ITU Workshop on "New challenges for Telecommunication Security Standardizations"
9 (Afternoon) to 10 February 2009, Geneva
Final Report

Introduction

ITU has successfully organized a two days workshop On "New challenges for Telecommunication Security Standardizations" at the ITU Headquarters, in Geneva, from 9 (afternoon) to 10 February 2009 prior to the ITU-T Study Group 17 (Security) meeting scheduled from 11 to 20 February 2009.
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 present telecommunication security as an essential part of the IP-based networks and IP-based services development. Integration of telecommunication and information security infrastructures is constantly increasing. The workshop was also provided an opportunity for discussions on the C2 (Information and communication infrastructure) and C5 (Building confidence and security in the use of ICTs) WSIS Action Lines to learn about main development trends and practical issues in these areas.
In addition, the workshop is seen as a follow-up of the Workshop on "New Horizons for Security Standardization" held in Geneva (3 - 4 October 2005) and of the side-event on cybersecurity held at WTSA-08 (23 Oct. 2008) in Johannesburg; and also a good opportunity to review the achievements of the ITU-T work on security in the last study period and in analyzing the new work programme resulting from the decision made at WTSA-08.
The final programme, all presentations and all information about the workshop is available at the address http://www.itu.int/ITU-T/worksem/security/200902/

Opening Session

The session started by a word from Mr. Reinhard Scholl, deputy to Director, Telecommunication Standardization Bureau (TSB), who stressed on the importance of this workshop for the global world and specially for developing countries, then Mr. Alexander Ntoko, Head, Corporate Strategy Division, SPM Dept., ITU, thanks all audiences for coming and participating in this workshop and he said that he is just back from two events concerning security and on those events he learnt more than ever before the importance of standards to all ICT and specially to security.
Then Mr. Arkadiy Kremer, Chairman, ITU-T SG 17, thanks all the participants for coming despite the late invitation, and he is officially opened the workshop.

Session 1: "Networks, users, services and information as protected objects"
Chairman: Mr. Bill McCrum, (Industry Canada)
The objectives of this session are to explore the challenges in protecting public services accessed over public networks and it provides insights into new business models for network operators in light of both the need for more security and protection and the current disruptive drivers stemming from

convergence of services where voice, data/video and broadcasting are appearing on all types of network platforms.

This session consists of two presentations as follow:
First presentation: "From Public Networks to Public Services"
Presented by **Mr. Vladimir Belenkovich**, (AGCom, Russia)
This presentation describes a paradigm shift in the telecom world, which was initially seen mainly as the transition from the circuit switching to the packet switching, from TDM to VoIP, and its impact on networks and services designers and providers. The architecture of the underpinning network fabric is rapidly changing along with the new network technologies, and the service architecture and business architecture are moving to the focus of the public services area stakeholders. The carriers' networks do not provide yet full support and coverage for the new services already successfully tested and deployed in the public Internet space. In the future in order to be part of the Big Game coming, Network Service Providers need to adopt to the new inter-networking architecture, streamlined for added value, in order to retain their customers. The governments, both as service providers and as regulators, also have their own view of the new emerging world of services.

The second presentation: "New Business-Models for Network Operators"
Presented by **Mr. David Goodman**, (Profile Product Line Manager Subscriber Data Management, Converged Core Nokia Siemens Networks)
Mr. Goodman explains his vision on the business model of the telecommunication industry by the year 2015, when the whole world will be connected, and the challenges that will face the operators specifically.
And he concluded by saying that the next-generation business model for network operators demands subscriber-centric data consolidation to:

- Improve CAPEX/OPEX
- Improve time-to-market with new services
- Leverage subscriber loyalties
- Encompass Web 2.0/Telco 2.0 opportunities particularly through identity management-based services

Session 1, Highlights, Conclusions and Recommendations:

- In near future operators should fundamentally change the way they build networks and services;
- Service oriented architectures – is the name of the new challenge;
- Next-Generation business model for network operators demands subscriber-centric data consolidation;
- Network agnostic IdM is a key priority for trust/privacy/security concerns.

Session 2: "ITU Information Security Initiatives"
Chairman: Mr. Mohamed Elhaj, (Vice-Chair, ITU-T SG 17)
The objectives of this session are to provide in detail some of the ITU information security initiatives and discuss the usage of security standards in

business today. Furthermore, it presents international collaboration for national public networks security. This session also presents testability guides and techniques for ITU recommendations.

This session consists of three presentations as follow:
First presentation "Business use of telecommunication security project"
Presented by **Mr. Patrick Mwesigwa**, (Vice-Chair, ITU-T SG 17)
Mr. Mwesigwa described a new initiative that is proposed by SG17 to prepare a report on "Business use of telecommunication security standards", this report will consist of summary sheets for analysed security standards, these summary sheets will be prepared by security experts from organizations working on the field.
Mr. Mwesigwa described in detail the criteria to be applied in developing this report and he asked ITU to provide the financial and technical support for this project.
Then Mr. Mwesigwa spoke about the importance of using standards in a real application world.

Second presentation "Providing Testability for ITU Recommendations"
Presented by **Mr. Ostap Monkewich**, (Consultant, Industry Canada)
The presentation looked at recommendations from the point of view of conformance and interoperability testing of products that implement ITU-T recommendations. It addressed why we need to test, the kinds of testing that is relevant, the expected quality of test results and what companion recommendations are needed for each base recommendation we develop. It pointed to the existing recommendations that prescribe these additional requirements and the means for developing higher-quality recommendations. At the end of the presentation Mr. Monkewich gave all references needed to develop high-quality recommendations and test specifications

Third presentation "International collaboration for national public networks security"
Presented by **Mr. Antonio Guimaraes**, (Vice-Chair, ITU-T SG17)
This presentation is an overview of WTSA-08 resolutions related to telecommunication security, followed by a more detailed analysis of a recommended security baseline for national public networks operators. These proposals cover aspects of operators' policy, technical tools and collaboration baseline. Finally, the ITU role in organizing and coordinating the international collaboration for national public networks security is discussed.

Session 2, Highlights, Conclusions and Recommendations:

- SG17 rising an initiative to prepare a report "Business use of telecommunication security standards", many benefits can gained by this report especially for developing countries, technical contributions from experts will be crucial for its success;
- Business and governmental bodies need to learn more about standards from their business applications rather than only from a technical point of view;

- A high-quality recommendations are needed to get a high quality test results;
- Network operators must have information security provisions compliant with legal and regulatory requirements and should adopt a security polices based on best practices;
- Operators should apply at least basic technical orientations, and collaboration among all stakeholders should be guaranteed;
- ITU has very useful security initiatives like Global Cybersecurity Agenda and Cybersecurity Gateway;
- TSB and BDT should work closely to support the creation of national computer incident response teams, where needed and are currently absent.

Session 3: "Cybersecurity"
Chairman: Mr. Koji Nakao, (Vice-Chair, ITU-T SG 17)
The objectives of this session are to share enlarging and diverse threats over the cyberspace such as Botnets, Virus, SPAM and DDoS and to further provide the current cybersecurity technologies against those cyber-threats. This session also focus on seeking interesting topics to be discussed for ITU-T standardizations in an arena of cybersecurity.

This session consists of three presentations as follow:
First presentation "Best practices for organizing national cybersecurity efforts'
Presented by **Mr. James Ennis**, (US Government)
The presentation described IP-based networks as a critical part of national economic infrastructures today. One way that IP-based networks add value to a national economy is by facilitating commercial activities in all other national economic sectors.
Because the Internet and other IP-based networks are global, the problem is also global. That is to say, instituting good cybersecurity practices in one country has a limited effect as long as other countries do not also institute good cybersecurity practices. Therefore, it is in the interest of all countries to work together to achieve global cybersecurity.
The ITU is addressing this problem in a number of ways. One way is to reach out to the developing world to assist developing countries to develop national cybersecurity programs based on best practices. One high level effort in this regard is found in the work of Question 22 of Study Group 1 of the ITU Development Sector. Q22 is developing a report on national best cybersecurity practices.
Mr. Ennis described the contents of the report including two annexes that discuss spam and Identity Management and an extensive list of references and links to places where additional information on these topics can be found.

Second presentation "IP NGN Security Framework"
Presented by **Mr. Mikhail Kader**, (Cisco)
Mr. Kader described how maintaining service predictability is a primary challenge faced by today's service providers in the presence of an outbreak of malicious traffic sourced. In today's terms, this type of behavior has been

identified with threats such as distributed-denial-of-service (DDoS) attacks, turbo worms, e-mail spam, phishing, and viruses. The amount of traffic generated by infections and subsequent outbreaks can disrupt the normal operation of a modern network. Security has become a critical characteristic of all services and is essential to the profit line of service providers. The presentation discusses how to maintain heightened network security, transition from the traditional reactive stance to an incrementally proactive stance by reducing windows of vulnerability, improving reaction times, and effectively mitigating attacks.

Third presentation "Fighting Cybercrime in 2009"
Presented by **Mr. Magnus Kalkuhl**, (Virus Analyst, Global Research and Analysis Team Kaspersky Labs GmbH)
Mr. Kalkuhl compared malware in the past by modern malware and described how it does more than just infecting a couple of files for the fun of it's author. Nowadays, malware is written for profit. Mr. Kalkuhl showed how this illegal business works and what can be done in order to protect the internet and its users.

Session 3, Highlights, Conclusions and Recommendations:

- ITU-D Q22/1 is developing a comprehensive report on national best cybersecurity practices this report is also containing two annexes provide introductions to concepts of SPAM and Identity Management;
- Today, all critical sectors of economy rely on IP networks for transacting business, government services, etc. IP networks, not designed to be secure, face increasing numbers of cyber attacks;
- To maximize the value IP networks can add to a national economy, they must be reliable, secure, & trusted;
- 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.
- Today's threats are becoming more professional and mainly targeting money gain;
- Security helps meet all key business goals and objectives for service providers;
- Migration to 3.5G or IP networks brings changes threat landscape hence a Risk Analysis is necessary;
- Define a security model to reach operational excellence based on security policies and process gaining enhanced visibility, control and high availability;
- Cybercrime business is organized, but more as “crime that is organized” rather than “organized crime”;
- Antivirus companies can protect servers and client computers against initial infections, and also they can exchange information with CERTs, authorities and researchers;

- International Cyberspace police who is able to act quickly in cases of emergency can also help;
- It is further required for SG17 to study especially on "packet inspection technology" in collaboration with the work in SG13.

Session 4: "Secured applications"
Chairman: Mr. Heung Youl Youm, (Vice-Chair, ITU-T SG 17)
This session is to address a number of key technical topics in order to identify the possible gaps and determine future direction for standardization work in the secured applications area including the future of internet security.

This session consists of three presentations as follow:
First presentation "Secure Mobile Banking as Telecommunication Operator Service"
Presented by **Mr. Igor Milashevskiy**, (INTERVALE)
This presentation described the importance of having a secure transaction exchange environment in order for a mobile terminal to act as a payment or banking terminal. The implementation of such solutions leads to an effective extension of a banking infrastructure to all mobile terminals, which enables quicker adoption of banking services and makes financial environment potentially less conductive to fraudulent and disruptive activities.
A critical element needed to establish such mobile payment system is a robust interface between the banking system and mobile telecommunications networks, which will provide a binding and secure link between a person identity and a mobile subscriber identity.
The existing infrastructure of secure key storage and cryptographic calculation provided by the Subscriber Identity Module (SIM) / Universal Subscriber Identity Module (USIM) / Removable User Identity Module (RUIM) used in today's mobile networks, on one side, and standard cryptographic Hardware Security Modules (HSM) used in modern banking systems, on the other side, can enable identity authentication within such solutions, combining security, reliability and non-repudiation. The importance of the security framework for a secure mobile banking was stressed.

Second presentation "Future Internet Security"
Presented by **Mr. Michel Riguidel**, (Telecom ParisTech, France)
Mr. Riguidel in his presentation said that the current internet was unable to adapt either to mobility, or to modern security. He added, the internet of the future will be polymorphous, created on the basis of different infrastructures. It is necessary to incorporate the split, the dynamic and evolving nature of digital systems. Our current information technology paradigms are in the process of being dissolved. The dichotomies between computer and networks, between hardware and software, between applications and services, between the logical and the virtual, between software and information, are in the process of being blurred or, more precisely, the terms of the caesura are radically changing meaning. The road map for the network architecture is following the same itinerary as the history of computer languages. It was recognized that the security, dependability, privacy, and trust should be taken

into account upfront when the future internet is designed and it was recognized to define the trust management infrastructure when designing the future internet security.

Third presentation "ITU-T Security Standardization on Mobile Web Services" Presented by **Mr. J.S. Lee**, (ETRI, Korea)
Mobile industry is adopting Web Services technologies to the mobile domain since they can solve integration problems between operators, service providers, and content providers. Security is one of the important issues in the adoption of Web Services in the mobile environment, and this presentation provided a summary of standardization activities related to Mobile Web Services security in ITU-T SG17 focusing on X.1143(X.websec-3). X.1143 describes the security architecture and security service scenarios for message security in mobile Web Services. This presentation also briefly introduced X.websec-4 which is in the early stage of standardization in ITU-T SG17. X.websec-4 describes security threats and security requirements of the enhanced Web based Telecommunication Services.

Session 4: Highlights, Conclusions and Recommendations:

- Creating effective mobile Web Services requires an architecture that addresses issues related to Security and Identity Management;
- It is possible to use the following cryptographic infrastructures in the secure mobile banking;
    - Subscriber Identity Module (SIM) / Universal Subscriber Identity Module (USIM) / Removable User Identity Module (RUIM) used in today's mobile networks, or
    - Standard cryptographic Hardware Security Modules (HSM) used in modern banking system.
- The key elements such as future web, computational cryptography, privacy, virtual world, language evolution, and network evolution, should be investigated for designing future Internet;
- The current internet has several drawbacks; lack of security, lack of mobility, lack of ensuring privacy, and lack of trust.
- Web technologies such as SOA, Web 2.0, and mashups are being applied to telecommunication domain including mobile services;
- It is recognized that the security, dependability, privacy, and trust should be taken into account upfront when the future internet is designed.
- ITU-T SG17, especially WP2/SG17, is required to continue to develop the draft recommendations in the area of application security, as the security for various applications is so critical and there are still significant gaps.
- Security framework for a secure mobile banking system should be developed by global SDOs, especially ITU-T, for a global interoperable operation.

Session 5: "SDOs' security standardization, implementation and evaluation strategy"
Chairman: Mr. Herb Bertine, (former Chairman, ITU-T SG 17)
The objectives of the session are to provide an overview of key security standardization activities in Standards Development Organizations and to identify which issues are amenable to a standards-based solution and how standards organizations can most effectively play a role in helping address these issues. Furthermore, to consider how standards organizations can collaborate to improve the timeliness and effectiveness of security standards and avoid duplication of effort.
This session consists of four presentations covering security standards work in ISO/IEC JTC 1/SC 27, ETSI, 3GPP SA3 and ITU-T.
First presentation "ISO/IEC JTC 1/SC 27 - IT Security Techniques"
Presented by **Mr. Walter Fumy**, (ISO/IEC JTC 1/SC 27)
Mr. Fumy in his presentation described JTC 1 Sub-Committee 27 as a primary resource of International Standards on application-independent IT security techniques. The group has developed many specifications and guidelines already in use by commerce, industry and government. Major achievements range from cryptographic techniques to security management guidelines and security evaluation. By continuously enhancing its work program and taking on board the latest in business practice (such as privacy technology and Identity Management), new and emerging threats and risks, as well as advances in technology, SC 27 is well positioned to shape the future of IT security.
Regarding coordination, Dr. Fumy noted that given the limited availability of resources for the development of security standards, we must avoid duplication of effort and make use of effective cooperation and collaboration. And that given the vast number of activities in the area of security standards, we must bring together information about existing standards, standards under development, and key organizations that are working on these standards.

Second presentation "ETSI Security Standardization"
Presented by **Mr. Carmine Rizzo**, (ETSI)
The presentation provided an overview of security issues covered by ETSI. The increasing complexity and rapid development of new systems and networks, the sophistication of changing threats, and the presence of intrinsic vulnerabilities present demanding challenges for the Information society in its efforts to secure ICT systems and networks against the threats and related risks to which they are subject. To minimize exposure to risks, security must be built in from the beginning when designing new architectures, and not added on at a later stage as an optional feature. In such a challenging scenario, information security standards are essential to ensure interoperability among systems and networks, compliance with legislations and adequate levels of security, thus creating a more secure and profitable environment for the industrial sector from SME to large global companies, as well as benefits for governmental organizations, research bodies and universities.
ETSI has two important security coordination activities: an operational co-ordination ad hoc group on security and a horizontal co-ordination structure for security issues. Four future challenges were highlighted: prioritization in

security standardization, security metrics, privacy, and how to "evaluate" security standards in implementations.

Third presentation "3GPP SA3 status"
Presented by **Mr. Valterri Niemi**, (3GPP SA3, Chairman)
In his presentation Mr. Niemi explained the scope of the 3rd Generation Partnership Project (3GPP) which is "to produce Technical Specifications and Technical Reports for a 3G Mobile System based on evolved GSM core networks and the radio access technologies that they support." His presentation also described security integrated and updated for each release of the 3GPP.
Mr. Niemi gave an example set of security threats: compromise of credentials (e.g. cloning of credentials), physical attacks (e.g. physical tampering), configuration attacks (e.g. fraudulent software updates), protocol attacks (e.g. man-in-the-middle attacks), attacks against the core network (e.g. denial of service), attacks against user data and identity privacy (e.g. by eavesdropping), and attacks against radio resources and management.

Fourth presentation "ITU-T Security Standardization"
Presented by **Mr. Arkadiy Kremer**, (Chairman, ITU-T SG 17)
The presentation provided an overview of key security standardization activities in the ITU-T SG 17. The presentation explained the mission and advantages of the ITU in ICT security standardization as the only global intergovernmental and industry collaborative technical organization. Collaboration with the other SDOs will present as a key for the work on security standards to improve the timeliness and effectiveness and avoid duplication of effort.
Mr. Kremer concluded by making the following 6 points:

- Need a common vocabulary for cybersecurity – among technical, business, legal, evaluation, and standards
- Necessary to assure continued relevance – keep standards current
- Attention needed on trust between operators and vendors
- Elaboration of security methodologies and procedures are necessary for compliance in the network infrastructure
- Need to understand security standards from a business application viewpoint; e.g., to support procurement strategies
- Need to support work on conformance and interoperability testing of implementations of security standards

The session discussion period raised the following as items to think about:

- Strategy for security standardization
- Prioritization of security standardization
- What new things can be done to improve cooperation and avoid duplication and gaps in security standardization?
- Should an oversight entity be created across standards bodies
- "Seal of approval" for security standards
- Security standardization must be a continuing process

Session 6: "Identification Services"
Chairman: Mr. Jianyong Chen, (Vice-Chair, ITU-T SG 17)
The objectives of this session are to address current key challenges of Identity Management and its global vision in the future and to discuss standardization activities in this area in order to identify the future standardization work in ITU-T.

This session consists of three presentations as follow:
First presentation "Identity Management"
Presented by **Mr. Tony Rutkoswki**, (VeriSign)
Identity Management is the foundation and core for all telecommunication/ICT security. The explosively expanding and vast array of "network nomadic" individuals, providers, and objects has challenged our ability to effectively manage their identities and trust anchors. This presentation described these Identity Management challenges and the current global ecosystem of related work and activities, including a set of unique and critically important initiatives underway in the ITU-T designed to address those challenges. The presentation concluded with a global vision of Identity Management capabilities for 2009 and beyond that promise substantial enhancements for telecommunication/ICT security.

Second presentation "Identification Services as provided by directories (X.500 incl. X.509)"
Presented by **Mr. Erik Andersen**, (Rapporteur, ITU-T SG 17)
Identification services are essential within several IT-security areas. Secure identification is required for protecting of information against misuse, malicious modification, destruction of information and for preventing spiteful and unwanted use of services. The X.500 Directory specification provides means for storing identification information and it specifies elaborate mechanisms for protecting such information. In addition, X.509 provides specification for secure authentication and authorization also to be used outside the strict areas of directory. X.509 also provides specifications for how to establish the necessary infrastructure for providing secure authentication and authorization.

Third presentation "Trend in User-Centric Identity Management Technology"
Presented by **Mr. Sang Rae Cho**, (ETRI, Korea)
This presentation provided a brief summary on how IdM technology has been evolved and why current IdM technologies have focused on three different aspects: user-centric, network-centric and application-centric. The presentation also explained the current standardization effort in ITU-T and other Standardizations Development Organizations. At the end, brief idea and concept of Digital Identity Wallet be explored to demonstrated the state-of-art IdM technology.

Session 6: Highlights, Conclusions and Recommendations:

- Identity Management is the foundation and core for all telecommunication/ICT security;
- Object Identifiers becoming increasingly important for

    - Network elements (especially forensic acquisition locations in a network);
    - Terminal devices, software, RFID tagged objects, sensors, biometric scanners, e-health, power management, and intellectual property.
- Number of a big companies uses Lightweight Directory Access Protocol (LDAP is a dear child of X.500) as major component in their IdM solutions (like Microsoft, IBM, Novell, Oracle, Sun and Siemens)
- The main challenges regarding X.500 are:
    - Extending X.500 support to meet new Identity Management requirements;
    - Make the community aware of the X.500 capabilities;
    - Get new blood into the process.
- **Main functions of Digital Identity Wallet are:**
    - Site registration and authentication;
    - Identity share and synchronization;
    - User privacy protection;
    - Mobile Digital Identity Wallet.

Closing session

The closing session started by words from the session chairmen concluding their session presentations and highlighting the hot issues, then Mr. Reinhard Scholl, Deputy to the Director, Telecommunication Standardization Bureau (TSB), emphasized again on the importance of information security in our lives and thanked all the audiences.

Then Mr. Alexander Ntoko, Head, Corporate Strategy Division, SPM Dept., ITU, thanked all the participants for being here with us discussing this very important topic of security which is on a very high priority and it is one of the seven strategic goals of the World Summit on the Information Society (WSIS) he also stressed on the role of standards.

At the end of his word Mr. Ntoko wished all the success to the study group 17 on its new study period and, because of the importance of the SG17 meeting which will be starting from 11 to 20 of February, he ensured that the Secretary General of the ITU will attend the closing session of the meeting.

Then Mr. Arkadiy Kremer, Chairman, ITU-T SG 17, thanks all the speakers, chairmen and all participants and he sent special thank to Judith for her endless effort to organize the workshop, then he is officially closed the workshop.