Final Report

ITU Workshop on " Addressing security challenges on a global scale", 6 December (Afternoon) to 7 December 2010, Geneva

Introduction

ITU has successfully organized a one and half day workshop On “Addressing security challenges on a global scale” at the ITU Headquarters, in Geneva, from 6 (afternoon) to 7 December 2010 prior to the ITU-T Study Group 17 (Security) meeting scheduled from 08 to 17 December 2010.

Participation of this workshop was open to ITU Member States, Sector Members and Associates and to any individual from a country that is a member of ITU who wishes to contribute to the discussions. This includes individuals who are also members of international, regional and national organizations.

The objective of this workshop is to address the main challenges of the ICT/telecommunication security and how ITU and SDOs deal with these challenges.

The workshop attracted 115 participants from 29 countries all around the world.

This workshop is a chance for sharing valuable information and promote increased cooperation between organizations engaged in security standardization with four basic keywords: Sharing, Collaboration, Coordination, and Promotion.

This workshop also provides a good opportunity to overview new areas of security studies including Smart Grid and Cloud Computing.

The final programme, all presentations and all information about the workshop is available at the workshop address:

http://www.itu.int/ITU-T/worksem/security/201012/index.html.

Session 1 : Introduction and Opening Comments

Chairman : Mr. Mohamed M. K. Elhaj (Vice-Chair, ITU-T SG17)

The session started by a word from Mr. Elhaj who officially announce the starting of the ITU-T security workshop that organized by the study group 17 and he welcomes the audiences and thanks them for coming and participating.

Then Mr. Malcom Johnson, the director of the ITU Standardization Bureau, thanks all the participants for coming and thanks the organizers, the moderators and speakers for their contribution, and he wishes a very productive and enjoyable workshop for everyone, Mr. Johnson then emphasizes again that cybersecurity is one of the ITU's top priorities. Then Mr. Johnson speaks about the security new resolutions at the Plenipotentiary Conference, that was held a few weeks ago in Guadalajara, Mexico.

Mr. Johnson also emphasizes the importance of ITU work on standards to address security concerns. At the end of his comments Mr. Johnson congratulates the Chairman of Study Group 17 and his team for assembling an excellent programme of distinguished speakers.

After that Mr. Arkadiy Kremer, Chairman of ITU-T SG 17, welcomes all the participants and thanks them for coming and participating in this very important event. Then Mr. Kremer speaks about the challenges of the Telecommunication security and security standards challenges.

Then Mr. Kremer describes the structure of the workshop and he stated that the workshop will discuss very practical issues on the ICT industry perspectives, like Identity and privacy in ICT, ICT and cloud security, Creation of national ICT security infrastructure for developing countries, Global Cyber security exchange framework, Telebiometrics technology, applications, benefits and standardization, SDOs activity and collaboration in ICT security.

Session 2 : "ICT Industry Perspectives"

Chairman : Mr. Antonio Guimaraes (Vice-Chair, ITU-T SG 17)

Introduction :

ICT security is an essential part of IP-based networks and services development. Integration of ICT and security infrastructures is constantly increasing. Convergence of services where voice, data/video and broadcasting are appearing on all types of network platforms.

Internet is an essential part of ICT infrastructure. Next-generation business model for network operators demands subscriber-centric data consolidation. In this session representatives of ICT industry companies provides new trends and challenges in ensuring confidence and security under using ICT.

This session consists of five presentations as follow:

First presentation: "Cyber Security in the Smart Grid"

Presented by **Mr. George Arnold** (National Coordinator for Smart Grid Interoperability National Institute of Standards and Technology (NIST)).

The electric grid is one of the most complex and important infrastructures ever created, and is vital to modern quality of life and the economy. The basic architecture of the grid has not changed much in 100 years, and use of information technology to increase efficiency and reliability has lagged behind other infrastructures such as telecommunication. The smart grid represents the integration of information and communications technologies into the existing power system to provide measurement and control needed for increased use of distributed and renewable generation, enabling dynamic management of demand as well as generation, improving reliability, and support for electric vehicles.

This presentation describes efforts led by the National Institute of Standards and Technology to address cybersecurity challenges for the smart grid.

Second presentation:

Presented by **Mr. Kim Cameron** (Chief Architect of Identity, Identity and Access Division, Microsoft).

In this presentation Mr. Kim Cameron discusses challenges related to cloud computing environment and its associated business models.

Mr. Kim also presents a cloud identity conceptual architecture and some future perspectives of this technology.

The increasing compliance requirements, some emerging technologies as “Claims-Base Identity” were discussed too.

Third presentation: "National Cybersecurity Management System"

Presented by **Mr. Taieb Debbagh** (Secretary General, Ministry of Industry, Trade and New Technologies, Department of Post, Telecommunications & New Technologies, Morocco).

In this presentation Dr. Taieb Debbagh introduced a comprehensive model for a National Cybersecurity Management System.

This model includes a guide for the development of a National Roadmap of Cybersecurity Governance, a kind of a generalization of ISO 27000 series standards at the national level, consisting of the following components:

- NCSec Framework,
- NCSec Maturity Model,
- NCSec RACI chart, and
- NCSec Implementation Guide.

Fourth presentation: "Securing the Public & Private Clouds"

Presented by **Mr. Mikhail Kader** (Systems Engineer for Security, Cisco Systems, Russia).

This presentation discusses current cloud computing service delivery models. An it analyzes security threats and vulnerabilities related to cloud computing and how they should be addressed.

Fifth presentation: "Security by Design"

Presented by **Mr. Scott Vanstone** (Cryptographic Expert, RIM).

In this presentation Mr. Scott discusses the importance of designing cryptography in from the very start and provides examples were this has been the case and success achieved. He is also speaks about the state-of-the-art in cryptography, why a large part of the world is moving in this direction and how we can provide this new technology on constrained platforms such as smart cards and smart phones.

Session 2 : Highlights, Conclusions and Recommendations:

- The smart grid represents the integration of information and communications technologies into the existing power system to provide measurement and control needed for increased use of distributed and renewable generation, enabling dynamic management of demand as well as generation, improving reliability, and support for electric vehicles.
- Introduction of ICT technologies into the grid presents significant new cybersecurity challenges.
- Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication.
- Cryptography plays a fundamental role in securing information based systems. Often cryptography (and security in general) is an afterthought and as such it is bolted on after the overall system has been completed.

Session 3 : "Identity and Privacy in ICT"

Chairman : Mr. Abbie Barbir (Identity Management Rapporteur, ITU-T SG 17).

Introduction:

Identity Management plays an important role in protecting consumer data and can help to protect their data privacy. If not managed properly, identity management systems can be used to collect personal identifiable information about consumers and organizations.

This session explores available methods, best practices, standards work and identity management techniques such as strong authentication and context aware access controls and its impact on data privacy and telecom networks. The session also investigates work underway in the ITU-T to ensure that identity management systems support privacy with known risk management in particular in relation to cloud computing.

This session consists of six presentations as follow:

First presentation "Open Identity and Open Trust Frameworks"

Presented by **Mr. Don Thibeau** (Chairman and President, The Open Identity Exchange).

This presentation describes the Open Identity Framework created to meet global business to business needs. It also addresses government to citizen applications like those of US government certification requirements of while meeting the privacy requirements of citizens.

This presentation finally shared updates on the status of OIX Trust Framework Working Groups in the telecommunications, research and internet identity markets.

Second presentation "Identity: Enterprise to the Cloud"

Presented by **Mr. Anil Saldhana** (OASIS Co-chair, ID Cloud TC, OASIS ID Trust Steering Committee Member).

Enterprises have invested in solving Identity Management challenges for many years. While they have not fully conquered the field, they have to now deal with rapid advancement of Cloud Computing infrastructures, where different challenges exist.

This presentation discusses the role of Identity as we move from the enterprise to the cloud.

Third presentation "Use of Public Key Infrastructure"

Presented by **Mr. Erik Andersen** (Rapporteur, ITU-T SG 17).

The presentation shortly introduces the basic PKI concepts, including asymmetric keys, certificates, digital signatures, certification authorities, trust anchor, certificate revocation lists, etc.
Many PKI uses are discussed in detailed in this presentation, for example:

- Use of PKI within Identity Management
- Use of PKI for IP Security (IPSec)
- Use of PKI for RFID applications
- Use of PKI within cloud computing

Fourth presentation "A Service and Functions-Based Reference Model for Data Privacy"

Presented by **Mr. John Sabo** (Director, Global Government Relations, CA Technologies).

This presentation provides a detailed discussion of the Privacy Management Reference Model developed by the International Security Trust and Privacy Alliance (ISTPA) and contributed to the OASIS Privacy Management Reference Model (PMRM) Technical Committee, a committee affiliated with the OASIS IDtrust Member Section.

Fifth presentation "Security Aspects of Locator/ID Separation Protocol"

Presented by **Mr. Gregg Schudel** (Technical Marketing Engineer, LISP, Cisco Systems, Inc.).

This presentation provides an overview of security-related implications of deploying Locator/ID Separation Protocol (LISP) from the perspective of the Enterprise.

This presentation then describes the advantages of using LISP such as improved scalability of the routing system through greater aggregation in the location namespace, improved multi-homing efficiency, including ingress traffic engineering, simplified IPv6 transition, and improved endpoint mobility, etc.

Deploying LISP has the potential to provide significantly useful security benefits, such as end-to-end session identification, including source location, spoofed packet protection, and ingress traffic control, including selective source push-back for DoS/DDoS protection.
Deploying LISP also presents potential risks, as it will require additional functionality to be implemented on security devices for them to be aware of or incapable of inspecting packets within the LISP encapsulation header.

Sixth presentation "NemID: An Agile National eID"

Presented by **Mr. Jon Shamah** (European Sales Manager, eSecurity Enterprise Solutions, NETS).

This paper describes the NemID – The Danish National eID program - currently deploying, and shows how a ‘light’ eID can be an advantage in stimulating user acceptance and building critical mass.

Session 3 : Highlights, Conclusions and Recommendations:

- Trusted identities and consumer control of personal information are essential to the effectiveness of transactions on the Internet.
- Trusted frameworks that provide identity assurance are a critical factor in the success of the digital identity ecosystem.
- Public-Key Infrastructures (PKI) is widely used for sure identification in many diverse areas, like e-government, banking, etc. New areas for the use of PKI are emerging.
- Unlike the information security discipline with which it is closely tied, there are no standards-based operational models enabling the development of privacy-compliant technical architectures.
- The Locator/ID Separation Protocol (LISP), currently under working-group development by the Internet Engineering Task Force (IETF), implements a new routing and addressing architecture that splits identity and location into their own namespaces.
- The current Internet routing and addressing architecture overloads the semantics of the IP address by using a single namespace that simultaneously expresses two functions about a device: its identity, and its location.

Session 4.1 : "ICT and Cloud Security"

Chairman : Mr. Koji Nakao (Vice-Chair, ITU-T SG 17 and Vice-Chair of Focus Group on Cloud).

Introduction :

Recently, Cloud computing has rapidly developed and implemented in all over the world. Cloud computing is massively complex systems which can be reduced to simple primitives that are replicated thousands of times as common functional units. In ITU-T, the Focus Group on Cloud computing was established from the standardization view points and within the competences of ITU-T, to identify potential impacts on standards development and priorities for standards needed to promote and facilitate telecommunication/ICT support for Cloud computing and so on. In the FG discussion, Cloud security is one of the major subjects to be studied in ITU-T and is required to analyze security threats and risks, and to investigate security requirements for Cloud computing.

This session brings together some of the key statements involved in the Cloud security area to discuss security technologies/management for Cloud computing in view of Telecom perspective.

This session consists of five presentations as follow:

First presentation "Privacy and Security Issues for Cloud Computing Service"

Presented by **Mr. Heung Youl Youm** (Vice-Chair, ITU-T SG 17).

Privacy is one of the most critical problems for providing the cloud computing service. In this presentation, various privacy threats identified and some security guidelines addressed. In addition, some recommendations of encryption and key management being described for protecting user's privacy. And finally Mr. Youm presents legal risks associated with cloud computing services.

Second presentation "Cardspace in the Cloud"

Presented by **Mr. David W. Chadwick** (Professor of Information Systems Security, University of Kent, Canterbury).

This presentation describes an enhanced information card model which allows a user to click on several cards in a single transaction, whilst only requiring the user to authenticate once per session (instead of once per selected card). In order to facilitate this, the model proposes a new service called the Identity Aggregator. The presentation also describes how we have mapped this model and its protocols onto existing standard protocols, in order to facilitate interoperability between multiple service providers and card issuers.

Third presentation "Cloud Computing and Cybercrime"

Presented by **Mr. Nir Kshetri** (Professor of Business Administration, University of North Carolina, USA).

This paper analyzes how the cloud’s characteristics such as newness, nature of the architecture, and attractiveness and vulnerability as a cybercrime target may help upgrade criminal practices on the Internet to cybercrime2.0. It also investigates how the contexts provided by formal and informal institutions affect security issues associated with data in the cloud.

Fourth presentation "WWRF – Cloud Implications to Security, Privacy, and Trust"

Presented by **Mr. Mario Hoffmann** (Head of Department "Secure Services & Quality Testing", Fraunhofer Institute for Secure Information Technology) and Mr. **Werner Streitberger** (Senior Research, Fraunhofer Institute for Secure Information Technology).

In these days, Cloud Computing is the major outsourcing trend bringing all related technologies, services, and process aspects together in a mature and professional way. The term Cloud Computing refers to infrastructure, platforms, and software which can be rent as a service on demand in a very flexible and dynamic way. The Telco industry is one natural provider of such Cloud services. Some features, however, imply well-known as well as new challenges to security, privacy, and trust. This paper analyses these challenges for Telcos, identifies open issues, and discusses a research roadmap towards secure and trustworthy Cloud Computing for all participants.

Fifth presentation "The Latest Activities on ITU-T Focus Group on Cloud Computing"

Presented by **Mr. Victor Kutukov** (Chairman of ITU-T Focus Group on Cloud).

ITU-T FG Cloud Computing has been established in Feb. 2010 at the last TSAG to identify the study subjects related to Cloud Computing for SGs in ITU-T. After the third FG, the FG meeting has successfully provided their output as a set of materials on Cloud Computing including Cloud Security.

This presentation introduces the latest activities on the FG especially focusing on Cloud Security.

Session 4.1 : Highlights, Conclusions and Recommendations:

- Cloud computing is a double-edged sword from the security standpoint, despite its potential to provide a low-cost security, individuals and organizations may increase risks by storing sensitive data in the cloud.
- New institutions and the redesign of existing institutions needed to confront emerging security and privacy problems.
- Work items for Cloud Security must be encompassed by many domains including Management, Technology, Operations, Educations, Regulations, etc.
- Need of Collaboration among related Working Groups (CSA, ISO/IEC, DMTF, etc.) on Cloud Security could be also recognized.
- The ITU-T FG could provide an initial document for discussion on Cloud Security by the middle of Feb. 2011. The document should be shared among other SDOs as well as SGs in ITU-T in order to jointly and collaboratively investigate targets study issues for Cloud Security Standardization.
- The research leading to enhanced information card model which allows a user to click on several cards in a single transaction has received funding from the European Community's Seventh Framework Programme.

Session 4.2: "Creation of National ICT Security Infrastructure for Developing Countries"

Chairman : Mr. Patrick Mwesigwa (Vice-Chair, ITU-T SG 17).

Introduction:

Practical issues and experience of creation the national ICT security infrastructures for developing countries are discussed at this session.

This session consists of four presentations as follow:

First presentation "ITU-D Question 22 – Building Blocks for Organizing National Cybersecurity Efforts"

Presented by **Mr. James G Ennis** (Department of State, USA and ITU-D Question 22/1 Rapporteur).

This presentation describes in detail the five keys to develop a good national cybersecurity program,

- National strategy;
- Government & industry collaboration;
- Deterring cybercrime;
- National incident management capability; and
- National awareness.

And it describes ITU-D Q22/1 comprehensive report on national best cybersecurity practices.

Second presentation "National IP-based Networks Security Centres for Developing Countries"

Presented by **Mr. Mitry V. Kostrov** (Associate Rapporteur, ITU-T SG 17).

This presentation underscores the need for concerted effort from nations to address the risks associated with globally interconnected networks

Three categories of NCNS services were identified:

- Reactive services;
- proactive services; and
- security quality management services.

Mr. Kostrov then identified a number of challenges faced by developing countries in creating NCNSs such as access to new technologies and training of experts.

Third presentation "How We Work as a National CERT in China"

Presented by **Mr. Yonglin Zhou** (CNCERT/CC, People's Republic of China).

This presentation highlights Internet Development in China which by June 2010, had 420 million internet users.

The presentation also reveals a number of cyber attack incidents experienced in china in the recent past.

Mr. Zhou also describes the role of CNCERT/CC in coordination of national and international efforts related to cybersecurity in China.

Fourth presentation "Raising Awareness for ICT Security Infrastructure Industry-Wide Approach"

Presented by **Mr. Miho Naganuma** (ISOG-J, Q.3 Rapporteur, ITU-T SG 17)

This presentation introduces the new industry-wide approach for information exchanges by Managed Security Service Providers (MSSP), one of major stakeholders for ICT infrastructure, to raise awareness and promote effective incident responses. It also addresses the issues for information exchange through practical activities and highlights challenges to developing countries.

Session 4.2 : Highlights, Conclusions and Recommendations:

- Five Keys to a good national cybersecurity program:
  - National strategy;
  - Government & industry collaboration;
  - Sound legal foundation to fight cybercrime;
  - National incident management capability;
  - National awareness of the importance of cybersecurity.
- It is imperative to share consistent resources including information and technology in a broad range of areas at national level, local community level, and industry level to protect ICT infrastructure.
- It is important to develop an ITU Recommendation on cooperation and security exchange between NCNS (National IP-based Networks Security Centres) and other security bodies and one on architecture of NCNS.

Session 5.1 : "Toward a Global Cybersecurity Information Exchange Framework"

Chairman : Mr. Tony Rutkowski (Cybersecurity Rapporteur, ITU-T SG 17).

Introduction :

One of the most critical and rapidly evolving security challenges today requires a broad consensus on the protocol platforms for the trusted exchange of information necessary for "locking down" the integrity of ICT systems, watching for undesired incidents, and sharing forensics from those incidents. This challenge has engaged the resources of many parties worldwide who are contributing their work and community standards to an initiative facilitated by the ITU-T Cybersecurity Rapporteur Group with an array of new recommendations planned for adoption over the coming months/years.

This session brings together some of the key parties involved in this topical area to describe the development and implementation of the emerging framework.

This session consists of six presentations as follow:

First presentation "Vendor Neutral Security Measurement & Management with Standards"

Presented by **Mr. Robert A. Martin** (Principal Engineer, MITRE, CNIS Group).

This presentation explores how the Making Security Measurable standards being fostered by MITRE and others over the last 10 years are facilitating the use of automation to assess, manage and improve the security posture of enterprise security information infrastructures while also fostering effective security process coordination across the adopting organizations and creating a vendor and tool neutral environment for managing the security posture of an organization.
The basic premise of these efforts is that for any enterprise to measure and manage the security of their cyber assets they are going to have to employ automation. For an enterprise of any reasonable size that automation will have to come from multiple sources and so to make the finding and reporting issues consistent and composable across different tools there has to be an underlying set of standard definitions of the things that are being examined, reported and managed by the different tools.

Second presentation "CSIRT, Information Sharing and You"

Presented by **Mr. Damir Rajnovic** (FIRST SDO Liaison, FIRST).

This presentation has two main goals:

1-To showcase the current state of information exchange among CSIRTS and other teams handling security incidents.

2-To give practical and concrete examples of how participants can get involved and interact with various groups from the community.

This presentation discusses what the CSIRTs doing, as well as what can be expected from them and how to interact with them.

Third presentation "Challenges in Sharing Security Information"

Presented by **Mr. Ian Bryant** (EU NEISAS Project).

This presentation covers the challenges in engendering trust which have to be taken into account when developing structures and mechanisms for sharing security information, and explores the work done by the MS3i and NEISAS Projects in this area.

Fourth presentation "Ontological Approach Toward Cybersecurity in Cloud Computing"

Presented by **Mr. Takeshi Takahashi** (NICT) and **Mr. Youki Kadobayashi** (NICT).

This presentation describes an ontological approach for cybersecurity information sharing, especially for Cloud Computing.

Widespread deployment of the Internet enabled building of an emerging IT delivery model, i.e., cloud computing.

Mr. Takeshi then describes their proposal of an ontological approach to cybersecurity in cloud computing.

Fifth presentation "An Operational Model of CIRT Processes for Improved Collaboration and Capability Development"

Presented by **Mr. Thomas Millar** (Senior Researcher, Analyst & Action Officer, United States Computer Emergency Readiness Team (US-CERT)).

This presentation describes US-CERT approach to a process model and accompanying domain ontology for cyber security incident response, with potential applications for event management and threat analysis, as well as broader risk management functions such as software assurance. The model I presenting differs significantly from similar recent work due to its grounding in real-world CIRT operational processes and decision-making needs.

Sixth presentation "Cyber Defence Data Exchange and Collaboration Infrastructure (CDXI)"

Presented by **Mr. Luc Dandurand** (Senior Scientist, CAT2 - Cyber Defence and Assured Information Sharing NATO C3 Agency).

This presentation outlines the NATO C3 Agency's work on the high-level requirements for an infrastructure to automate the exchange of various data for Cyber Defence purposes. This data includes both operational information on ongoing incidents as well as supporting data such as lists of vulnerabilities, malware, applications, amongst others. The services provided by this infrastructure is intended to be closely integrated into Cyber Defence applications and will include collaboration mechanisms to assist in the refinement of the data.

Session 5.1 : Highlights, Conclusions and Recommendations:

- A consensus emerged that common global protocol platforms for the trusted exchange of information were essential.
- It was plain that the notion of "security by design" is not a reasonable objective today, as the systems are too complex and constantly changing.
- What is necessary is putting into place the means to:
    - Know your weaknesses;
    - Minimize the vulnerabilities;
    - Know your attacks; and
    - Share the heuristics within trust communities.
- The sharing of information about the security risks facing networks is self evidently beneficial to both government and industry.
- Albeit cloud computing-based services have rapidly developed, their security aspects are still at the initial stage of development.
- Information security measurement and management, as currently practiced, is complex, expensive, and fraught with unique activities and tailored approaches.
- To support organizational discipline and accountability objectives while enabling innovation and flexibility, the security industry needs to move to a vendor neutral security management and measurement strategy that is agnostic to the specific solution providers while also flexible enough to work with several different solutions simultaneously.
- There are two main objectives that are always present in cross-CSIRT incident response:
    - Contact an individual or an organisation outside of your own organization.
    - Exchange information in order for the incident to be handled.

Session 5.2 : "Telebiometrics: Technology, Applications, Benefits and Standardization"
Chairman : Mr. Hakil Kim (Telebiometrics Rapporteur, ITU-T SG17).

Introduction :

While biometrics is a method of authentication which overcomes weaknesses of traditional authentication methods such as passwords or keys, Telebiometrics is an emerging technology for authentication of humans at remote sites using biometrics in the telecommunication environment. The application domain of Telebiometrics has been growing from Tele-banking to Telemedicine. Since the Question for Telebiometrics has been established at ITU-T SG 17 in 2003, there have been 10 Recommendations published including 3 Amendments and 12 Recommendations under development. Even though more than 20 experts from 7 different nations have participated in its development, the Telebiometrics is still unacquainted to many other Questions in ITU-T SG 17 and even new technology to most of the developing countries. This session introduces broad knowledge about current and future works on Telebiometrics, and provides guidelines and case-studies of use of the Telebiometrics standards into privacy protection requested services in various countries.

This session consists of six presentations as follow:

First presentation "Remote Clinical Examination: the Key Issue of Telemedicine"

Presented by **Mr. Enrico M. Staderini** (Western Switzerland University of Applied Science, Switzerland).

In this paper the author is proposing a sort of roadmap to enhance collaboration and coordination to promote telemedicine as an integral part of the medical profession based on robust and rigorous methodology, standards and philosophy.

Second presentation "Developing a Framework for Health IT standardization"

Presented by **Mr. Arturo Serrano** (CICESE Research Center, Mexico).

In this presentation Mr. Serrano emphasizes the important of developing a comprehensive standards framework for Health IT and he proposed in this contribution the incorporation of three elements in this framework which, he believes, are key to improving the Health IT services in developing countries: adoption and usability factors, innovation strategies and sustainable development factors.

Third presentation "Integrated Framework for Telebiometric Data Protection"

Presented by **Ms. Yong Nyuo Shin** (Hanyang Cyber University, Korea).

In this presentation Ms. Shin provides an integrated framework for protection of biometric data and private information in Telehealth. She defined a model of health services using Telebiometrics for user identification and authentication. This system identifies the threats in transmitting various sensory data related to human health and provides the countermeasures for secure transmission when applying this integrated framework.

Fourth presentation "Telebiometrics Applications"

Presented by **Mr. Yoshiaki Isobe** (Hitachi, Japan).

This presentation introduces the vein biometrics technologies, some security technologies with template protection technique for biometrics and those applications. And it introduces relationships of ITU-T Telebiometrics Recommendations and the telecommunication systems.

Fifth presentation "Biometric Information Protection Standard in ISO/IEC JTC 1 SC27"

Presented by **Mr. Myung-Geun Chun** (Chungbuk National University, Korea).
ISO/IEC JTC SC27 has been preparing a standard which will provide guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. The standard also describes the relationship between the biometric reference and other personally identifiable information (PII). The increasing linkage of biometric references with other PII and the sharing of biometric information across legal jurisdictions make it extremely difficult for organizations to assure the protection of biometric information and to achieve compliance with various privacy regulations. Therefore, this standard also provides guidance on requirements on the secure and privacy-compliant management and processing of biometric information and also clarifies the responsibility of the biometric system owner.

Session 5.2 : Highlights, Conclusions and Recommendations:

- Telebiometrics is wide-spreading all over the world as a convenient and secure user authentication method in various privacy protection requested telecommunication applications such as Telehealth.
- Standardization is one of the most important factors for Telebiometrics to be more prevailing inter-nationally.
- SG17 Q.9 expects more recognition and participation from more countries and increasing adoption of Telebiometrics .
- Patient-physician interaction in remote clinical examination poses important challenges if the standard clinical examination paradigm (and associated reliability) is to be granted.
- Communication standards and Telebiometrics standards will foster best practices in telemedicine.
- It is time to develop a comprehensive standards framework for Health IT based in the collaborative work of IT research institutions, governmental and private health institutions and physicians involved in Health IT practices in both urban and rural locations.
- Security technologies are required to protect remote medical systems vulnerabilities, while effectively safeguarding it against external attacks and personal privacy should be assured.
- To provide stable biometric telemedicine and telehealth services, user authentication and service aspects should be considered.
- Appropriate countermeasures to safeguard the security of a biometric system and the privacy of its data subjects are essential.

Session 6 : "SDOs Activity and Collaboration in ICT Security"
Chairman : Mr. Herb Bertine, (former Chairman, ITU-T SG 17).

Introduction :

This session will use a roundtable discussion to explore the critical ICT security areas where standardization is urgently needed, what various SDOs are doing in the high priority areas, what collaboration initiatives are in place, and future opportunities where collaboration would be helpful.

Presenters and Panelists :

George Arnold (Chairman, SAG-S)
Walter Fumy (Chairman, JTC 1/SC 27)
Tim Polk (Security Area Director, IETF)
Carmine Rizzo (Security Coordinator, ETSI)
Anil Saldhana (Co-chair, OASIS)
Markus Wong (Security Group Vice-chair, 3GPP)
Jianyong Chen (Vice-Chair, ITU-T SG 17)

This session consists of two parts, in the first part a brief presentation was given of each SDO that covered :

- Scope of ICT security work;
- Major accomplishments;
- Future directions.

In the second part a roundtable discussion :

- Critical gaps, standardization priorities;

- Collaboration, cooperation;
- Improving usefulness of standards, metrics.

Views expressed during the roundtable include:

- Critical ICT security gaps, standardization priorities :
  - Educating people of the importance of security for their work;
  - Helping others to incorporate security in their work.
  - Solving scalability issues;
  - Building in extensibility in protocols so that they can evolve without breaking to counter new threats;
  - Extending security work to wireless;
  - Addressing human factors, probably the weakest link;
- Collaboration, cooperation :
  - Successful collaboration requires commitment;
  - Collaboration works best where members are active in both groups;
  - Cross referencing of specifications is part of collaboration
  - ITU-T has tools to facilitate collaboration including JCAs, FGs, roadmaps, etc.
  - Important opportunity is with organizations where ICT security is not their core business, while recognizing it takes effort due to different cultures when crossing domains
  - Collaboration needs to start in home companies that participate in multiple SDOs;
- Improve usefulness of standards, metrics :
  - Difficult up-front to determine ultimate usefulness but some upfront efforts to determine level of commitment and business value have been useful;
  - Some simple metrics are hits/downloads of standards, number of references to the standard by others, number of volunteers actively contributing to development and does it change during development process, number of implementations under test (and feedback from these tests);
  - Ultimately, is it widely implemented, deployed and used – the marketplace will decide;
  - Differing views regarding shutting down work viewed as unlikely to succeed.

Session 7 : Closing Comments, Recommendations, Discussion

Chairman : Mr. Mohamed M. K. Elhaj (Vice-Chair, ITU-T SG 17)

Co-Chairman : Mr. Reinhard Scholl (Deputy to the Director of TSB)

Panelists:

Antonio Guimaraes (ITU-T SG 17 Vice-chair)
Abbie Barbir (ITU-T SG 17 Identity Management Rapporteur)
Koji Nakao (ITU-T SG 17 Vice-Chair and Vice-Chair of Focus Group on Cloud)
Patrick Mwesigwa (ITU-T SG 17 Vice-chair)
Tony Rutkowski (ITU-T SG 17 Cybersecurity Rapporteur)
Hakil Kim (ITU-T Telebiometrics Rapporteur)
Herb Bertine (Former Chairman, ITU-T SG 17)

In the closing session Mr. Elhaj congratulates the TSB, SG17, Workshop Steering Committee, Sessions Coordinators and Speakers for their excellent job, and he thanks the audiences for coming and contributing.

Then sessions chairs presented a brief presentation about their sessions. The last part of this closing session was the Comments and Questions from the audiences.

Mr. Scott then officially ended the security workshop wishes all the success in the SG17 meeting.

_____