Trusted Computing and Trustworthy Networks in Tsinghua University (THU)

Chuang Lin
chlin@tsinghua.edu.cn

Outline

- **Introduction to Tsinghua Unveirsity and CS Dept.**
  - **Overlook for Tsinghua University**
  - **General Information of CS Department**
  - **Institutes & Laboratory in CS Department**
- **Trusted Computing of TCG**
  - **Basic concepts & history of Trusted Computing**
  - **A reference architecture of TCG**
  - **TCG-related products**
  - **Trusted Network Connection**
- **Trustworthy Networks of THU**
  - **Why propose Trustworthy Networks**
  - **What is Trustworthy Networks**
  - **Scientific challenges and Open Key Issues**
  - **How to construct Trustworthy Networks**
  - **Related works**
- **Our Investigation Plan**

1. Introduction of CS Department of THU

- **Overlook for Tsinghua University**
- **General Information of CS Department**
- **Institutes & Laboratory in CS Department**

1.1 Overlook for Tsinghua University

- BRIEF HISTORY
  - Tsinghua School was founded in 1911 on the site of “Tsinghua Yuan”, a former imperial garden of the Qing Dynasty.
  - In 1928, the school was named National Tsinghua University.
  - In 1952,with the restructuring of Chinese higher education system, the university became focused on science and engineering.
  - Since 1978, many schools have been restored and new ones established.
  - Tsinghua University is now a multi-disciplinary university with 12 schools and 48 departments.

1.1 Overlook for Tsinghua University

- CAMPUS
  - Tsinghua University is located in the northwestern part of Beijing.
  - The campus covers an area of 3.8 square kilometers with more than 50,000 people living on it including all of the full time students.
  - Supermarkets, bookstores, hospital, kindergarten, primary school, high school and other facilities on campus make daily life very convenient.

1.1 Overlook for Tsinghua University

- Culture
  - The educational doctrine of Tsinghua is “to train the students with integrity”
  - Self-discipline and Social Commitment
  - Action speaks louder than words

1.1 Overlook for Tsinghua University

- Students

Total	25,474
Undergraduates	14,260
Graduate students	11,214
(PhD candidates)	3,782

1.1 Overlook for Tsinghua University

- Faculty

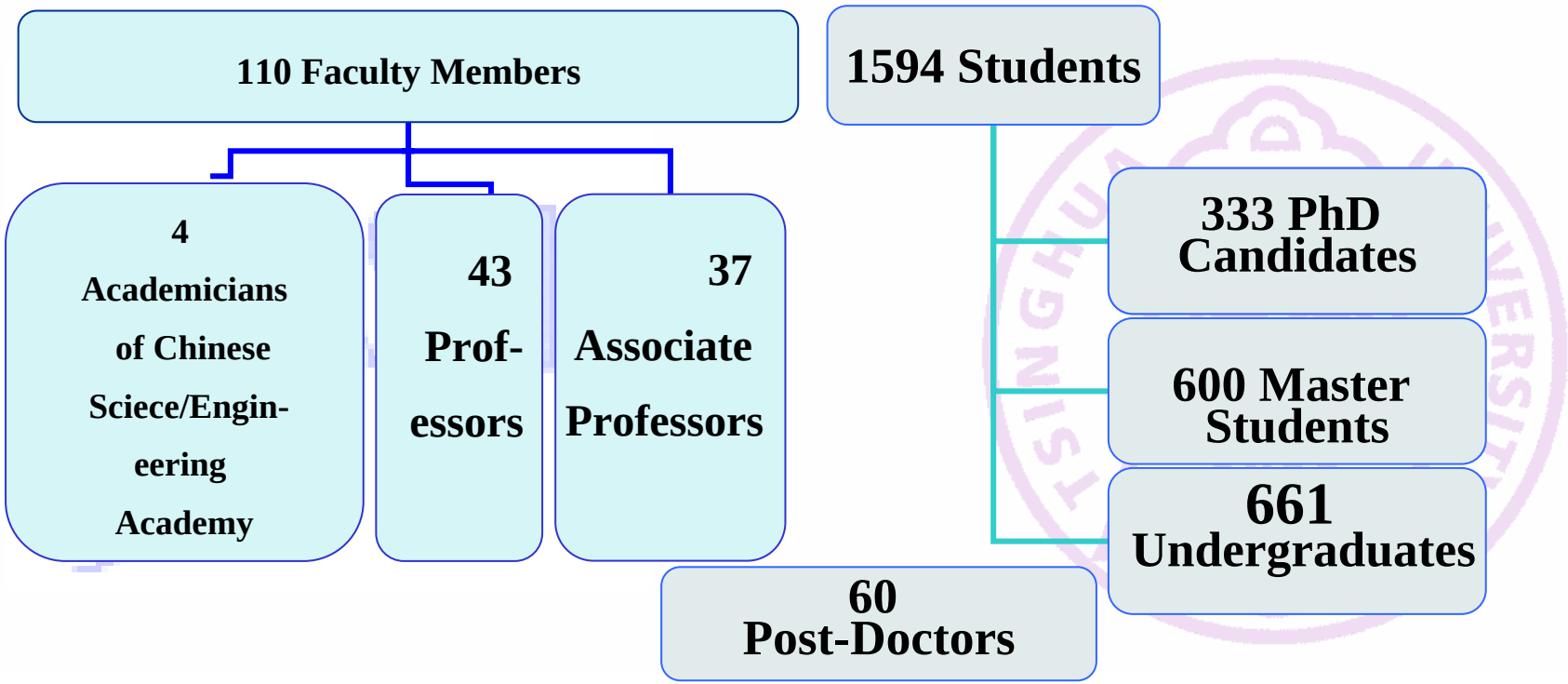
Faculty members	5,488
Full professors	1,105
Associate professors	1,814
Members of the Chinese Academy of Sciences	25
Members of the Chinese Academy of Engineering	24

1.1 Overlook for Tsinghua University

- University Calendar
  - Fall Semester---Early September to middle January
  - Spring Semester---Late February to late June
  - Summer Session---Early August to early September
    - The summer session is mainly for internship and elective courses.

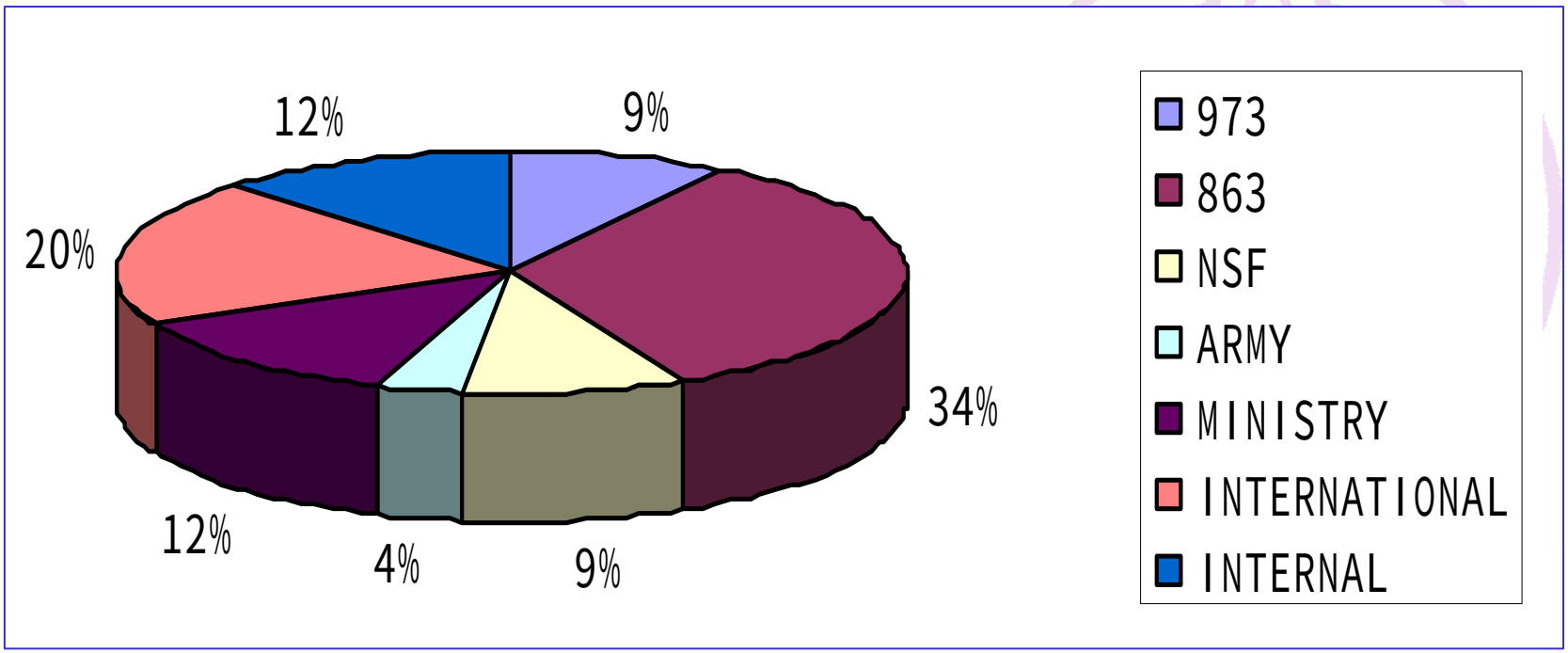
1.2 General Information of CS Department

People of CS Department



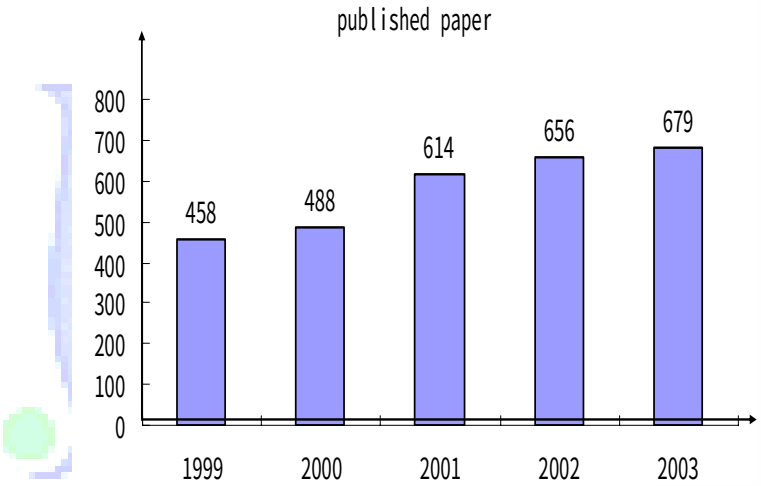
1.2 General Information of CS Department

- Research Projects of CS Department
  - **in 2004, 290 Research Projects with 51,140,000RMB funding**



1.2 General Information of CS Department

- Publications of CS Department
  - Published 676 papers in 2003 and 712 papers in 2004



  - Obtained 4 National Invention Patents
  - Obtained 3 National Awards

Courses of CS Department

- Courses in 2004：
  - Undergraduate Courses: 80
  - Graduate Courses: 60
- Excellent Course：
  - National Level：“Computer Language and Program Design”
  - MOE Level: “ Multimedia Computing: Technology and Application”
  - University Level：4 Undergraduate Courses +7 Graduate Courses
- Visitors and talks: more than 100 famous universities and IT companies in the world in 2004
- Lectures: more than 60 from famous professors

1.3 Institutes & Laboratory in CS

- Institute of Computer Network Technology
- Institute of High Performance Computing
- Institute of Computer Software and Computing Theory
- Institute of Human-Computer Interaction and Media Integration
- State Key Lab of Intelligent Technology and Systems

1.3 Institutes & Laboratory in CS

- **Computer Network Technology**
  - Next Generation Internet (NGI)
  - Network Protocol Testing
  - Distributed Information System (DIS)
  - Resource Management and Task Scheduling
  - Computer Supported Cooperative Work (CSCW)
  - Network Information Security

1.3 Institutes & Laboratory in CS

- **Computer Network Technology**
  - New Projects:
    - 973 Project: Foundation Research for the Next Generative Internet(funding: 15million RMB)
    - CNGI backbone networks and IPv6 project with Japan (funding: 250 million RMB)
      - CERNET2 will be the largest IPv6 network in the world
    - Recourse Management and QoS Modeling for the Next Generative Internet (funding from NSFC: 2million RMB)

1.3 Institutes & Laboratory in CS

- **High Performance Computing**
  - High Performance Computer Architecture and Cluster Computing
  - Hierarchical Storage Architecture for Massive Information
  - Network Storage Architecture and Technology
  - Grid Techniques and Environments
  - Advanced Computational Infrastructure (ACI)
  - CPU Design
  - Bioinformatics

1.3 Institutes & Laboratory in CS

- **Computer Software and Computing Theory**
  - Data Engineering and Knowledge Engineering
  - Design Automation of Computer and VLSI Circuits
  - Visualization and Computer Graphics
  - Software Engineering.

1.3 Institutes & Laboratory in CS

- **Human-Computer Interaction and Media Integration**
  - Human Computer Interaction
  - Pervasive Computing
  - Media Information Processing and Understanding

1.3 Institutes & Laboratory in CS

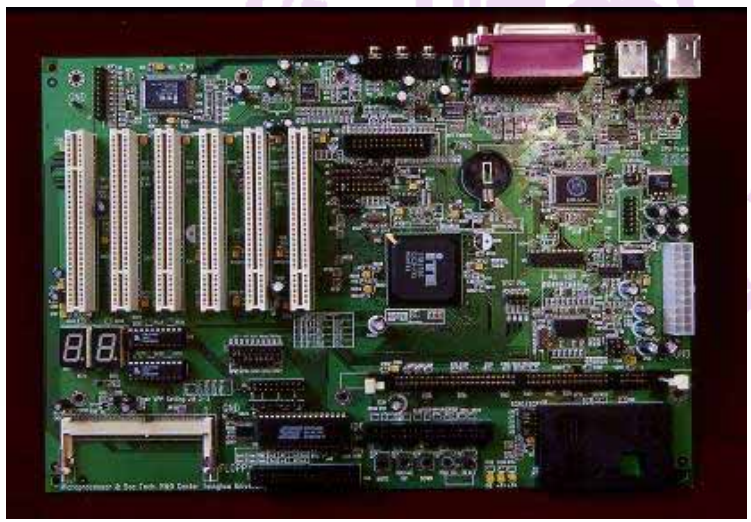
- **State Key Laboratory of Intelligent Technology and Systems**
  - foundation of AI
  - formal methods
  - quantum computation and quantum information
  - intelligent information processing
  - (speech, document etc.)
  - natural language processing
  - intelligent control and robots

Achievements

IPv4/v6 Dual Stack Router

Achievements

- **High-Performance and low-power Embedded Microprocessors (CPU)**
  - running at the speed of 400MHz at the typical case and 500MHz at the best case
  - power consumption below 0.5W at typical case.



Achievements

Network Storage Architecture (NSA) Systems:

Obtained 10 National Invention Patents

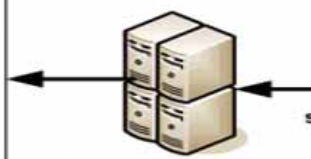
Obtained 13 Software Copyrights

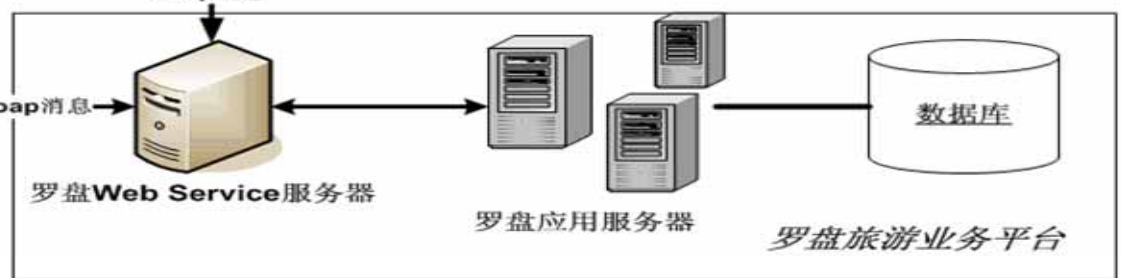
Achievements

Smart Classroom

Achievements

Web Services Management Middleware(WSMS, Web Services management system) which aims to help the Web Service applications to choose and integrate Web Services among Web Service providers by using workflow technology .





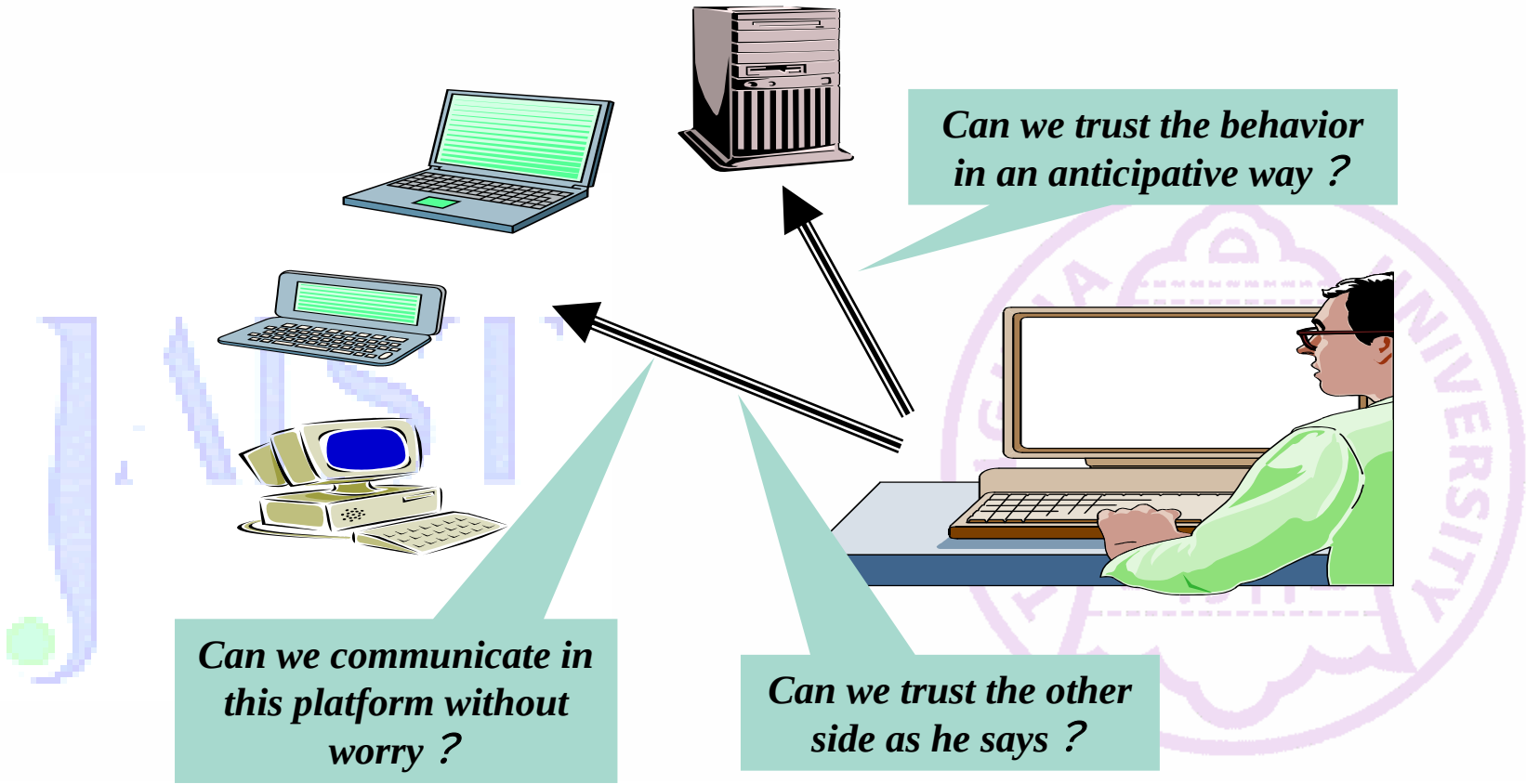
罗盘旅游业务平台是基于J2EE + XML技术实现的Web应用系统，并对外提供旅游业务的Web服务。该图是罗盘系统向北京旅游局网站提供旅游业务功能示意图。

Achievements

2. Trusted Computing of TCG

- Basic concepts & history of Trusted Computing
- A reference architecture of TCG
- TCG-related products
- Trusted Network Connection

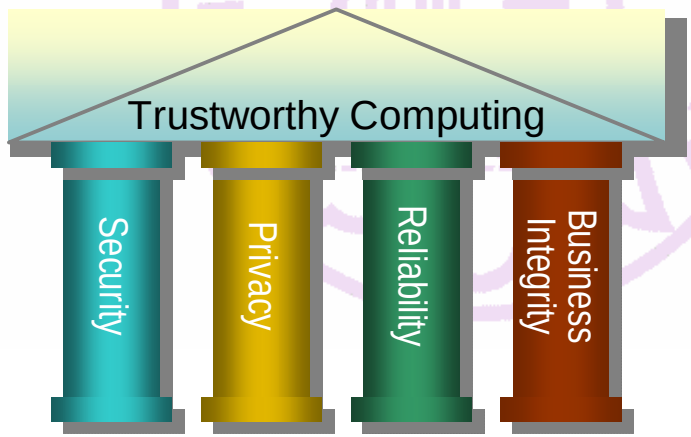
2.1 Basic concepts & history of Trusted Computing



Basic problem in Trusted Computing

2.1 Basic concepts & history of Trusted Computing

- **Concept of Trusted Computing**
  - if something happens with its behavior and result foreseeable，then it’s trusted
  - Target of Trusted Computing：to protect data in the key information system



2.1 Basic concepts & history of Trusted Computing

- **History of trusted computing**
  - TCPA， Trusted Computing Platform Alliance
    - Originated and set up by IBM、Intel、Microsoft in October 1999
    - Aim of TCPA
      - is to establish an open standard of trusted computing
        - » standardization of software and hardware
        - » Require current platform to support trusted computing
        - » Feature：safe start-up、platform validation and protected storing

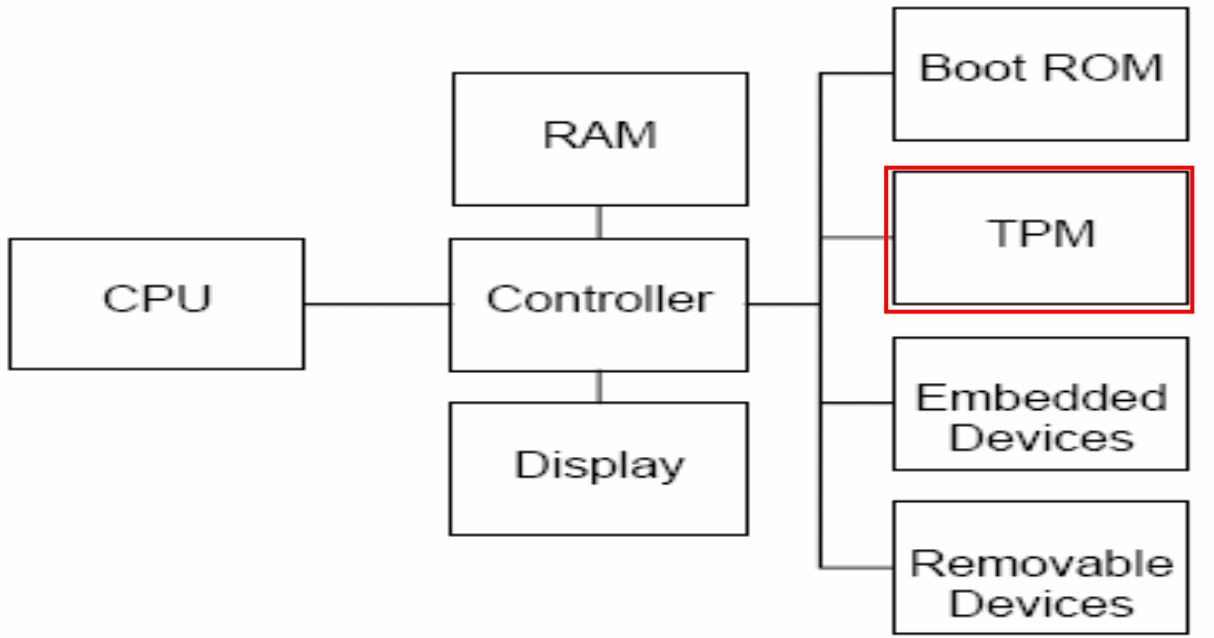
2.1 Basic concepts & history of Trusted Computing

- **History of trusted computing**
  - TCG, Trusted Computing Group
    - On April 8th 2003，TCPA is reorganize to TCG
    - keep using technical specification established by TCPA
    - establish TPM1.2 technology specification
  - At present TCG holds more than 200 members，most of which are international IT corporations
    - IBM, AMD, Hewlett-Packard , Intel Corporation, Microsoft , Sony Corporation, Sun Microsystems, Fujitsu, Hitachi, **Lenovo**, NEC,

2.1 Basic concepts & history of Trusted Computing

- **TCG Usage Scenarios**
  - Risk Management
  - Asset Management
  - E-commerce
  - Security Monitoring
  - Emergency Response

2.2 A reference architecture of TCG



Reference PC Platform Containing a TCG Trusted Platform Module (TPM)

2.2 A reference architecture of TCG

- **TPM** (Trusted Platform Module)
  - storing secret key、cipher and digital certificatio n
  - Integrated into main board
  - Function of anti-juggle and anti-polling-out
  - Providing powerful cipher operation

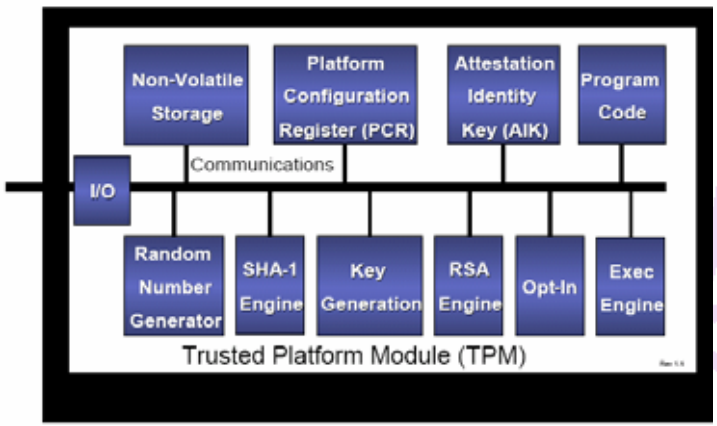
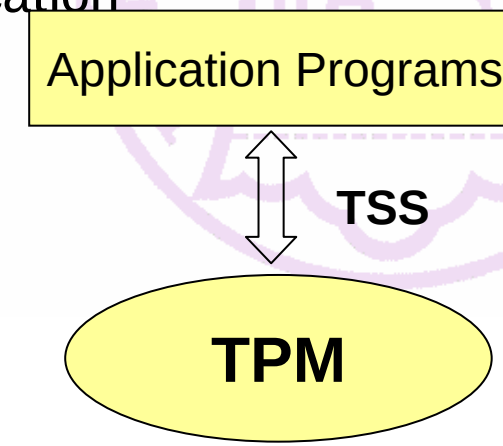


Fig. TPM components architecture

ensure each computer will report its configuration parameters in a trustworthy manner

2.2 A reference architecture of TCG

- **TSS** （TCG Software Stack Specification）
  - Standard API of accessing TPM
  - Application program Entrance to TPM
  - Providing synchronization access
  - Hiding command sequence of application
  - Managing TPM resources
  - Releasing TPM resources



2.3 TCG-related Products

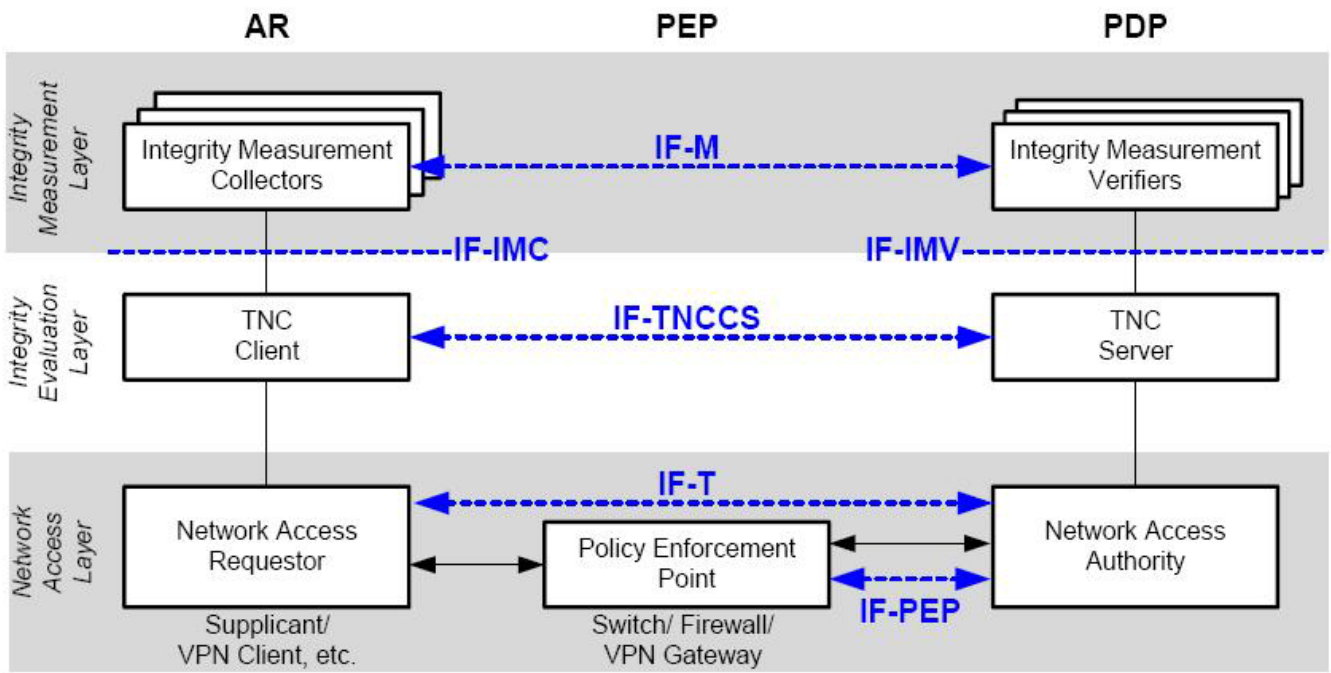
- **Palladium**
  - Released by Microsoft in June 2002
  - one Windows edition implementing trusted computing
- **ESS**（Embedded Security Subsystem）
  - Released by IBM in 2002
  - Used in ThinkPad notebook PC
- **LaGrande**
  - Released by Intel in Sep. 2003
  - Supporting Palladium
  - Adopted in CPU and chipset of Intel
- …

|Desktops || Laptops || Tablets || Reference Designs ||Motherboards ||White Box Manufacturers | |Other Use | |TPM Manufacturers ||Processors | |TPM Software |

2.4 Trusted Network Connection

- TNC architecture focuses on interoperability of network access control solutions, and leverage and integrate with existing network access control mechanisms such as 802.1X , VPN, TLS or others.
- Trusted computing is used as the basis for enhancing security of those solutions.
- Integrity measurements are used as evidence of the security posture of the endpoint.
- Access control points can evaluate the endpoint's suitability for being given access to the network.

2.4 Trusted Network Connection

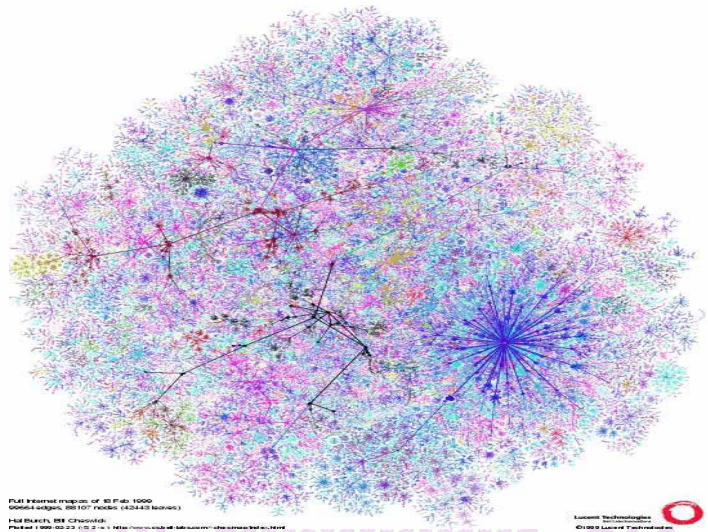


TNC Architecture

3. Trustworthy Networks of THU

- Why propose Trustworthy Networks
- What is Trustworthy Networks
- Scientific challenges and Open Key Issues
- How to construct Trustworthy Networks

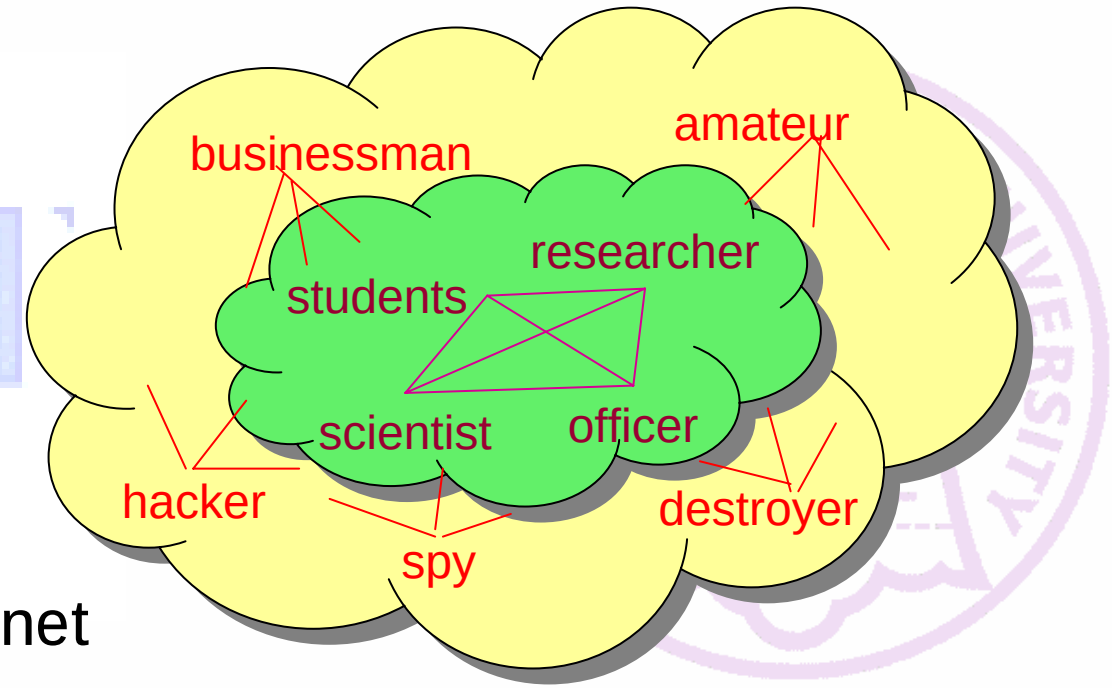
3.1 Why propose Trustworthy Networks



- More users、more application、more capability
- amalgamation of heterogeneous networks

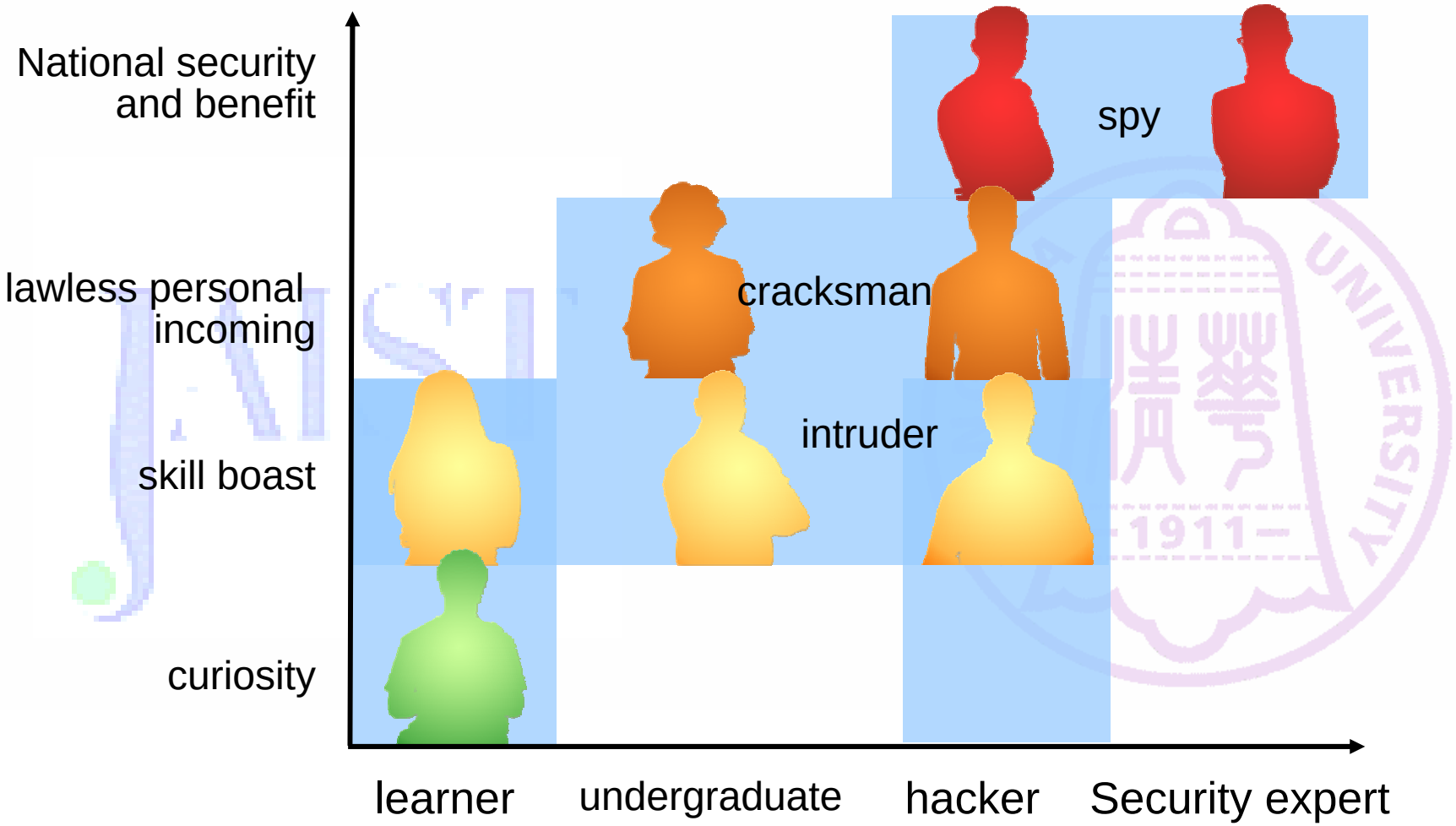
3.1 Why propose Trustworthy Networks

- Early Internet
  - a group of mutually trusting users attached to a transparent network



- The current Internet
  - Behaviors are various
  - Lack of trust among users

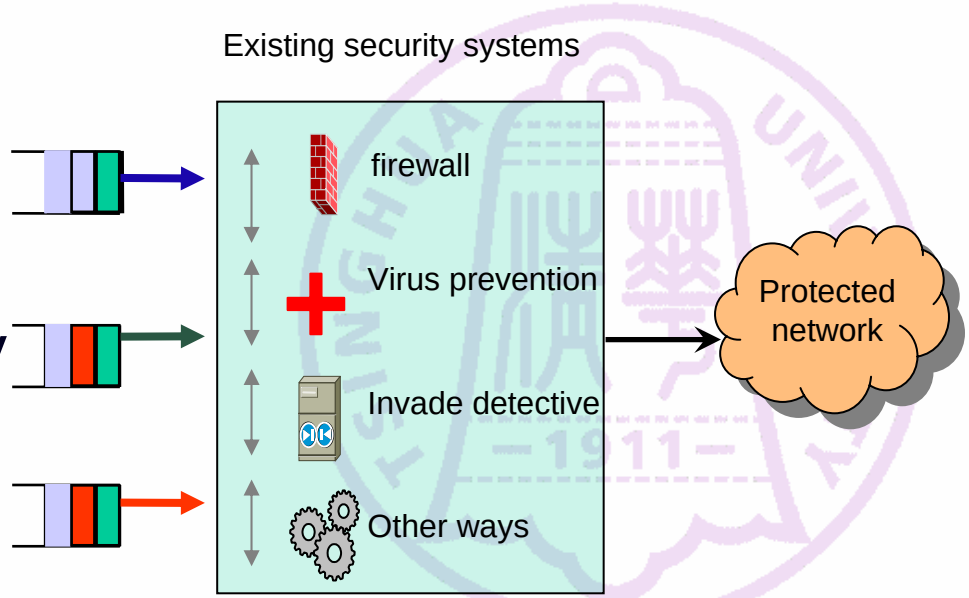
3.1 Why propose Trustworthy Networks



3.1 Why propose Trustworthy Networks

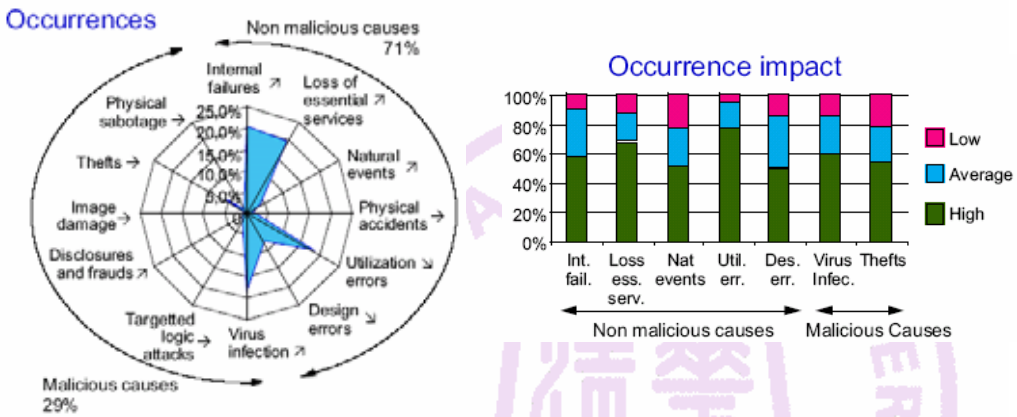
Internet cannot be trusted currently

- Current security system
  - Isolated,
  - Add-on
  - Patchwork
  - Passive
- Future networks security
  - Systematic
  - Holistic
  - In architecture
  - Active



3.1 Why propose Trustworthy Networks

- Malicious factor
  - Virus, worm, hacker a ttack, troy
- Unmalicious factor
  - Misoperation, manage leak, hardware fault, s oftware fault, natural damage



Survey on computer damages in France

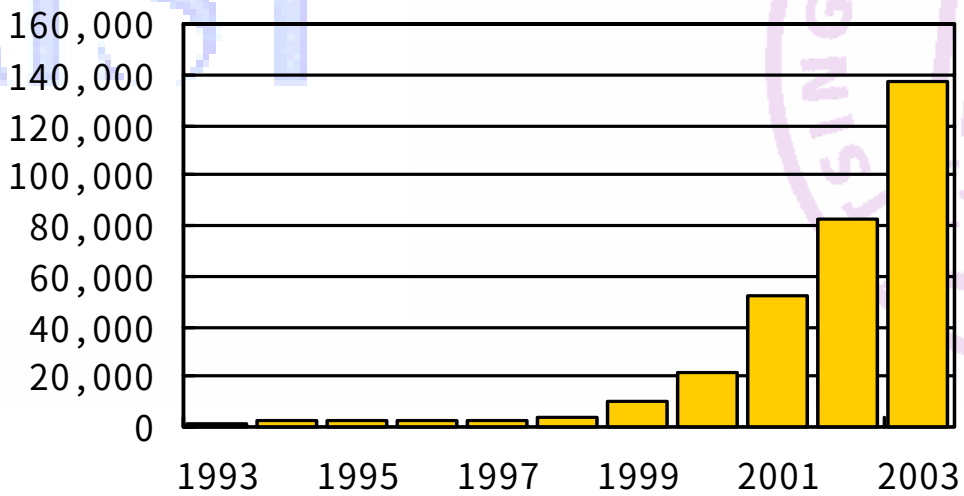
------CLUSIF

- The existing security system is not enough to fight these fact ors
  - malicious factor less than 1/3
  - Unmalicious factor more than 2/3

3.1 Why propose Trustworthy Networks

Network everywhere, threats everywhere!

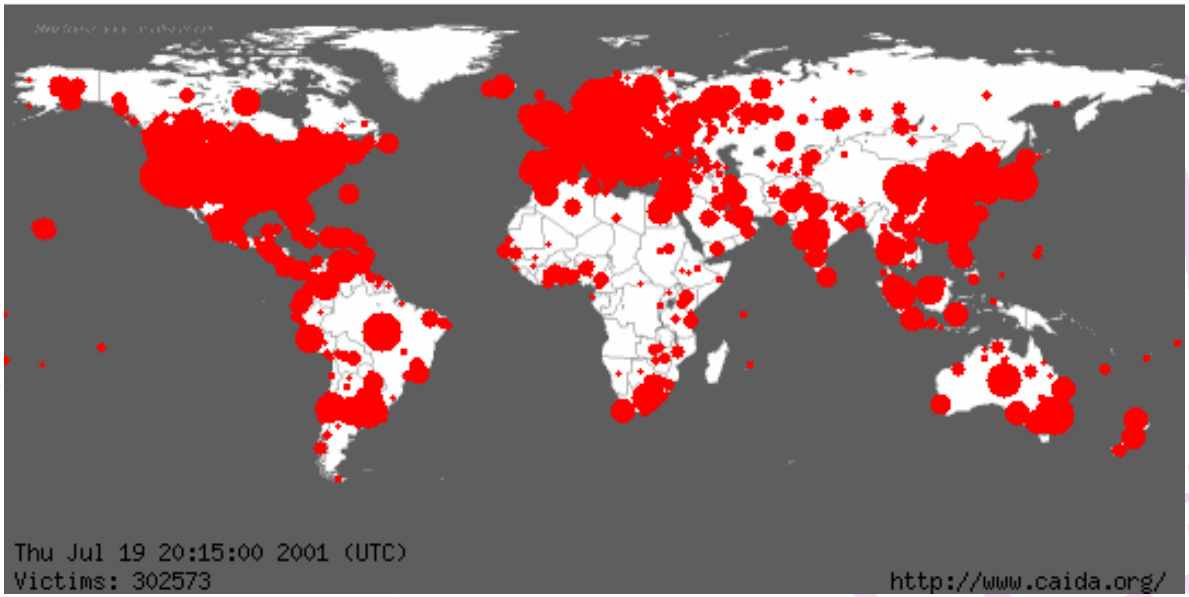
- In 2004,infection rate of computer virus of Chinese computer users is 87.9%, ,increased 2% then last year
- In 2004,rate of network security event of investigated units in China is 58%
- In 2003,the number of security event achieved to 137,529 in CERT/CC, increased 67.5% and 161% according to statistics in 2002 and 2001 respectively.



Stat. of Security event in CERT/CC

3.1 Why propose Trustworthy Networks

“red code” worm virus



- On July 19th 2001，more than 359，000 computers around the world had been infected in just 13 hours.
- economy loss came up to 2.4billion dollars.

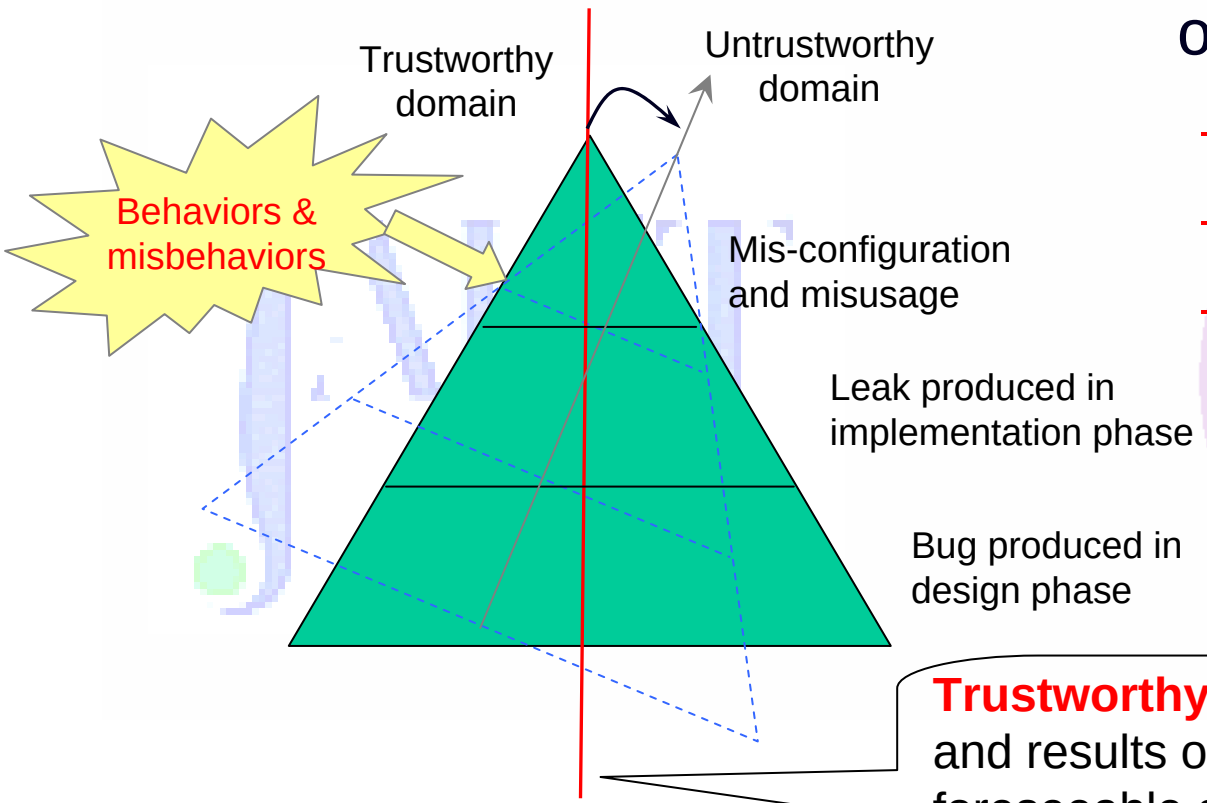
3.1 Why propose Trustworthy Networks

- Traditional research aims at pursuing high efficiency behaviors，but now high trustworthy network services need to be established for computer system，trustworthiness should becomes capability which can be scaled and validated。

  ------ David Patterson， American Engineering academician

- Trustworthy networks breakthrough object sand concepts of traditional security，and provide systemic security service，which is an important direction of network research.

3.2 What is Trustworthy Networks



- **Three basic properties** of trustworthy networks
  - Security
  - Survivability
  - Controllability

Trustworthy Networks：behaviors and results of network and users are foreseeable and controllable

3.2 What is Trustworthy Networks

- **Property I: Security**
  - Reduce system vulnerability and attack opportunity
    - Implementing **traditional security**
      - Confidentiality
      - Integrality
      - Availability
    - **Authenticity**
      - user ID
      - source
      - content
    - **Accountability**: any behaviors launched by network entity could be traced to entity itself
    - **Privacy**: some applications could be anonymous
    - Etc.

3.2 What is Trustworthy Networks

- **Property II: Survivability**
  - Maintain the key attributes of key network services in spite of attacks and faults
    - self-test
    - self-diagnose
    - self-recovery
    - self-organization
    - Fault-tolerance
    - Intrusion-tolerance

3.2 What is Trustworthy Networks

- **Property III: Controllability**
  - Current Internet cannot be controlled absolutely, but future internet should be controllable sufficiently
    - Provide connect-oriented property to some extent, via
      - Maintain some state information
      - Take some control based the information
    - Decrease the threat of attacks by
      - Checking data streams
      - Strict control in key nodes

3.3 Scientific challenges and Open Key Issues

- **Scientific challenges**
  - It is difficult to describe and analyses misbehaviors via the current models because attack behaviors own
    - Diversity
    - Randomicity
    - concealment
    - prevalence
  - How to construct a holistic and systemic secure service architecture. The current security system is
    - Isolated
    - Separate
    - Add-on or patchworks
    - Passive defense

3.3 Scientific challenges and Open Key Issues

- **Scientific challenges**
  - How to guarantee the key attributes of key network services, when facing
    - Inherent vulnerability in networked system
    - Unavoidable man-made mis-configuration and misusage
    - Various attack and destruction
  - How to provide powerful control and monitor mechanisms, holding the efficiency resulted from
    - Edge-oriented theory
    - connectless

3.3 Scientific challenges and Open Key Issues

- **Key scientific problems**
  - **Trustworthiness model** of network and user's behaviors
    - Describe trustworthiness characteristics of behaviors
    - build basic model and evaluation theory
  - **Architecture** of trustworthy networks
    - Design architecture of trustworthy networks
    - Provide systemic security services
  - **Survivability** of services
    - Provides continuable and recoverable network services, especially security service.
  - **Controllability** of network
    - Build internal and correlative mechanisms to control and monitor networks

3.4 How to construct Trustworthy Networks

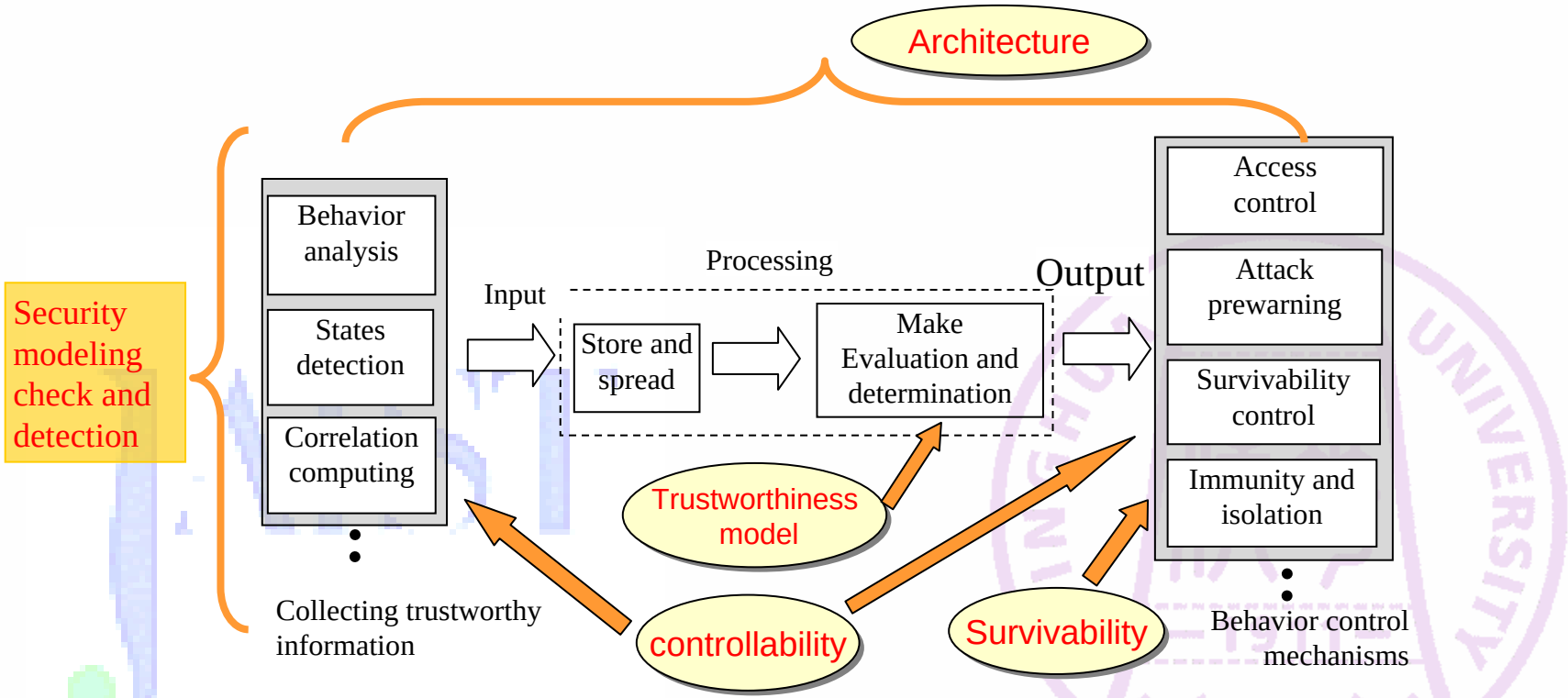


Fig. . Trustworthiness maintenance and behavior control.

- Closed correlation among scientific problems
- The four scientific problems are contacted via maintaining trust relationship making response to behavior

3.4 How to construct Trustworthy Networks

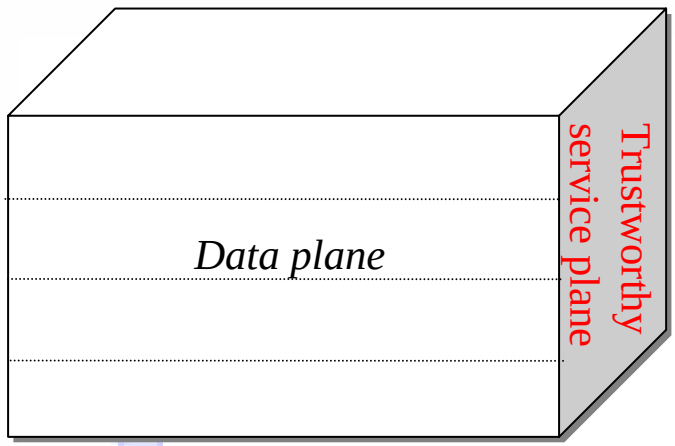


Fig. Framework trustworthy networks

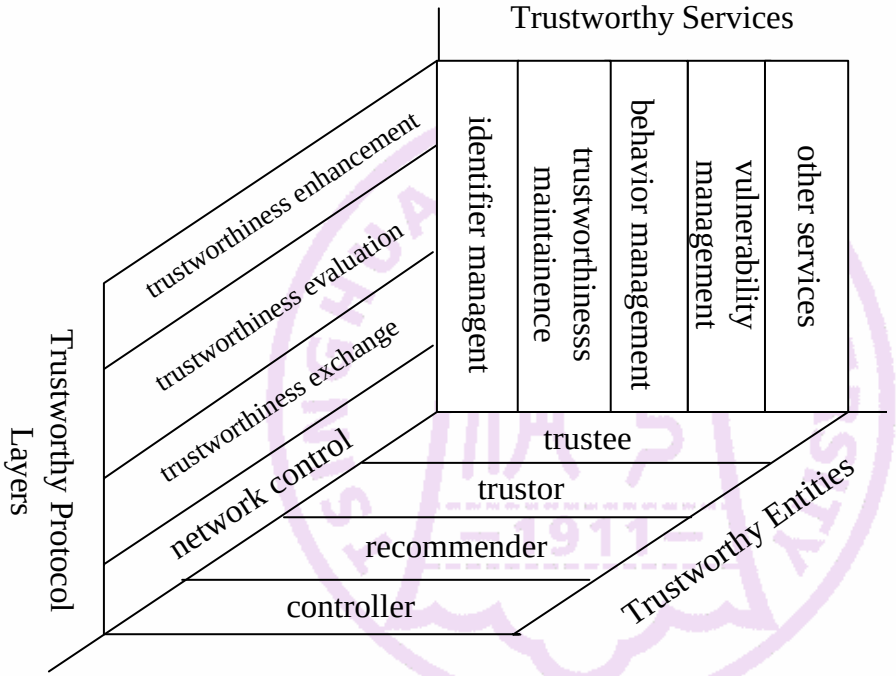


Fig. Three dimension model of Trustworthy Service Plane

3.4 How to construct Trustworthy Networks

- Trustworthy connection owns selectivity
- Build trust level of end-point，to ensure integrity of endpoint security policy
- Confirm security level of accessing user and maintain access policies
- Isolate abnormal terminal, and provide remediation resource

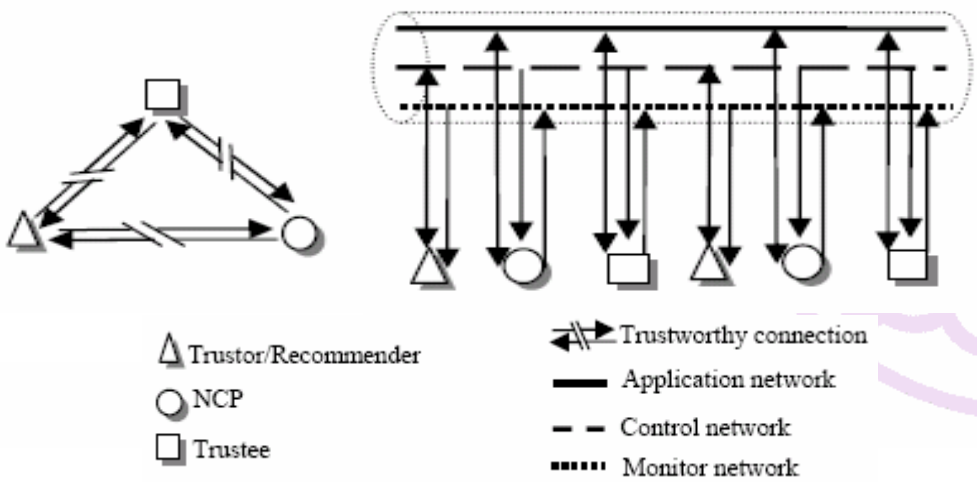


Fig. Three logical networks of trustworthy networks

3.5 Related works

- **Trust in Cyberspace**, proposed by ***National research council***
- **OAASIS** (organically assured survivable information systems), proposed by ***DoD***
- **MFTIA** (malicious and accidental fault tolerance for internet applications), boosted in ***Europe***.
- **CHAT** (composable high-assurance trustworthy systems), proposed by ***DARPA***.
- **TRIAD** (trustworthy refinement through intrusion-aware design), proposed by ***Carnegie Mellon University***.
- **ROC** (recovery-oriented computing), boosted in ***Stanford University***.
- **TNC** (trusted network connect), standardized by ***TCG***
- **Trustworthy e-Society**, proposed by ***JAIST***

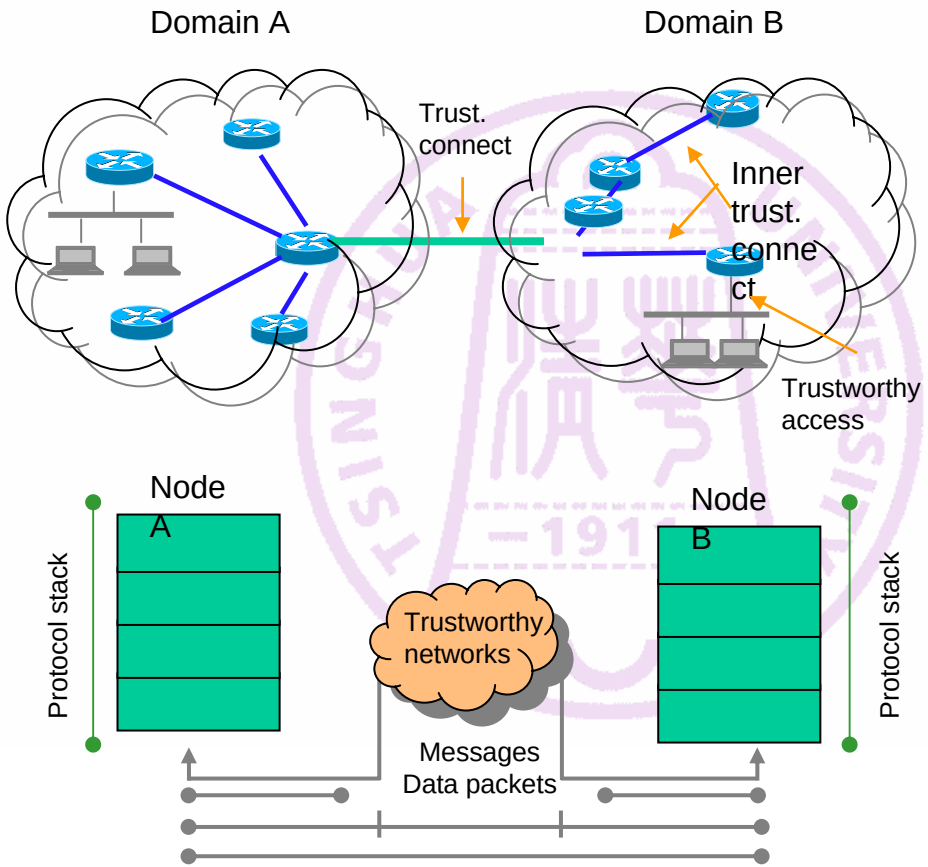
4. Our Investigation Plan

Main research contents

- Architecture of trustworthy networks security service
- Fundamental model and evaluation theories of trustworthy networks
- Theory and technology of survivability of trustworthy networks
- Theory and technology of controllability of trustworthy networks
- Integrity experiment and validation of trustworthy networks

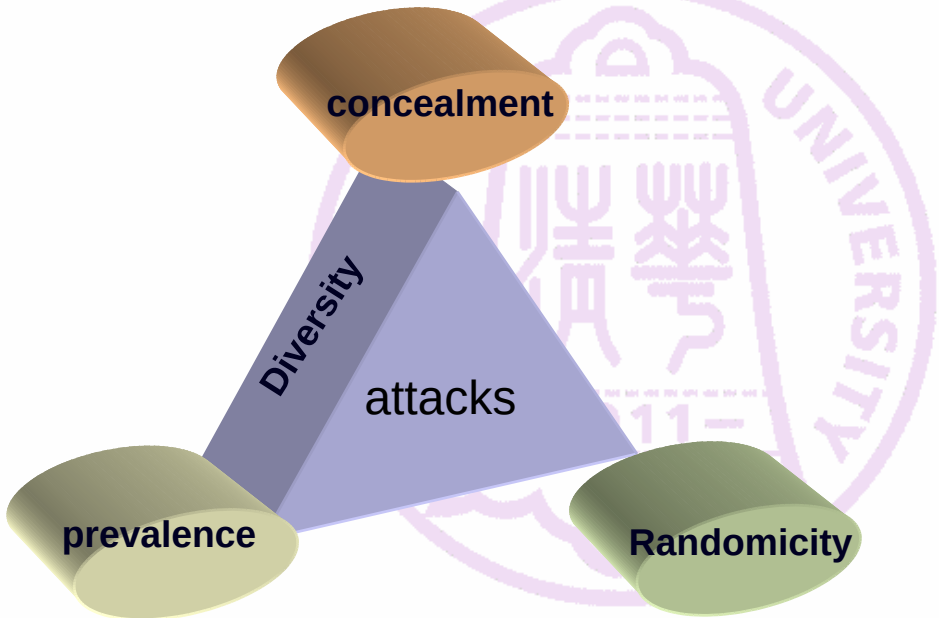
4. Our Investigation Plan

- **Architecture of trustworthy networks security service**
  - Architecture of trustworthy networks
  - Modeling and evaluation of vulnerability
  - Access control based on Trustworthy connect
  - Trustworthy protocols and protocol trustworthiness
  - Trustworthy routing, switch and mobile services



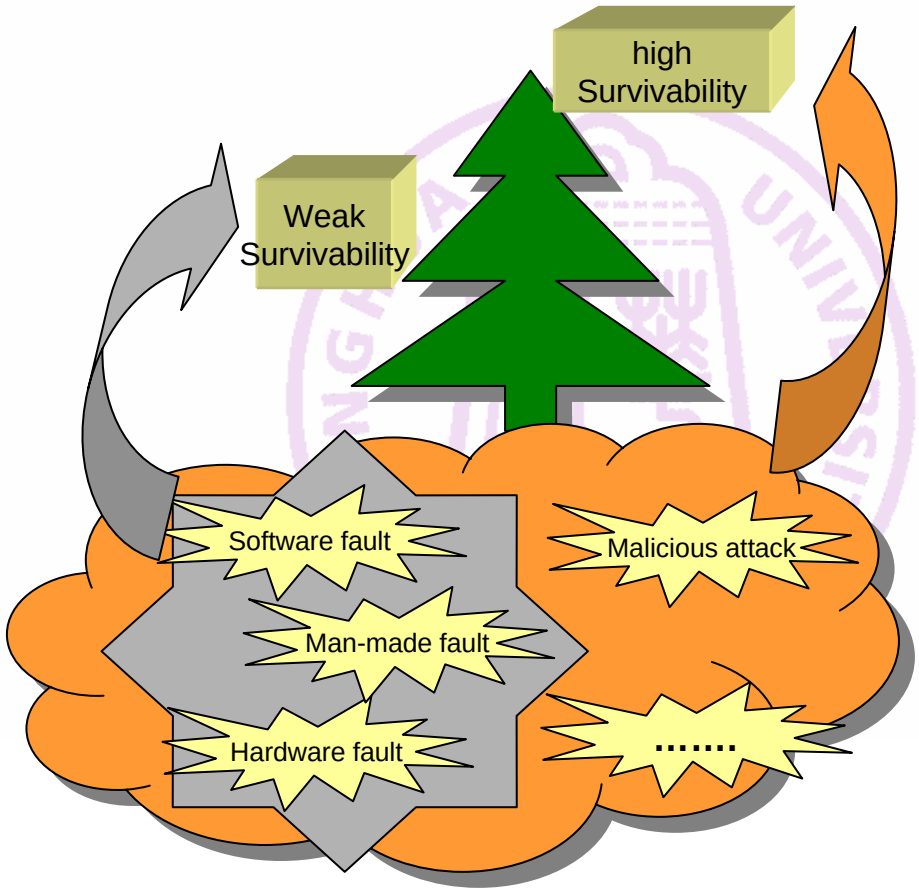
4. Our Investigation Plan

- **Fundamental model and evaluation theories of trustworthy networks**
  - Behaviors trustworthiness model
  - mathematic model theory of dynamic network process
  - Theory of evaluating trustworthiness
  - Theory of forecasting risk



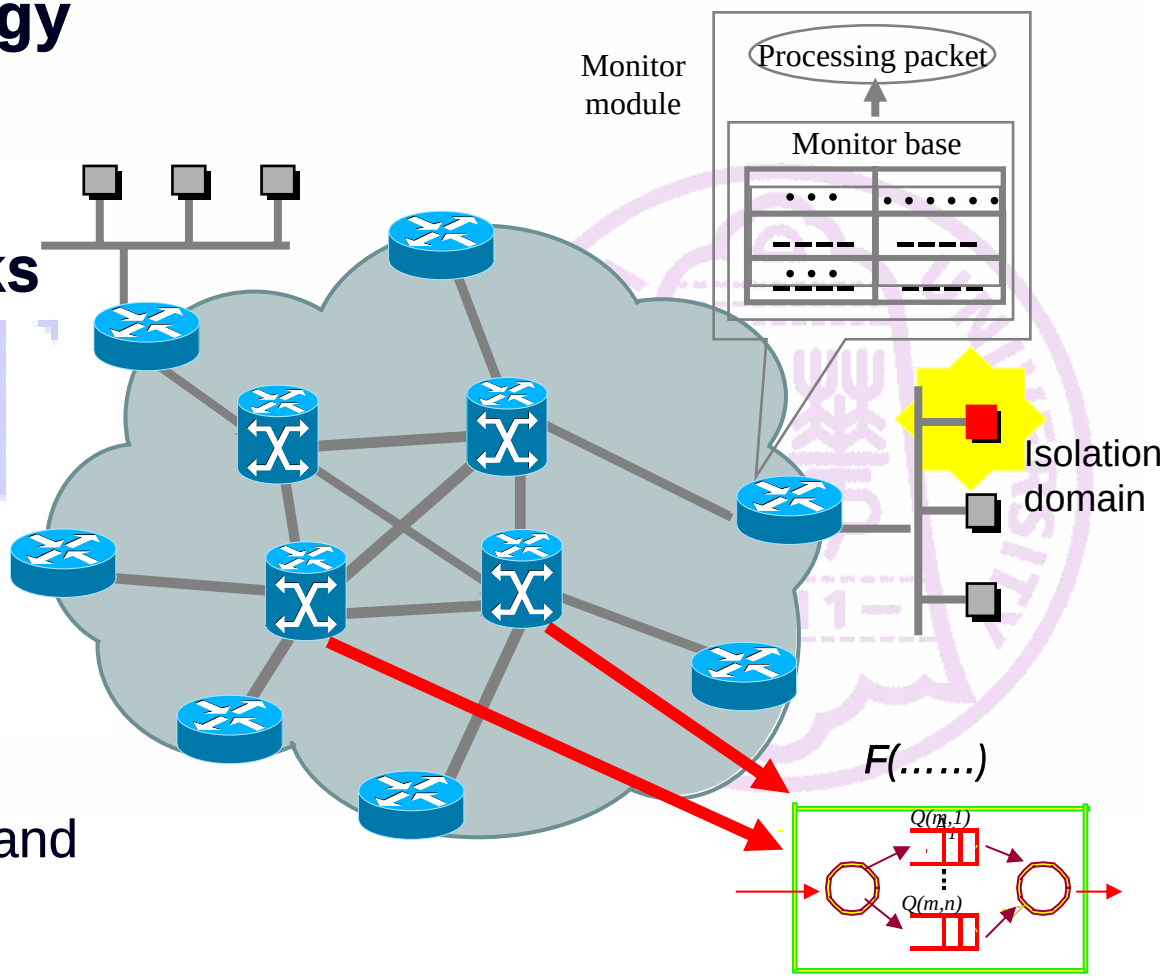
4. Our Investigation Plan

- **Theory and technology of enhancing trustworthy networks survivability**
  - Survivability model and evaluation
  - Measurable design of protocol and validation
  - Theory and technology of fault-tolerance and intrusion-tolerance



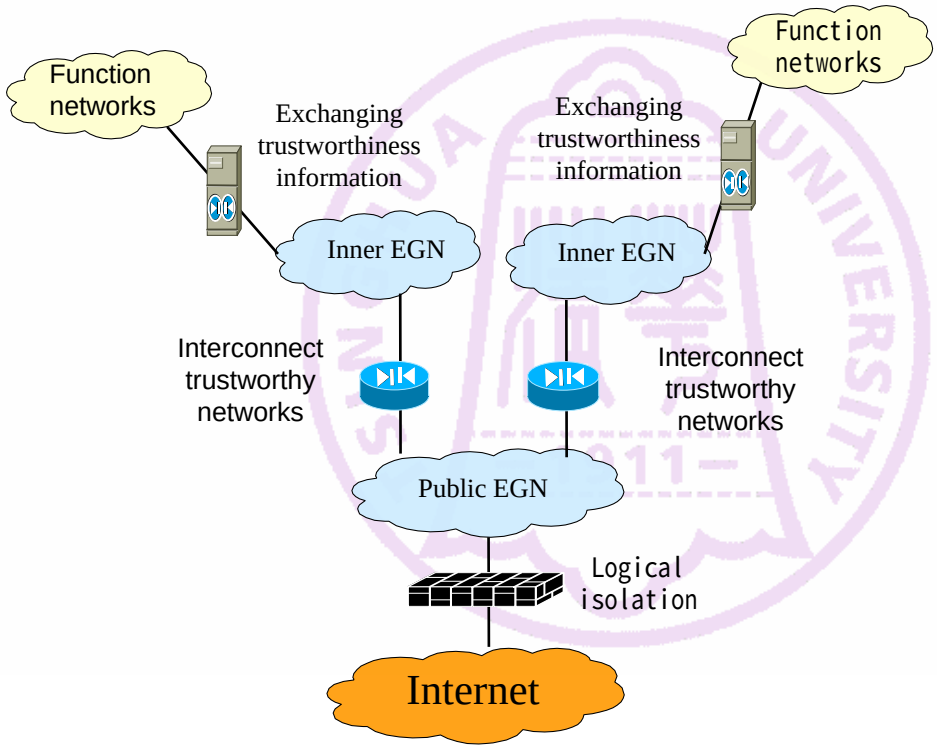
4. Our Investigation Plan

- **Theory and technology of enhancing controllability of trustworthy networks**
  - Controllability model
  - Connect-oriented design
  - High efficient Intrusion-detect
  - Real-time monitor and control approaches to misbehaviors
  - Access control, isolation and remedy



4. Our Investigation Plan

- **Integrity experiment and validation of trustworthy networks**
  - Experiment and validation of trustworthy networks architecture
  - Monitor platform and on-line monitor technology
  - Trustworthy endpoint
  - **Trustworthy e-government networks (EGN)**



4. Our Investigation Plan

Implementation of TNC System based on IXP2350 in Gigabit Ethernet

- Funded by Intel corporation, research council university program.

Thank you

Wish a happy Collaboration