at level 2 is further required to control the distribution of the access right, and to prevent the unauthorized access to objects based on the user defined or default access right. The granularity of the access control is on the individual user.

TCSEC and GB 17859-1999



TCSEC	GB 17859-1999
D — Minimal protection	--
C1 — Discretionary Security Protection	Level 1 - Discretionary Protection
C2 — Controlled Access Protection	Level 2 - System Audit Protection
B1 — Labeled Security Protection	Level 3 - Security Flag Protection
B2 — Structured Protection	Level 4 - Structure Protection
B3 — Security Domains	Level 5 - Access Verification Protection
A1 — Verified Design	--

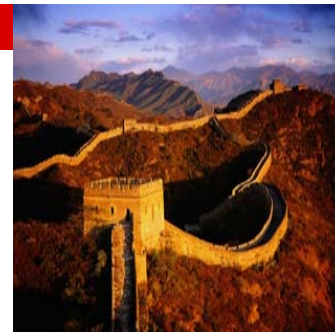
TCSEC and GB 17859-1999 (Continued)



- TCSEC groups its requirements into the following areas:
 - Security Policy
 - Discretionary Access Control, Object Reuse, Labels, Mandatory Access Control
 - Accountability
 - Identification and Authentication, Trusted Path, Audit
 - Assurance
 - Operational Assurance: System Integrity, Covert Channel Analysis, Trusted Recover, Life-Cycle Assurance
 - Documentation

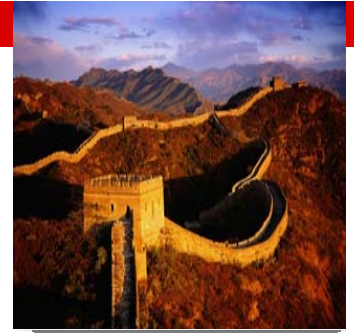
- GB 17859 flattens the internal grouping structure of TCSEC and adopts security function requirements from the various groups.

From GB 17859-1999 to GB/T 20271-2006



- GB/T 20271-2006 details the security functional requirements for each of the five security protection levels defined in GB 17859-1999.
- GB/T 20271-2006 shares a high degree of similarities with CC:
 - Security function technical requirements (chapter 4)
 - Physical Security
 - Operational Security
 - Data Security
 - Security assurance technical requirements (chapter 5)
 - SSOIS (Security Subsystem of Information System) Self-Security Protection
 - SSOIS Design and Implementation
 - SSOIS Security Management
 - Technical requirements for information systems security level classification (chapter 6)

Chapter 4 of GB/T 20271: Security Functional Requirements (1)



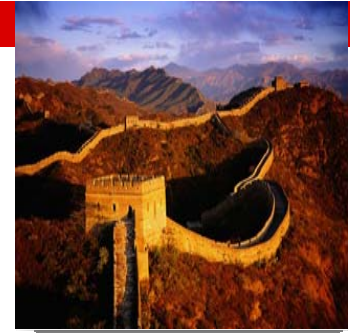
■ Physical Security

- Environment Security (e.g. location, fire hazard, pollution)
- Equipment Security (e.g. tamper-evident label, monitoring system)
- Media Security (e.g. prevention of unauthorized copy/modification/destruction)

Note:

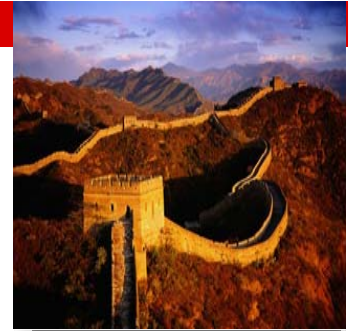
In an ST or PP, under the CC framework, the physical security requirements are often covered by the assumptions for the TOE environment. Comparing with the CC, the physical security requirements in GB/T 20271 are much more detail-oriented.

Chapter 4 of GB/T 20271: Security Functional Requirements (2)



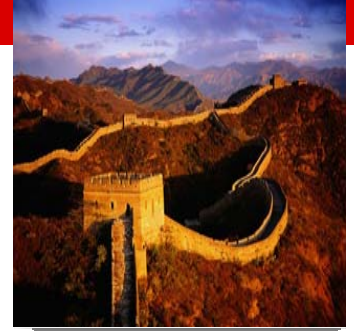
- Operational Security
 - Risk Analysis (natural disaster, human errors, system malfunctions)
 - Information System Security Assessment (OS/DB/Network vulnerability and mitigation)
 - Information System Monitoring
 - Security Audit (details GB 17859 on generation, analysis, selection, storage, etc.)
 - Information System Boundary Protection (external ports/interface)
 - Backup and System Recovery (details GB 17859)
 - Malware Prevention
 - Information System Emergency Handling
 - Trusted Computing and Trusted Connectivity

Chapter 4 of GB/T 20271: Security Functional Requirements (3)



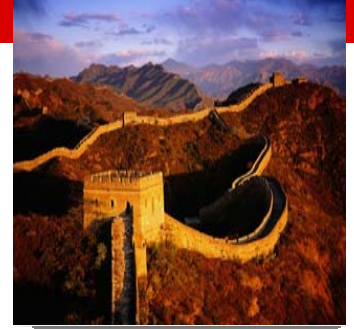
- Data Security
 - Identification and Authentication (class FIA in CC V2.3)
 - Non-repudiation (class FCO in CC V2.3)
 - Discretionary Access Control (FDP_ACC in CC V2.3)
 - Labels (FDP_IFF in CC V2.3)
 - Mandatory Access Control (FDP_ACC in CC V2.3)
 - User Data Integrity (FDP_SDI and FDP_UIT in CC V2.3)
 - User Data Confidentiality, including Object Reuse (FDP_UCT and FDP_RIP in CC V2.3)
 - Data Flow Control (FDP_IFC and FDP_IFF in CC V2.3)
 - Trusted Path (class FTP)
 - Cryptographic Support (class FCS)

Observations on Chapter 4 of GB/T 20271



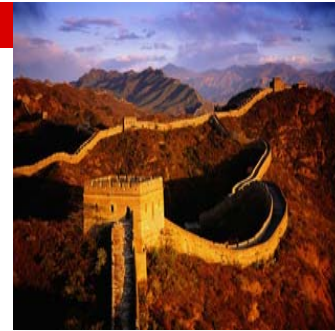
1. The operational and data security functional requirements stated in chapter 4 cover all security functional requirements except for Convert Channel in GB 17859. Convert Channel is discussed in chapter 5.
2. Chapter 4 provides much more detailed requirements for each security function that is identified in GB 17859.
3. Going beyond what's required in GB 17859, chapter 4 defines and discusses more types of security functions (e.g. Cryptographic support)
4. The detailed functional requirements in chapter 4 are largely adopted from CC V2.3. This is especially true for the data security requirements.
5. The role that chapter 4 of GB/T 20271 plays in Chinese standards is similar to Part 2 in the CC world.

Chapter 5 of GB/T 20271: Security Assurance Requirements (1)



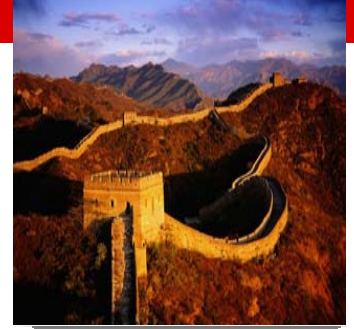
- SSOIS Self-Security Protection
 - SSF (SSOIS Security Function)
 - Detection of physical attack (FPT_PHP.1 in CC V2.3)
 - Notification of physical attack (FPT_PHP.2 in CC V2.3)
 - Resistance to physical attack (FPT_PHP.3 in CC V2.3)
 - SSF Operational Security Protection
 - Underlying abstract machine test (FPT_AMT in CC V2.3)
 - Fail secure (FPT_FLS in CC V2.3)
 - Replay detection (FPT_RPL in CC V2.3)
 - Reference mediation (FPT_RVM in CC V2.3)
 - Domain separation (FPT_SEP in CC V2.3)
 - State synchronization protocol (FPT_SSP in CC V2.3)
 - Reliable time stamp (FPT_STM in CC V2.3)
 - Trusted recovery (FPT_RCV in CC V2.3)
 - Self test (FPT_TST in CC V2.3)

Chapter 5 of GB/T 20271: Security Assurance Requirements (2)



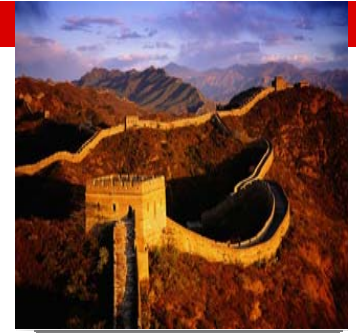
- SSF Data Security Protection
 - Availability of exported SSF data (FPT_ITA in CC V2.3)
 - Confidentiality of exported SSF data (FPT_ITC in CC V2.3)
 - Integrity of exported SSF data (FPT_ITI in CC V2.3)
 - Internal SSOIS SSF data transfer (FPT_ITT in CC V2.3)
 - Inter-SSF SSF data consistency (FPT_TDC in CC V2.3)
 - Internal SSOIS SSF data replication consistency (FPT_TRC in CC V2.3)
 - Trusted path between user and SSF (FTP_TRP in CC V2.3)
 - Inter-SSF trusted channel (FTP_ITC in CC V2.3)
- SSOIS Resource Utilization
 - Fault tolerance (FRU_FLT V2.3)
 - Priority of service (FRU_PRS V2.3)
 - Resource allocation (FRU_RSA V2.3)

Chapter 5 of GB/T 20271: Security Assurance Requirements (3)



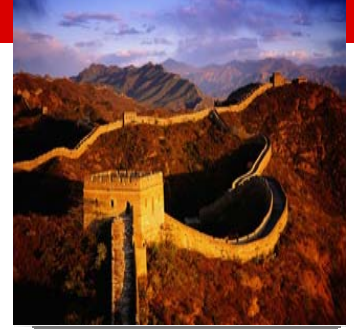
- SSOIS Access Control
 - SSOIS session establishment (FTA_TSE in CC V2.3)
 - Limitation on scope of selectable attributes (FTA_LSA in CC V2.3)
 - Limitation on multiple concurrent sessions (FTA_MCS in CC V2.3)
 - SSOIS access history (FTA_TAH in CC V2.3)
 - Session locking (FTA_SSL in CC V2.3)
- SSOIS design and Implementation
 - Configuration management (class ACM in CC V2.3)
 - Delivery and operation (class ADO in CC V2.3)
 - Development (class ADV in CC V2.3)
 - Documentation requirements (class AGD in CC V2.3)
 - Life cycle support (class ALC in CC V2.3)
 - Tests (class ATE in CC V2.3)
 - Vulnerability assessment (class AVA in CC V2.3)

Chapter 5 of GB/T 20271: Security Assurance Requirements (4)



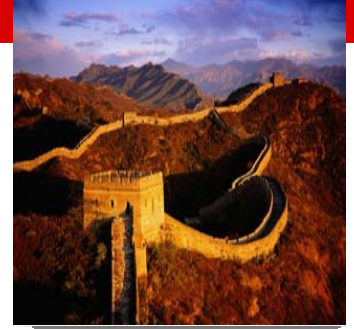
- SSOIS Security Management (class FMT in CC V2.3)
 - Management of functions in SSF (FMT_MOF)
 - Management of security attributes (FMT_MSA)
 - Management of SSF data (FMT_MTD)
 - Definition and management of security roles (FMT_SMR)
 - Centralized management of SSOIS security mechanism (sort of FMT_SMF)

Observations on Chapter 5 of GB/T 20271



1. SSOIS and SSF are the equivalents of TOE and TSF in CC terminology.
2. Some of the security assurance requirements in chapter 5 can be mapped to the security functional requirements from CC V2.3 Part 2.
3. Some of the security assurance requirements in chapter 5 can be mapped to the security assurance requirements from CC V2.3 Part 3.
4. CC V2.3 Part 2 and Part 3 cover all requirements given in chapter 5.
5. CC has evolved from V2.3 to V3.1. The Chinese translation of CC V3.1 will be published in 2013. GB/T 20271 is currently based on CC V2.3. Migrating GB/T 20271 to adopt CC V3.1 will be quite a task.

Chapter 6 of GB/T 20271: Technical Requirements for Information System Security Classification (1)



1. Discretionary Protection Level

- Physical Security ([chapter 4](#), e.g. reference to 4.1.1.1, 4.1.2, 4.1.3)
- Operational Security ([chapter 4](#), e.g. reference to 4.2.1-2, 4.2.5-8)
- Data Security (from [chapter 4](#), e.g. reference to 4.3.1.1-3, 4.3.1.2, 4.3.3, 4.3.6, 4.3.10)
- SSOIS self security protection ([chapter 5](#), e.g. reference to 5.1.1.1, 5.1.2.1-2,7,9, 5.1.3.4, 5.1.4.1-3, 5.1.5)
- SSOIS design and implementation ([chapter 5](#), e.g. 5.2.1.1, 5.2.2.1-2, 5.2.3.1,3-7, 5.2.4, 5.2.5.3, 5.2.6.3-4)
- SSOIS security management ([chapter 5](#), e.g. reference to 5.3.1)

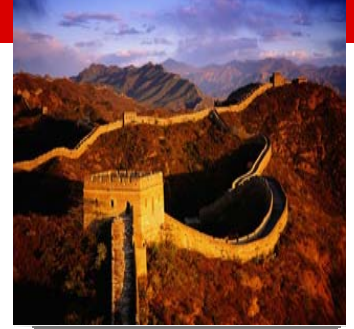
2. System Audit Protection Level

3. Security Flag Protection Level

4. Structure Protection Level

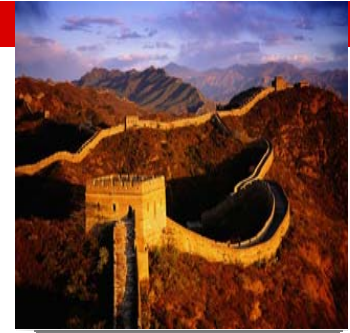
5. Access Verification Protection Level

Chapter 6 of GB/T 20271: Technical Requirements for Information System Security Classification (2)



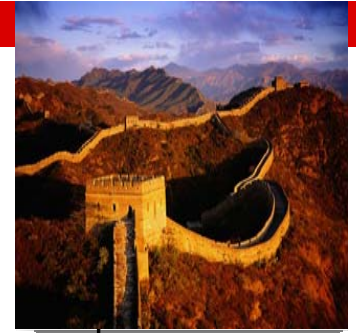
2. System Audit Protection Level

- Physical Security ([chapter 4](#), e.g. reference to 4.1.1.1-[9](#), [4.1.1.2](#), 4.1.2, 4.1.3)
- Operational Security ([chapter 4](#), e.g. reference to 4.2.1-2, [4.2.4.1-6](#), 4.2.5-8)
- Data Security ([chapter 4](#), e.g. reference to 4.3.1.1-3, 4.3.1.2, 4.3.3, 4.3.6, [4.3.7](#), 4.3.10)
- SSOIS self security protection ([chapter 5](#), e.g. reference to 5.1.1.1, 5.1.2.1-2,7,9, 5.1.3.4, [5.1.3.6](#), 5.1.4.1-3, 5.1.5)
- SSOIS design and implementation ([chapter 5](#), e.g. 5.2.1.1, [5.2.1.3](#), 5.2.2.1-2, 5.2.3.1,[2-7](#), 5.2.4, 5.2.5.[1,3-4](#), 5.2.6.[1,2,3-4](#), [5.2.7](#))
- SSOIS security management ([chapter 5](#), e.g. reference to 5.3.1, [2,3](#))



Observations on Chapter 6 of GB/T 20271 (1)

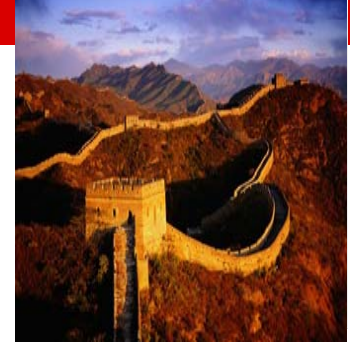
1. Chapter 6 selectively bundles security functional requirements from chapter 4 and security assurance requirements from chapter 5 and then defines an overall set of requirements for each security level as outlined in GB 17859-1999.
2. Compared to GB 17859-1999, chapter 6 provides much more detailed requirements for each of the five classified security protection levels.



Observations on Chapter 6 of GB/T 20271 (2)

3. Unlike the EALs defined in CC Part 3, the security levels elaborated on in chapter 6 include both security functional and assurance requirements.
4. Unlike CC which uses acronyms like FDP and ALC and a four-layer structure of class-family-component-element to organize the requirements, chapter 6 references to section/subsection numbers in chapters 4 and 5 for requirements. It reduces the readability.
5. Unlike CC, which defines the dependent and hierarchical relationship among requirements, chapter 6 highlights the incremental requirements in bold to indicate the stronger requirements from a lower security level to a higher one.

A Summary of GB/T 20271



Chapter 6 Security Classification

Access Verification Protection

Structure Protection

Security Flag Protection

Audit Protection

Discretionary Protection

Physical Security

Operational Security

Data Security

Chapter 4 Functional Requirement

SSOIS self Protection

SSOIS Design and Implementation

SSOIS Security Management

Chapter 5 Assurance Requirement





IT Security Product Certification in China – Compulsory and Voluntary

Compulsory Certification



- CC-IS is the Compulsory Certification scheme for Information Security products based on the Chinese national standards. The certification is compulsory for government procurement, and is voluntary in all other areas. There have been 167 certificates issued as of January 2011.



Voluntary Certification

- The Voluntary IT security certification program covers all types of IT products.
- The ISCCC certification is based on GB/T 18336 (the Chinese translation of CC V2.3). There have been 31 certificates issued as of January 2011.

The Product Categories and Types subject to Compulsory Certification



Product Category	Specific Product Types
Border Security	(1) firewalls (2) network security separation cards and line selectors (3) security isolation and information exchange products
Communication Security	(4) secure routers
Authentication and Access Control	(5) smart card chip operating systems
Data Security	(6) data backup and recovery products (7) secure operating systems (8) secure database systems
Content Security	(9) anti-spam products
Valuation, Audit, and Control	(10) intrusion detection systems (11) network vulnerability scanning products (12) security audit products
Application Security	(13) website recovery products



Applicable Chinese Standards for CC-IS (1)

No.	Product Name	Applicable Standard
1	Firewall	GB/T 20281-2006 Information security technology - Technique requirements and testing and evaluation approaches for firewall products
2	Network secure separation card and line selector	GB/T 20279-2006 Information security technology - Security techniques, requirements of separation between components of network and terminal equipment
3	Secure separation and information exchange products	GB/T 20279-2006 Information security technology - Security techniques, requirements of separation between components of network and terminal equipment
4	Secure router	GB/T 18018-2007 Information security technology - Security requirements for router

Applicable Chinese Standards for CC-IS (2)



No.	Product Name	Applicable Standard
5	Smartcard chip	Operating System GB/T 20276-2006 Information security technology- Security requirements for smartcard embedded software(EAL4+)
6	Data backup and recovery products	CNCA/CTS 0051-2007 Technical specifications for data backup and recovery products
7	Secure Operating System	GB/T 20272-2006 Information security technology - Security technique requirements for operating system
8	Secure Database System	GB/T 20273-2006 Information security technology - Security technique requirements for database management system
9	Anti-spam products	CNCA/CTS 0031-2008 Technical specifications for anti-spam product certification

Chinese Standards applied for CC-IS (3)



No.	Product Name	Applicable Standard
10	Intrusion Detection System	GB/T 20275-2006 Information security technology-Technical requirements and testing and evaluation approaches for intrusion detection system
11	Network Vulnerability Scanners	GB/T 20280-2006 Information security technology - Testing and evaluation approaches for network vulnerability scanners GB/T 20278-2006 Information security technology - Technical requirements for network vulnerability scanners
12	Security Audit products	GB/T 20945-2007 Information security technology - Technical requirements, testing and evaluation approaches for information system security audit products
13	Website recovery products	CNCA/CTS 0050-2007 Technical specifications for website recovery product certification

Comparable Standards on Operating System



- The Operating System Protection Profile by German BSI
 - BSI-CC-PP-0067, version 2.0
 - http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf

- The Operating System Protection Profile by the U.S.
 - U.S. GOVERNMENT PROTECTION PROFILE FOR GENERAL-PURPOSE OPERATING SYSTEMS IN A NETWORKED ENVIRONMENT (V1.0)
 - http://www.niap-ccevs.org/pp/pp_os_br_v1.0/

- The Chinese Standard for Secure Operating System
 - GB/T 20272-2006 Information security technology - Security techniques requirement for operating system
 - <http://www.isccc.gov.cn/zxyw/cprz/gjxxaqcprz/rzfw/11/341638.shtml>

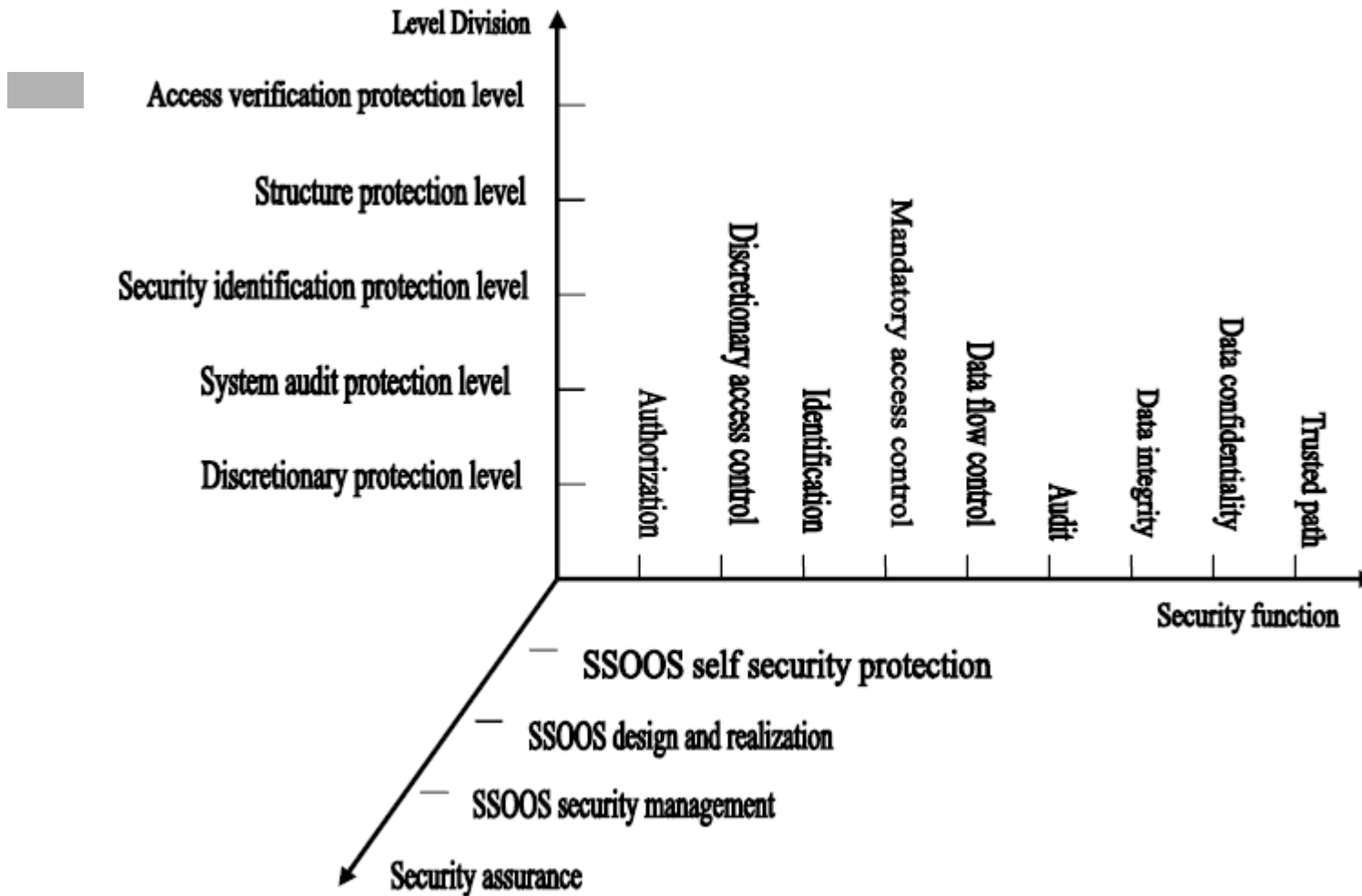
Comparable Standards on Database Management System



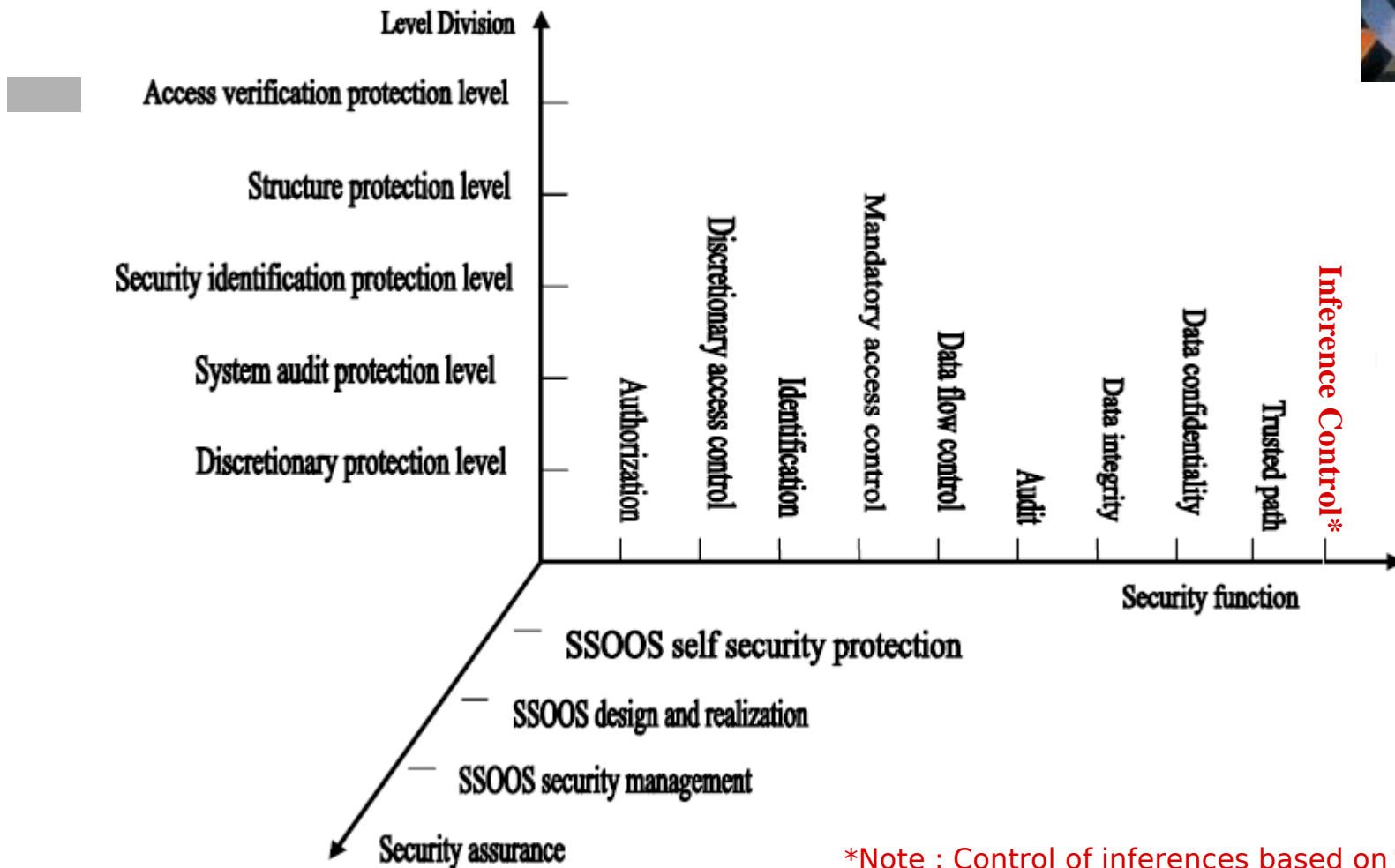
- The DBMS Protection Profile by the U.S.
 - U.S. Government Protection Profile for Database Management Systems (Version 1.3)
http://www.niap-ccevs.org/pp/pp_dbms_v1.3/

- The Chinese Standard for Secure Database System
 - GB/T 20273-2006 Information Security Technology - Security Technology Requirement for Database Management System
<http://www.isccc.gov.cn/zxyw/cprz/gjxxaqcprz/rzfw/11/341637.shtml>

Structural Diagram of Chinese Secure OS Standard



Structural Diagram of Chinese Secure DBMS Standard



*Note : Control of inferences based on aggregated statistic data

Observations of Chinese Product-Oriented Standards



- At first glance, the Chinese standards appear very different from the CC and its related PPs, that one may conclude that they are nothing alike.
- However, if one looks deeper into the Chinese standards, it's easy to recognize that most of the basis for the Chinese standards is actually adopted from CC, such as:
 - Functional components from FIA, FAU, FDP, FPT, FTA, FMT, and FRU classes
 - Assurance components from ADV, AGD, ALC, ATE, and AVA classes
- The differences are mainly at the layer of presentation, packaging, and formality, as outlined in the following page.

Difference in Presentation (1)



- The Chinese standards are presented from the perspective of building a Security Subsystem of an Information System (SSOIS) which is the Trusted Computing Base (TCB) of an information system.
- The CC and its companion CEM are viewed as the rule set for product evaluation. At its core is the notion of a Target of Evaluation (TOE), and the CC draws a boundary around it and differentiates the TOE from its environment.

Difference in Presentation (2)



- GB/T 20271 spells out the requirements for physical and operational security as an integral part of building up an SSOIS.
- The CC threat model starts from what attacks may occur once the system is in use.
- Similarly, Appendix B of GB/T 20271 also recommends assessing the risks involved to determine an appropriate security level for an SSOIS. The risk assessment is tied to the value of the information that may be stored, processed, or transmitted by the SSOIS.

Difference in Packaging Strategy



- Chinese standards and the CC use different packaging structures:
 - The Chinese standards package both security functional requirements and security assurance requirements into a particular security level.
 - The CC only has fixed packages of security assurance requirements known as EALs. However, security functional requirements can be packaged into a Protection Profile for a certain product type, such as an OS and DBSM, in conjunction with a conforming EAL.
- The CC framework is flexible enough to accommodate the Chinese packaging structure if needed, but the reverse will not work.

Difference in Formality (1)



- The CC uses a formal structure in Part 2 and Part 3 to specify SFRs and SARs. The requirements are organized into a hierarchy of classes, families, components, and elements. The requirements are subject to operations such as selection, assignment, refinement, and iteration to make the general requirements specifically tailored to a certain type of (or, specific) product.

Difference in Formality (2)



- GB/T 20271 includes the ideas of specifying security functional requirements as well as security assurance requirements like the CC, but leaves out all formality. Instead of using acronyms like FIA, FAU, and FDP etc., section numbers are used as cross-referencing labels. For example, section 4.1.1.2 in GB/T 20272-2006 refers to section 6.1.3.2 in GB/T 20271-2006, which renders it non-apparent that this functional requirement is about Discretionary Access Control.

Difference in Formality (3)



- While GB/T 20272 extensively references the corresponding sections in GB/T 20271, requirements in GB/T 20271 often get refined by those in GB/T 20272 or more details are added especially for Security Subsystems of Operating System (SSOOS).
- Unlike the relationship between PPs (e.g. OSPP) and the CC which is apparent via assignment/selection/refinement/iteration operations, the changes made between these two mentioned Chinese standards are not traced.

Final Remarks



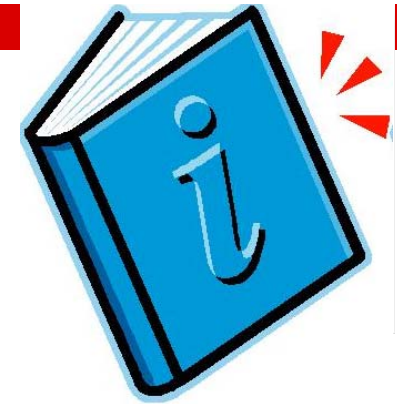
- The fact that Chinese standards use a large majority of the same requirements as the CC proves that the CC is not only valuable for the security evaluation of an information system or product, but equally valuable for the establishing and evaluating the structure of a secure information system.
- On the other hand, the Chinese standards have elaborated on some physical and operational requirements that are not found in the CC, but would make positive contributions to the CC community if they were reconstructed as extended classes for functional or assurance requirements.

References



- ISO/IEC 15408
- ISO/IEC 18045
- GB/T 18336
- GB 17859 - 1999
- GB/T 20271 - 2006
- GB/T 20272 - 2006
- GB/T 20273 - 2006
- BSI-CC-PP-0067, Operating System Protection Profile, version 2.0
- U.S. GOVERNMENT PROTECTION PROFILE FOR GENERAL-PURPOSE OPERATING SYSTEMS IN A NETWORKED ENVIRONMENT V1.0
- U.S. Government Protection Profile for Database Management Systems V1.3

Contact Information



Yi Mao, Ph.D., CISSP, PCI QSA
Principal Consultant
atsec information security corporation
yi@atsec.com

Xiaohua Chen, Ph.D.
Vice Director
China Information Security Certification Center
chenxh@isccc.gov.cn

Yan Liu, CISSP, PCI QSA, PA QSA
Managing Director
atsec China
yan@atsec.com



Thank you for
your attention!