OUTLINE of NICT

~ INTRODUCTION of R&D ACTIVITIES for INFORMATION SECURITY ~

Yuichi Matsushima

Executive Director; Information and Network Systems Department
NICT:
National Institute of Information and Communications Technology
Japan

15 November 2005
Outline

1. Outline of NICT: organization and activities;

2. Overview the Ubiquitous Network Society (UNS) Research Programs by MIC, Japan;


4. R&D Activities for Information Security Center;
1. **Outline of NICT**: organization and activities;

Koganei Head Office
www.nict.go.jp
address: 4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795 Japan
NICT: after merger of CRL and TAO in April 2004
Outline of NICT

- Establishment date: April 1, 2004
- Mid-term plan: April 2001 through March 2006
- Budget & Personnel:
  - Budget: about ¥59.6 billion  (US$ 514 M)
  - Personnel: Full-time employees, about 480
    - Tenure researchers: 305 (Ph.D: 186)
    - Non-permanent researchers: 600 (PD, Graduate students included)
Incorporated Administrative Agency

- Medium-Term Goals (2001-2005)
- President
- Mid-Term Plan (2001-2005)
- Annual Plan
- Operating Expenses
- Review Committee on each IAA
- Policy Evaluation and Evaluation Committee on All IAA

- Commission
- Results reviewed every year
- Opinions on medium-term goals and plans
- NICT

MIC (The Ministry of Internal Affairs and Communications)
Organizational structure of NICT

Top Management
President and 5 Vice-presidents

General Affairs
General affairs
Finance

Intramural R&D
Information and network systems
Wireless communications
Applied research & standard
Basic & advanced research

Extramural R&D
R&D Management
Collaborative Research management

Funding
Key Technology research management
Information and communications promotion

Advisory committee

Partially support this joint conference
International Collaborative Research Grant Scheme
(Advanced Technology Research and Development Grant)

1. Acceptance of Grant Application (Beginning of the FY2006)
2. Proposal of Research and Development Plan
3. Grant Approval
4. Achievement Report
5. Grant Payment (end of the FY2006)

Screening Committee (Outside Experts)

International Collaborative Research Grant
Since 1996

Advanced Technology Research and Development Grant

Communication and Broadcasting Service Enrichment Research and Development Grant for the Senior and the Handicapped
Since 1997

Advanced Technology Research and Development Grant (Telecom Incubation)
Since 1995

• Venture Company
• The Senior and The Handicapped Service Company
• International Collaborative Research Team, etc

Short of money ・
Good idea!
Basic Research, Applied research, and Funding for New Business

Basic Research
Intramural R&D
- High-risk
- Long-term

Applied Research
Extramural R&D
Crossing the Valley of Death
Collaboration with Industries and Universities

New Business
Funding
R&D for New Business
- Promotion

NiCT
2. **Overview of UNS Strategic Programs**

ICT R&D Programs for the Ubiquitous Network Society

- For the **Ubiquitous Network Society (UNS)**
  - Universal Communications
  - New Generation Networks
  - Security and Safety

- The Telecommunications Council; Ministry of Internal Affairs and Communications
- Issued July 2005
**Direction of ICT Research and Development**

**Maintain/improve international competitiveness**

*International competitiveness in ICT*: contribute to the world through playing a leading role in international standardization; create new technology generating a paradigm shift.

*International competitiveness through ICT*: Enhance Japan’s international competitiveness through the advanced use of ICT; develop the world’s leading ubiquitous network society.

**Establish a secure and safe society**

*ICT security / safety*: Ensure the dependability of ICT as a social infrastructure as well as its security / safety.

*ICT for security / safety*: Utilize ICT to solve issues in various fields: healthcare, welfare, food, agriculture, crime prevention, disaster reduction, and the urban / natural environment.

**Promote intellectual dynamism**

*Creating knowledge*: Bring out the potential of individual and promote the creation of value through various areas of knowledge.

*Using knowledge*: Various issues in society can be solved and advanced; easy-to-use services as well as people-friendly communication realized.
Priority Areas in ICT Research and Development

Direction in R&D

- Maintain / strengthen international competitiveness
- International competitiveness in ICT
- International competitiveness through ICT
- Establish a secure and safe society
- ICT security / safety
- ICT for security / safety
- Promote intellectual dynamism
- Creating knowledge
- Using knowledge

Priority areas in ICT Research and Development

- New Generation Networks Technologies
  - Enable Japan to maintain / strengthen international competitiveness in core technologies: optical, mobile, and devices
  - Advanced basic technologies enable Japan to play a leading role in global ICT development

- ICT Security and Safety Technologies
  - Ensure security / safety of ICT networks that are the basis of social and economic activities
  - ICT Technologies to ensure security to realize a safe / secure social environment

- Universal Communications Technologies
  - Content creation technologies promoting intellectual creativity of individuals
  - Communication technologies transcending barriers in language, culture, and physical capabilities

**Communications Research Laboratory (CRL)**
Information and communications crisis management technology, as leading-edge R&D

**Telecommunications Advancement Organization of Japan (TAO)**
Network Security Basic Technology, as practicable R&D

- Training of Researchers
- Research Experience, Highly Neutrality & Publicity
- Using Actual Field Data

**the Information Security Center**
4. R&D Activities for Information Security Center

Objectives

- Build R&D Framework from Basic Leading-Edge Level to an Application Level
- Immediately Carry out the Result of Achievement Into Society
- Promote International Standardization against the World-Wide Information Security Crises
Role of Information Security Center

Role as powerful central force that advances research and development in Japan

Information Security Center

Government

Feedback to National Policy

Support for R&D

Collaboration on R&D

Talent exchange

Sharing of latest information

University and Research Laboratories

Industrial world

Collaboration on R&D

Talent exchange

Security Organizations

Collaboration on R&D
Information Security Unit

- Against cyber attack, to realize function of advanced analysis center and reinforcement technology of network security
- Aiming research & development to become our country bullet, realizing the test bed that such research organization as experimental system for illegal access reproduction
- Researching & developing a code-certification technology, realizing strength maintenance of code in electric government
- Considering telecommunications during emergency situation such as natural disasters, to cooperate and to reinforce realization of big-scale proof field

Information Security Connection Engine

- Telecom-ISAC Japan
  Joint ownership of incident information & analysis technique by ISP
- NIRT
  Research・Report・Advice
  About Information security of Electric government against each Ministry & Government Office
- CRYPTREC
  Objective evaluate of code technology & reliability
- IAA Alliance
  Security of disaster restoration and safety confirmation

NICT & Reflection of Quick Results

Improvement of Security level in our Country

Tight Cooperation
Advanced common security technology for encryption, authentication, etc.

Establishment of security at user level

Establishment of important telecommunications during emergency situations such as natural disasters

Advanced technology for measures against cyber attacks

Establishment of a test bed for R&D on information security

Establishment of security for a ubiquitous environment combining cable and wireless

Establishment of crisis management in terms of telecommunications

Establishment of a test bed for R&D on information security
IAA System

- A system for registering and retrieving victim information by internet at the time of large-scale disasters, and for retrieving with complete agreement of victims’ names or nom de plume.
- Main registering items: victims’ safeties, names (nom de plume), and the others (addresses, blood types, physic characteristics, etc.).
- In examination of systems to use more closely practicing our results to have ever done.

Results (correspondence • practice at the time of the other disasters etc.)
- Sumatra offing earthquake in 2004
- Tokachi offing earthquake in 2003
- Miyagi offing earthquake in 2002
- Synchronized terrorist attacks in USA in 2001

The number of registering/retrieving in Niigata Chuetsu earthquake
Security Integrated Operation Studio, SIOS

To be able to expand each resources connecting with network

→ Realizing nearer realistic environment
  - Reappearing flexibly network organization
  - Taking outside resources in a large scale
  - Tight security

SIOS
(Hardware simulator)

VM Nebula
( Software simulator)

Outside node

Remote control・monitoring system

JGNII

Star BED
(Monster cluster computer)
Log Analysis System

Probe system 

country

Monster collection 
database

Wide-area 
monitoring system 
(Commission Research)

Operation Center 
(ISAC)

Analyzing computer

Advanced Analysis 
Center (Independent Research)

Incident Handling System (IHS) (In Operation)

Researchers

Information Security Service in Telecom-ISAC Japan

Members/ Non-members

### Support of CRYPTREC (Hush Function Connection)

#### A Crisis of Hush Function

A simple version of SHA-1 in August of 2004 (A version which decreased 36 steps to 80 steps) Beginning that a collision between MD4 and MD5 was reported (easy forgery), a crisis of Hush function to be pivot of an electric signature etc.

#### Correspondence in NICT

A cross inspection if reports of the arts & sciences actually influence the users, based on the results, it is contribution greatly to a correspondence policy in CRYPTREC.

<table>
<thead>
<tr>
<th>Applied Examples in Hush Function</th>
<th>Influence Degree</th>
<th>Future Counter Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electric signatures</td>
<td>There is it (under the present conditions, the electric signature method is not recognized except SHA-1)</td>
<td>Installing an anti-public key code measure WG in CRYPTREC, leading the revision of electric signatures methods.</td>
</tr>
<tr>
<td>Time stamps</td>
<td>There is it (Influences to long-time use of time stamp. Time business began since February 7th in H. 17)</td>
<td>Inputting information to Time Business promotion meeting, participate time stamp technologies WG.</td>
</tr>
<tr>
<td>Key joint ownership technology</td>
<td>Small estimate</td>
<td>Inspection of problems in WG of CRYPTREC</td>
</tr>
<tr>
<td>Messages Certification (HMAC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pro-para-random-number generation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
THANK YOU

ICT Value Chain