

## Trusted Computing Activities in China

Prof. Sihan Qing  
Institute of Software  
Chinese Academy of Sciences



2008-8-14

Sihan Qing, Malaysia

1/99

## Agenda

- Part 1 – An overview of China's basic policy for information security assurance
- Part 2 – China's contribution to the development of information security standards
- Part 3 – Trusted Computing Activities in China
- Part 4 – Some important technical issues

2008-8-14

Sihan Qing, Malaysia

2/99

## Part 1

An overview of China's basic policy  
for information security assurance

2008-8-14

Sihan Qing, Malaysia

3/99

## Policy and Coordinator

- On June 2003, State Informatization Leadership Group reviewed and passed "the comments regarding the strengthening of information security assurance" at the group's third meeting
- The National Network and Information Security Coordination Team is responsible for the comprehensive coordination works of national information security assurance

2008-8-14

Sihan Qing, Malaysia

4/99

## Key Contents of the Information Security Assurance System

1. Strategic guidelines and objectives of the national information security assurance
2. Short-term strategic objectives
3. Basic principles of the strengthening of information security assurance
4. Primary tasks of the information security assurance

2008-8-14

Sihan Qing, Malaysia

5/99

## Strategic Guidelines of National Information Security Assurance

- Proactive Defense
- Comprehensive Precaution

2008-8-14

Sihan Qing, Malaysia

6/99

### Strategic Objectives

- Overall improvement of the defense capability for information security
- Focus on assurance of infrastructural information networks and critical information systems
- Establishment of safe and healthy network environment
- Assurance and promotion of informatization development, protection of public interests and maintenance of state security

2008-8-14      Sihan Qing, Malaysia      7/99

### Focuses of National Information Security Assurance

- Ensure the security of infrastructural information networks
  - Public telecommunication network, broadcasting and TV network, Internet
- Ensure the security of critical information systems of
  - Taxation, customs, bank, securities, electricity, civil aviation, railway, etc.

2008-8-14      Sihan Qing, Malaysia      8/99

### The Basic Principles

- Based on China's situation, management and technology be given equal weight
- Dealing correctly with the relation between security and development. Development based on security, and security amid development
- Strengthening the basic works of information security with comprehensive planning and distinguished focuses
- Defining responsibilities and obligations of the country, the enterprises and the individuals. All levels of the whole society be given full play to their roles to jointly construct the national information security assurance system

2008-8-14      Sihan Qing, Malaysia      9/99

### Primary Tasks for Information Security Assurance

- Construction and perfection of information security accountability system
- Basic works of the information security assurance
- Supporting works of the information security assurance

2008-8-14      Sihan Qing, Malaysia      10/99

### Primary Tasks for Information Security Assurance-Basic works

- Implementing the grading protection of information security and paying attention to the assessments of information security risks
- Construction of network trust system
- Construction of network security surveillance system
- Emergency response works for information security

2008-8-14      Sihan Qing, Malaysia      11/99

### Primary Tasks for Information Security Assurance-Supporting works

- Strengthen the research and development on information security technology, and promote the development of information security industry
- Strengthen legislations and standards formulations for information security
- Speed up the personnel training for information security, and strengthen citizens' awareness of information security
- Guarantee the funding for information security

2008-8-14      Sihan Qing, Malaysia      12/99

**National Notification Center for Network and Information Security (NOCNIS)**

- NOCNIS is responsible for aggregation, analysis, assessment, notification and early warning of information security related information across China

2008-8-14      Sihan Qing, Malaysia      13/99

**Strengthen Standardization Constructions**

- China Information Security Technology Committee was founded in 2002
- Strengthen the standardization works of information security
- Form the standard system that links with international standards, but entails China's characteristics
- Attach importance to promotion and application works for standards

2008-8-14      Sihan Qing, Malaysia      14/99

**Part 2**  
**China's contribution to the development of information security standards**

2008-8-14      Sihan Qing, Malaysia      15/99

The Data Encryption Standardization Sub-committee was established in July 1984, and recognized as the Information Security Technology Sub-committee under China Information Technical Standardization Committee in August of 1997.

2008-8-14      Sihan Qing, Malaysia      16/99

By the end of 2001, 42 national information security standards were promulgated, 36 among them adopted ISO counterparts and the rest 6 were military standards.

2008-8-14      Sihan Qing, Malaysia      17/99

In order to further advance the information security standardization, China Information Security Standardization Technical Committee (TC260 in short) was established in April 2002 with the approval of China Standardization Administration.

2008-8-14      Sihan Qing, Malaysia      18/99

- Its mission is to edit, evaluate and approve national information security standards.
- It has several working groups including cryptography, PKI/PMI, access control, information security assessment, information security management, trusted computing, biostatistics identification, etc.

2008-8-14

Sihan Qing, Malaysia

19/99

TC260 has established the following working principle: **openness, justice and fairness**, and has adopted the rule of **majority decision**.

2008-8-14

Sihan Qing, Malaysia

20/99

Since its establishment, TC260 has participated in the ISO conferences actively, voted and commented the suggestions regularly representing China.

2008-8-14

Sihan Qing, Malaysia

21/99

TC260 has successfully organized the International Trusted Computing Seminar jointly with TCG, and the International Information Security Management Standardization Seminar jointly with ISO/IEC JTC1/SC27/WG1.

2008-8-14

Sihan Qing, Malaysia

22/99

So far 69 national information security standards have been promulgated by the TC260.

2008-8-14

Sihan Qing, Malaysia

23/99

TC260 was rewarded as “National first-rank Standardization Technical Committee” in 2003 by China Standardization Administration for its proper coordination, effective working mechanism, and remarkable working effect.

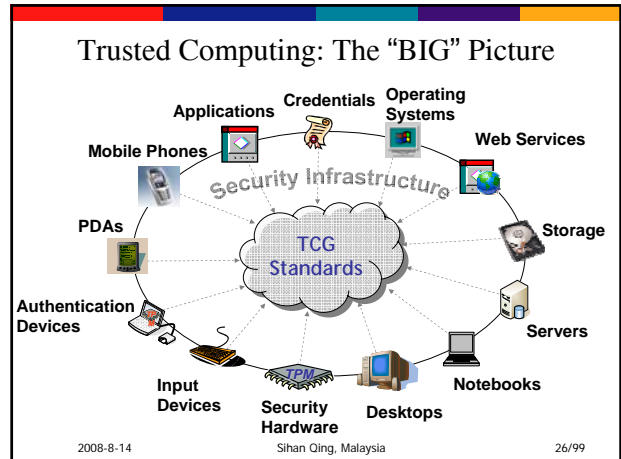
2008-8-14

Sihan Qing, Malaysia

24/99

Part 3  
Trusted Computing Activities in China

2008-8-14      Sihan Qing, Malaysia      25/99



- In January 2002, Bill Gates announced the Trustworthy Computing initiative which focused on building trust in the IT ecosystem. Although Trustworthy Computing was designed to focus on these attributes, including the related business practices that are necessary to implement and delivery it, most people initially equated it with security.

2008-8-14      Sihan Qing, Malaysia      27/99

- ### China's TC Working Group
- Set up on January 19th, 2005
  - One day meeting at Fujian Hotel, Beijing
  - 120 participants including government officials, enterprise CEO's, and potential users of information security products
  - Chair of TC working group: Prof. Sihan Qing
- 2008-8-14      Sihan Qing, Malaysia      28/99

- ### TC Working Group (cont.)
- Under the leadership of TC260
  - Supported by
    - The office of State Informatization Leadership Group
    - Research institutes and universities
    - IT enterprises
    - Banks, insurance companies, etc.
- 2008-8-14      Sihan Qing, Malaysia      29/99

- ### TC Working Group (cont.)
- Our mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate standardization, and promote international cooperation in the field of trusted computing
- 2008-8-14      Sihan Qing, Malaysia      30/99

**TC Working Group (cont.)**

- Long-term Plans
- Develop a series of TC national standards in China
- Help enterprises in China to set up a TCG like organization
- Suggest and propose projects of scientific research on TC topics

2008-8-14      Sihan Qing, Malaysia      31/99

**TC Working Group (cont.)**

- Work closely with TCG, and set up a long-term collaboration relationship
- Actively participate in international activities on TC topics

2008-8-14      Sihan Qing, Malaysia      32/99

**TC Working Group (cont.)**

- Short-term Plans
- Look at the evolution of TCG's standardization work closely
- Study on the published TCG standards
- Make detailed plans of developing China's TC standards

2008-8-14      Sihan Qing, Malaysia      33/99

**TC Working Group (cont.)**

- Seventh International Conference on Information and Communications Security (ICICS2005)
- 10-13 December, 2005
- Beijing, China
- TC is one of the focuses

2008-8-14      Sihan Qing, Malaysia      34/99

**ICICS Conference Series**

- ICICS'97, Beijing, Springer LNCS 1334
- ICICS'99, Sydney, Springer LNCS 1729
- ICICS'2001, Xi'an, Springer LNCS2229
- ICICS'2002, Singapore, Springer LNCS 2513
- ICICS'2003, Huhehote, Springer LNCS 2836
- ICICS'2004, Spain, Springer LNCS 3336
- ICICS'2005, Beijing, Springer LNCS 3783
- ICICS'2006, USA, Springer LNCS 4307
- ICICS'2007, Zhengzhou, Springer LNCS 4861
- ICICS'2008, UK, Springer LNCS

— Chair of Steering Committee: Prof. Sihan Qing

2008-8-14      Sihan Qing, Malaysia      35/99

**2008 International Trustworthy Computing and Trusted Computing Forum**

- October 22nd, 2008, Beijing
- Invited keynotes and Session Speakers:
  - Mr. Scott Charney, Vice President, Trustworthy Computing, Microsoft Corporation, has kindly accepted invitation to speak in the keynote session, and also spend the day with the participants through the technical and panel discussion sessions to discuss the questions, challenges, findings, and understanding relating to the topics of this Forum.

2008-8-14      Sihan Qing, Malaysia      36/99

## Functionality and Interface Specification of Cryptographic Support Platform for TC

- Announced on December 2007 by China National Cryptographic Administration Bureau

2008-8-14

Sihan Qing, Malaysia

37/99

## TCM—Trusted Cryptography Module

- SMS4—a Chinese symmetric encrypt/decrypt algorithm
  - 128 bits, CBC (Cipher Block Chaining) mode
- SM2—a Chinese asymmetric encrypt/decrypt algorithm (ECC- Elliptic Curve Cryptography)
- SM3—a Chinese hash algorithm

2008-8-14

Sihan Qing, Malaysia

38/99

## Part 4

### Some important technical issues

- Security model design and its formal analysis
- Covert channel analysis

2008-8-14

Sihan Qing, Malaysia

39/99

- A formal security model is essential when reasoning about the security of a system.
- Without an unambiguous definition of what security means, it is impossible to say whether a system is secure.

2008-8-14

Sihan Qing, Malaysia

40/99

Security models can be broken down into three major categories, listed in order of complexity:

- Models that protect against unauthorized disclosure of information,
- Models that protect against unauthorized tampering or sabotage, and
- Models that protect against DOS.

2008-8-14

Sihan Qing, Malaysia

41/99

Protection against disclosure of information has been understood the longest and has the simplest models. Protection against tampering or sabotage has been less well understood and appropriate models are only now under development. Protection against denial of service is not well understood today.

2008-8-14

Sihan Qing, Malaysia

42/99

Secrecy lattices, such as the Bell and LaPadula model while useful for protecting against unauthorized information disclosure, do not deal with unauthorized tampering or sabotage of information. The early military models focused only on secrecy.

2008-8-14

Sihan Qing, Malaysia

43/99

A commercial system, however, cannot be limited to only protecting the secrecy of information. Assuring that information is not tampered with is often much more important in a commercial setting.

2008-8-14

Sihan Qing, Malaysia

44/99

For example, when a cash card is used, ensuring that the correct amount of money are transferred may be much more important than keeping secret how much money were transferred.

2008-8-14

Sihan Qing, Malaysia

45/99

- Biba developed a model of mandatory integrity that is a mathematical dual of the Bell and LaPadula mandatory-security model.
- The principal difficulty with the Biba integrity model is that it does not model any practical system.

2008-8-14

Sihan Qing, Malaysia

46/99

Lipner developed an integrity model that uses both the mandatory security and mandatory integrity models to represent a software development environment in a bank. It tied the integrity modeling much closer to reality than the Biba model did, but it was still quite complex. No effort has been made to actually implement the Lipner model.

2008-8-14

Sihan Qing, Malaysia

47/99

Another famous integrity model is Clark and Wilson's model which focuses on two notions: *well-formed transactions* and *separation of duties*. Separation of duties is commonly used in commercial organizations to protect against fraud.

2008-8-14

Sihan Qing, Malaysia

48/99

The Clark and Wilson model consists of a set of certification and enforcement rules to be applied to a computer system. These rules apply to the operations of *transformation procedures* (TPs) that actually carry out the data manipulation in their system.

2008-8-14 Sihan Qing, Malaysia 49/99

Clark and Wilson clearly identified that the TPs needed to be certified to be valid. Unfortunately, they did not suggest any way to decide which TPs were valid and which were not. This is the same as the problem in the Biba model.

2008-8-14 Sihan Qing, Malaysia 50/99

- Role-based access control (RBAC) can implement sophisticated security policies that are difficult to implement otherwise.
  - For example, separation of duties can be implemented with role-based access control.
- 2008-8-14 Sihan Qing, Malaysia 51/99

We have made the following contributions: proposed a security architecture and three basic security models: confidentiality, integrity, and privilege control models.

2008-8-14 Sihan Qing, Malaysia 52/99

In Reference: Sihan Qing and Changxiang Shen. **Design of Secure Operating Systems with High Security Levels**. Science in China Ser F-Information Sciences. 2007 Vol. 50 No. 3, pp. 399-418, the design principles of the security architecture and three basic security models are discussed respectively. Three novel security models and a new security architecture are proposed. The prominent features of these proposals, as well as their applications to the ANSHENG OS, are elaborated.

2008-8-14 Sihan Qing, Malaysia 53/99

Covert channels are a real threat, although they are difficult to implement and exploit.

2008-8-14 Sihan Qing, Malaysia 54/99

The naissance of Covert Channel Concept

- Butler Lampson:
  - Note On the Confinement Problem, Communication of ACM, vol.16, 1973

2008-8-14      Sihan Qing, Malaysia      55/99

Covert channels became known to the community largely due to Lampson's "A Note on the Confinement Problem," which introduced the term "covert channels" but restricted its use to a subclass of leakage channels that excluded storage channels and "legitimate" channels".

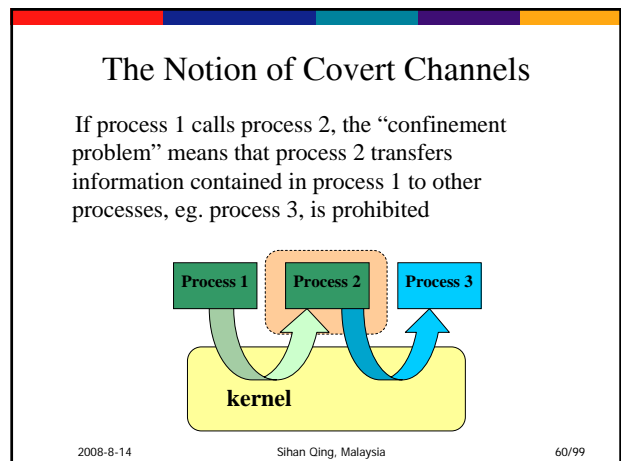
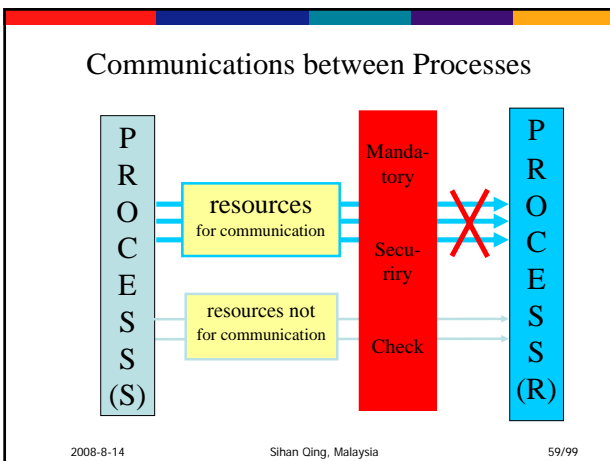
2008-8-14      Sihan Qing, Malaysia      56/99

Nowadays, we call storage channels and timing channels covert channels, and call legitimate channels examples of information hiding.

2008-8-14      Sihan Qing, Malaysia      57/99

Covert channels are a means of communication between two processes that are not permitted to communicate, but do so anyway, a few bits at a time, by affecting shared resources.

2008-8-14      Sihan Qing, Malaysia      58/99



### The Notion of Covert Channels

- In a secure OS with mandatory access control, the owner of the Trojan can receive info from the Trojan only through the use of a covert channel.

2008-8-14      Sihan Qing, Malaysia      61/99

### Direct Process Flow

- Process and state variable

2008-8-14      Sihan Qing, Malaysia      62/99

### Indirect Process Flow

- By indirect process flow the master of the Trojan horse can read the sensitive data.

2008-8-14      Sihan Qing, Malaysia      63/99

### The Objectives of CCA

- Covert Channel identification
- Covert Channel Bandwidth Estimation
- Covert Channel Handling
- Covert Channel Testing

2008-8-14      Sihan Qing, Malaysia      64/99

### Basic Flowchart of Covert Channel Analysis

```

    graph TD
      Start([Start]) --> CCID[CC Identification]
      CCID --> BE[Bandwidth Estimation]
      BE --> CH[CC Handling]
      CH --> DDP[Document Preparation]
      DDP --> End([End])
    
```

2008-8-14      Sihan Qing, Malaysia      65/99

### Covert Channel Definitions

- [Lampson 73] A communication channel is covert if it is neither designed nor intended to transfer info at all.
- [Schaefer 77] A communication channel is covert (e.g., indirect) if it is based on transmission by storage into variables that describe resource states.

2008-8-14      Sihan Qing, Malaysia      66/99

## Covert Channel Definitions

3. [Tsai 90] Given a nondiscretionary (e.g., mandatory) security policy model  $M$  and its interpretation  $I(M)$  in an OS, any potential communication between two subjects  $I(S_h)$  and  $I(S_i)$  of  $I(M)$  is covert iff any communication between the corresponding subjects  $S_h$  and  $S_i$  of the model  $M$  is illegal in  $M$ .

2008-8-14

Sihan Qing, Malaysia

67/99

## The Consequences of the above Definition

1. Irrelevance of discretionary policy models
2. Dependency on nondiscretionary security policy models
3. Relevance to both secrecy and integrity models
4. Dependency on TCB specifications

2008-8-14

Sihan Qing, Malaysia

68/99

## Classification

- Storage and Timing Channels
- Noisy and Noiseless Channels
- Aggregated versus Non-Aggregated Channels

2008-8-14

Sihan Qing, Malaysia

69/99

## Storage vs. Timing Channels

- Storage covert channel
  - A potential covert channel is a **storage channel** if in which the synchronization between the sender and the receiver uses storage variables.
- Timing covert channel
  - A potential covert channel is a **timing channel** if in which the synchronization between the sender and the receiver include the use of a time reference.

2008-8-14

Sihan Qing, Malaysia

70/99

## Noisy vs. Noiseless Channels

- A channel is said to be noiseless, if the symbols transmitted by the sender are the same as those received by the receiver with probability 1.
- With covert channels, each symbol is usually represented by one bit, and therefore, a covert channel is noiseless if any bit transmitted by a sender is decoded correctly by the receiver with probability 1.

2008-8-14

Sihan Qing, Malaysia

71/99

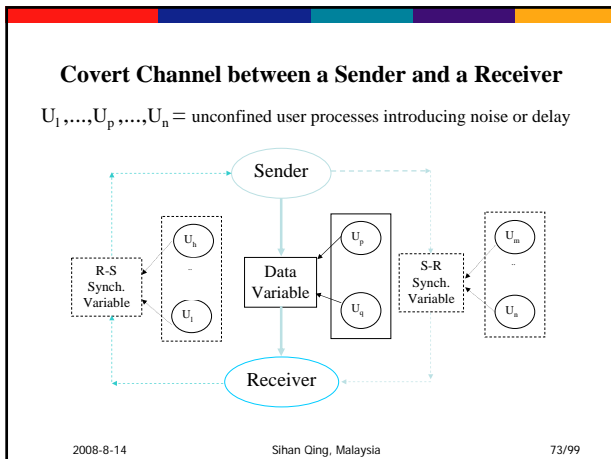
## Typical Storage Channels

- Policy conflict channels (noiseless)
- Resource exhaustion channels (noisy)
- Event-count channels (noisy)

2008-8-14

Sihan Qing, Malaysia

72/99



### Bandwidth

- Bandwidth is originally a term used in analog communication measured in hertz and related to information rate by the “sampling theorem”.
- Here the term “bandwidth” is used to denote the rate at which information is transmitted via a channel.
- In a covert channel context, bandwidth is given in bits/second rather than hertz, and is commonly used as a synonym for information rate.

2008-8-14      Sihan Qing, Malaysia      74/99

### Trusted Computing Base (TCB)

- Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy.

2008-8-14      Sihan Qing, Malaysia      75/99

### Looking for Covert Channels

1. Total reliance on the analysis of (formal or descriptive) top-level specifications (FTLS or DTLS) is inadequate, as such analysis cannot identify all covert channels that may appear in the implementation code.
  - Remark: Formal methods for showing the correspondence between top-level specifications and the implementation code do not exist to date.

2008-8-14      Sihan Qing, Malaysia      76/99

### Looking for Covert Channels

2. Total reliance on the analysis of design specifications is undesirable, as such analysis leads to the discovery of false information flows, i.e., flows that appear in the FLTS or DTLS but do not appear in the implementation code.

2008-8-14      Sihan Qing, Malaysia      77/99

### Looking for Covert Channels

3. To summarize, although the identification of potential covert channels in top-level specifications helps detect design flaws that may lead to covert channels in the final implementation, in order to search for covert channels thoroughly we still need to apply covert channel analysis to implementation code.

2008-8-14      Sihan Qing, Malaysia      78/99

Methods for Covert Channel Identification

1. The Shared Resource Matrix (SRM)
2. Information Flow Formulas
3. Covert Flow Trees
4. Noninterference Analysis

2008-8-14      Sihan Qing, Malaysia      79/99

The SRM (Shared Resource Matrix) Method

- A widely used approach proposed by Kemmerer in 1983, which can be applied to both TCB specifications and code.
- The SRM Method requires the following four steps.

2008-8-14      Sihan Qing, Malaysia      80/99

The SRM (Shared Resource Matrix) Method

1. Describe all TCB primitive operations by DTLS, FTLS, or source code.
2. Build a shared resource matrix consisting user-visible operations as rows and visible/alterable object attributes as columns, mark each <operation, attribute> entry by R or M depending on whether the attribute is read or modified.

2008-8-14      Sihan Qing, Malaysia      81/99

The SRM (Shared Resource Matrix) Method

3. Perform a transitive closure on the entries of the SRM.
  - Remark: This identifies all indirect process flows whenever this step is applied to an user-visible interface.

2008-8-14      Sihan Qing, Malaysia      82/99

The SRM (Shared Resource Matrix) Method

4. Discover scenarios of use for potential covert channels by analyzing all entries of the matrix. Analysis of matrix entry leads to one of the four possible conclusions:

2008-8-14      Sihan Qing, Malaysia      83/99

The SRM (Shared Resource Matrix) Method

- (1) A legal channel exists between the two communicating processes, labeled L.
- (2) No useful info can be gained from the channel, labeled N. (Remark: This will be the case if the only info that can be signaled over the channel is info that the receiver already possesses.)
- (3) The sending and receiving processes are the same, labeled S (Remark: Processes are allowed to "mumble").
- (4) A potential storage channel exists, labeled P.

2008-8-14      Sihan Qing, Malaysia      84/99

### The SRM (Shared Resource Matrix) Method

- Advantages:
  - It can be applied to both TCB specifications and source code.
  - In principle, it can be applied to both storage and timing channels.
  - It eliminates a major source of false illegal flows.

2008-8-14 Sihan Qing, Malaysia 85/99

### The SRM (Shared Resource Matrix) Method

- Disadvantages:
  - Individual TCB primitives cannot be proven secure in isolation, therefore this shortfall adds the complexity of incremental analysis of new TCB functions.
  - (Remark: Because of the lack of security-level assignment to variables.)
  - False illegal flows still exist.

2008-8-14 Sihan Qing, Malaysia 86/99

### An example of the identification result

No.	Name	Variable	Read operations	Write operations	Remark
1	Sd	dentry.d_name	Mkdir, creat	mkdir	Event-count
2	Pid	Last_pid	Fork/getpid	Fork, vfork, clone	Event-count
3	Nfi	Sb->u.ext3_sb.s_es->S_free_inodes_count	statfs	Creat, mknod	Event-count
4	Nfb	Sb->u.ext3_sb.s_es->S_free_blocks_count	statfs	Creat, mknod	Event-count
5	At	Inode.l_atime	stat	Open/read	Event-count
6	fd	files_stat_nr_unused	creat	Creat	Resource exhaustion

2008-8-14 Sihan Qing, Malaysia 87/99

### Methods for Handling Covert Channels

1. Elimination of covert channels
  - This requires that the design of an OS be changed so that no covert channels are left in the OS.

2008-8-14 Sihan Qing, Malaysia 88/99

### Methods for Handling Covert Channels

2. Bandwidth limitation
  - This requires the reduction of the maximum, or alternatively the average, bandwidth of any channel to a predefined acceptable limit.

2008-8-14 Sihan Qing, Malaysia 89/99

### Ways of limiting bandwidths

- a) Deliberately introducing noise into channels
- b) Deliberately introducing delays in each TCB primitive of a real channel

2008-8-14 Sihan Qing, Malaysia 90/99

**Methods for Handling Covert Channels**

3. Auditing the use of covert channels  
 -This approach allows all known channels to be used by any user but provides a mechanism that would discourage the use of the channels

2008-8-14      Sihan Qing, Malaysia      91/99

**Guidelines in TCSEC**

The TCSEC guidelines on covert channels suggest a combination of the above methods:

1. Use a bandwidth oriented policy to reduce the maximum bandwidth of each channel to 1 bit/second.
2. Use a deterrent policy to audit all channel use for channels with bandwidths between 0.1-1 bit/second
3. Use a “don’t care” policy for covert channels with bandwidths less than 0.1 bit/second.

2008-8-14      Sihan Qing, Malaysia      92/99

CCA has long been recognized as a notoriously hard problem to be solved. Although new countermeasures have been steadily improving, the current state of the art is still far from posing a satisfactory way of approaching this problem.

2008-8-14      Sihan Qing, Malaysia      93/99

We have considered the following two critical issues: 1) How to guarantee the completeness of covert channel identification? Namely, how to carry out a thorough search for covert channels? 2) How to identify covert channels more effectively and efficiently?

2008-8-14      Sihan Qing, Malaysia      94/99

In order to resolve the fundamental difficulties of CCA, we have proposed (1) a sound theoretical basis for completeness of covert channel identification, (2) a unified framework for covert channel identification, and (3) an efficient backward tracking search method.

The successful application of our new proposals to ANSHENG OS has shown that it can help ease and speedup the entire CCA process.

2008-8-14      Sihan Qing, Malaysia      95/99

**We have identified 20 covert storage channels**

- 1 channel belongs to process sub-system, 1 belongs to network sub-system, 13 belong to file sub-system, and 5 belong to IPC sub-system.
- If classified by coding characteristics, 8 event-count channels and 12 resource exhaustion channels.
- If classified by noisy characteristics, 16 noisy channels and 4 noiseless channels.

2008-8-14      Sihan Qing, Malaysia      96/99

- The above results appear to be the first report of CCA concerning Linux based OS.
- We have discovered the following covert channels which have never appeared in the literature before: sub-directory exhaustion channel; homonymy sub-directory channel; recent access time channel; index node number channel; IPC identifier reuse channel and IPC naming channel.

2008-8-14

Sihan Qing, Malaysia

97/99

### Reference:

Sihan Qing and Changxiang Shen. Design of Secure Operating Systems with High Security Levels.

Science in China Ser F-Information Sciences. 2007 Vol. 50 No. 3, pp. 399-418.

2008-8-14

Sihan Qing, Malaysia

98/99



# *Thank you*

2008年7月9日

卿斯汉 海南大学

99/99