



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



RECENT SECURITY DEVELOPMENT

ABSTRACT

The standards activities in ITU-T Study Group 17 (SG17) on Security, languages and telecommunication software were previously reported at the 2nd RAISS Forum meeting in Singapore. This report aims to update and summarize the current activities on the work of respective Questions in SG17.

1. Roles of Security Questions in ITU-T SG17

Study Group 17 has been designated the Lead Study Group (LSG) for **Telecommunication Security** in ITU-T. LSG is responsible for the study of appropriate core Questions¹. Activities of the LSG for Telecommunication Security may be categorized as core activities centered on defining and maintaining an overall security framework and project management involving the coordination, assignment and prioritization of efforts that would lead to timely communication system security Recommendations.

For the period of 2005 to 2008, Question 4/17 under SG17 has been identified as the coordinator for LSG for Telecommunication Security activities. This effort will be carried out closely with other Study Groups to identify and develop security solutions. Specific expertise to integrate these solutions with the technology under development, however, is available only from the Question developing the Recommendations for the Question. There is no plan for SG17 to develop specific cryptographic algorithms, register cryptographic algorithms, or certify the security of specific systems. All Study Groups are requested to keep SG17 informed of their work plans regarding security so that they can be integrated into the overall security work programme.

There are currently seven Questions allocated to SG17 and the latest updates, including their respective objectives and recommendations to be established are described in the following sections.

¹ In ITU-T, a Question is a topic of interest in which a working group is formed to establish appropriate recommendations for its resolution.

2. Latest Activities in SG17

2.1 Question 4/17: Communications Systems Security Project

2.1.1 Objectives

This Question is to develop a vision for ITU-T security and to act as the lead group on all communications security project-level issues for ITU-T.

2.1.2 Summary of Candidate Recommendations

1) X.sbno, Security baseline for network operators

This Recommendation defines a security baseline against which network operators can assess their network and information security posture in terms of what security standards are available, which of these standards should be used to meet particular requirements, when they should be used, and how they should be applied. This Recommendation describes a network operator's readiness and ability to collaborate with other entities (operators, users and law enforcement authorities) to counteract information security threats. This Recommendation can be used by network operators to provide meaningful criteria against which each network operator can be assessed if required.

2.2 Question 5/17: Security Architecture and Framework

2.2.1 Objectives

- a) Perform actions in accordance with ITU-T LSG's responsibility with the focus on architectural aspects of telecommunication security;
- b) Consider standardization needs related to security architecture for security services;
- c) Develop security concepts, architectures and Recommendations applicable to areas such as Internet Protocol (IP), Next Generation Networks (NGN), future wireless systems, and electronic business;

- d) Provide assistance to other ITU-T Study Groups in applying security architecture for specific security solutions, and review project-oriented security solutions for consistency;
- e) Maintain and update existing Recommendations;
- f) Coordinate security activities with other ITU-T Study Groups, ISO/IEC JTC 1, and other consortia and fora, as appropriate; and
- g) Provide awareness on new security technologies related to telecommunication security.

2.2.2 Summary of Candidate Recommendations

1) X.805+, Architecture for security controls division between the networks and the users

This Recommendation provides guidance for applying the concepts of the ITU-T Recommendation X.805 to division of security controls between the telecommunication networks and the end users' equipment.

This Recommendation is planned for consent at the September 2007 meeting of SG17.

2) X.805nsa, Network security assessment/guidelines based on ITU-T Recommendation X.805

This Recommendation provides a framework for network security assessment/guidelines.

3) X.akm, Framework for EAP-based authentication and key management

This draft Recommendation establishes a framework for EAP-based authentication and key management for securing the link layer. It also provides guidance on selection of the EAP methods. In addition, it provides the mechanism of the key management for the link layer.

4) X.pak, Password-authenticated Key Exchange Protocol (PAK)

This Recommendation specifies a password-based protocol for authentication and key exchange, which ensures mutual authentication of both parties in the act of establishing a symmetric cryptographic key via Diffie-Hellman exchange. The use of Diffie-Hellman

exchange ensures the perfect forward secrecy. With the proposed authentication method, the exchange is protected from the man-in-the-middle attack. The authentication relies on a pre-shared secret, which is protected (i.e. remains unrevealed) to an eavesdropper preventing an offline dictionary attack. Thus, the protocol can be used in a wide variety of applications where pre-shared secrets based on the possibly weak password exist.

5) X.spn, Framework for creation, storage, distribution, and enforcement of security policies for networks

This Recommendation establishes a set of security policies that will drive the security controls of a system or service. It also specifies a framework for creation, storage, distribution, and enforcement of policies for network security that can be applied to various environmental conditions and network devices.

2.3 Questions 6/17: Cybersecurity

2.3.1 Objectives

- a) Perform actions in accordance with LSG's responsibility with the focus on Cybersecurity;
- b) Identify and develop standards required for addressing the challenges in Cybersecurity, within the scope of Q.6/17;
- c) Provide assistance to other ITU-T Study Groups in applying relevant Cybersecurity Recommendations for specific security solutions, and review project-oriented security solutions for consistency;
- d) Maintain and update existing Recommendations within the scope of Q.6/17 (this includes E.409);
- e) Coordinate security activities with other ITU-T Study Groups, ISO/IEC JTC 1 (such as SC 6, SC 27 and SC 37), and other consortia as appropriate;
- f) Provide awareness on new security technologies related to Cybersecurity;

- g) Provide an Identity Management Framework that defines the problem space, representative use case scenarios and requirements. This includes leveraging other on-going Identity Management activities; and
- h) Collaborate with NGN activities in ITU-T in the areas of Cybersecurity and Identity Management.

2.3.2 Summary of Candidate Recommendations

1) X.cso, Overview of Cybersecurity

This Recommendation provides a definition for Cybersecurity. The Recommendation provides a taxonomy of security threats from an operator's point of view. Cybersecurity vulnerabilities and threats are presented and discussed at various network layers.

Various Cybersecurity technologies that are available to remedy the threats including routers, firewalls, antivirus protection, intrusion detection systems, intrusion protection systems, secure computing, audit and monitoring. Network protection principles such as defense in depth, access and identity management with application to Cybersecurity are discussed. Risk management strategies and techniques are discussed including the value of training and education in protecting the network. A discussion of Cybersecurity standards, Cybersecurity implementation issues and certification are presented.

2) X.vds, A vendor-neutral framework for automatic checking of the presence of vulnerabilities information update

This Recommendation provides a framework of automatic notification on vulnerability information. The key point of the framework is that it is a vendor-neutral framework. Once users register their software, updates on the vulnerabilities and patches of the registered software will automatically be made available to the users. Upon notification, users can then apply patch management procedure to update their software.

3) X.sds, Guidelines for Internet service providers and end-users for addressing the risk of spyware and deceptive software

This Recommendation provides guidelines for Internet Service Providers (ISP) and end-users for addressing the risks of spyware and deceptive software. The Recommendation

promotes best practices around principles of clear notices, and users' consents and controls for ISP web hosting services. The Recommendation also promotes best practices to end-users on the Internet to secure their computing devices and information against the risks of spyware and deceptive software.

4) X.cap, Guidelines on Cybersecurity vulnerability life-cycle management

This Recommendation specifies the Common Alerting Protocol (CAP) which is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increases warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as indicating an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

This Recommendation is technically equivalent and compatible with the OASIS Common Alerting Protocol, v.1.1 standard.

5) X.rfpg, Privacy guideline for RFID

This Recommendation recognizes that as RFID greatly facilitates the access and dispersion of information pertaining specifically to the merchandise that individuals wear and/or carry; it creates an opportunity for the same information to be abused for tracking an individual's location or invading their privacy in a malfeasant manner. For this reason, the Recommendation develops guidelines and best practices regarding RFID procedures that can be used by service providers to gain the benefits of RFID while attempting to protect the privacy rights of the general public within national policies.

6) X.idmr, Identity management requirements

This Recommendation develops used case scenarios and requirements for the Identity Management Framework Recommendation (X.idmf). The developed use cases cover Telecommunications and non-Telecom scenarios (i.e., the orchestration of business processes that include supply change management, client resource management, enterprise resource management, location, presence, and other services).

7) X.idmf, Identity management framework

This Recommendation develops an Identity Management Framework that leverages the use case scenarios as it applies to Telecommunications and includes non-Telecom applications when (i.e., the orchestration of business processes that include supply change management, client resource management, enterprise resource management, location, presence, and other services). The framework enables service providers to provide entities with reliable, trusted and secure IdM services over distributed networks, through the appropriate use of authorization, authentication, access control mechanisms, and policy management mechanisms.

8) X.idms, Identity management security

This Recommendation performs security analysis on the Identity Management Framework as developed in X.idmf. The Recommendation develops guidelines and best practices approach for ensuring that security is maintained when the Identity Management Framework is used as the vehicle for providing Telecommunications and non-Telecom IdM solutions.

2.4 Question 7/17: Security Management

2.4.1 Objectives

1) Information security management guideline for telecommunications

(Existing X.1051, Information security management system - Requirements for telecommunications (ISMS-T))

- a) Maintain and revise Recommendation X.1051. The title of X.1051 is 'Information Security Management Guideline for telecommunications based on ISO/IEC 27002'.
- b) Jointly develop a guideline on information security management with ISO/IEC JTC 1/SC 27.

2) Risk management methodology

- a) Review the similarities and differences among the existing management Recommendations in ITU and management standards in other standardization bodies for risk management.
- b) Study and develop a methodology of risk management for telecommunications in line with Recommendation X.1051.
- c) Produce and consent a new ITU-T Recommendation for risk management methodology.

3) Incident management

- a) Review the similarities and differences among the existing management Recommendations in ITU and standards in other standardization bodies for incident management.
- b) Study and develop a handling and response procedure on security incidents for the telecommunications in line with Recommendation X.1051.
- c) Produce and consent a new ITU-T Recommendation for incident management methodology and procedures.

2.4.2 Summary of Candidate Recommendations

1) X.1051 (revised), Information security management guidelines for telecommunications based on ISO/IEC 27002

This Recommendation establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications based on ISO/IEC 27002. The objectives outlined in this Recommendation provide general guidance on the commonly accepted goals of information security management for telecommunications.

This Recommendation may serve as a practical guide for developing telecommunication security standards and effective security management practices and to help build confidence in inter-telecommunication activities.

2) X.rmg, Risk management guidelines for telecommunications

This Recommendation describes and recommends techniques for information security risk management for telecommunications to support the X.1051, **Information security management guideline for telecommunications based on ISO/IEC 27002**. These techniques can be used to assess security requirements and risks identified in telecommunications, and help to establish and maintain the appropriate security controls, i.e. the correct information security level. There are many specific methodologies that have been developed to address the requirements for risk management. This Recommendation provides the criteria for assessing and selecting appropriate methodologies for a telecommunication organization. However, this does not aim to propose a specific risk management methodology for telecommunications.

3) X.sim, Security incident management guidelines for telecommunications

This Recommendation provides advice and guidance on information security incident management for information security managers on information systems, services and networks in telecommunications to support of the Recommendation X.1051. This is based on ISO/IEC TR18044 (**information security incident management**) and Recommendation E.409 (**Incident organization and security incident handling: Guidelines for telecommunication organizations**).

As the background of this study, after security controls have been implemented, residual weaknesses are likely to remain that may make information security ineffective and thus information security incidents possible, potentially with both direct and indirect adverse impact on a telecommunications' business operations. Inevitably, previously unidentified new threats will occur. Insufficient preparation by a telecommunication organization to deal with such incidents will make any actual response less effective, and potentially increase the degree of potential adverse business impact. Therefore it is essential for any telecommunication organization to detect, report, assess and respond to information security incidents. It is also important to learn from information security incidents and

to make improvements to the overall approach to information security incident management for telecommunications.

This Recommendation satisfies the above essential requirements for information security incident management in telecommunications.

2.5 Question 8/17: Telebiometrics

2.5.1 Objectives

The focuses of Q.8/17 are Telebiometric Multimodal Model Framework (TMMF), Telebiometrics System Mechanism (TSM), BioAPI Interworking Protocol (BIP), Telebiometrics Protection Procedures (TPP), Telebiometric Authentication Infrastructure (TAI), and Telebiometrics Digital Key Framework (TDK).

1) X.1081, Telebiometric Multimodal Model Framework (TMMF)

- a) Identify security issues in biometric identification and authentication processes and develop specifications of means to obtain quality results based on metrological quantification (measurements).
- b) Identify safety issues in recording and collecting of biometric data and provide guidance of usage in accordance with currently valid safety standards. Establish means of calculating the correct upper and lower safety thresholds from the products of the International Union of Sciences and the World Health Organization for each of the measurable telebiometric interactions in order to avoid safety risks.
- c) Clarify biometric identification and related processes in order to prevent security risks.
- d) Promote the ITU-T telebiometric database, and make possible data to be uploaded from ITU-T Recommendations by Telebiometric Database Editor.

2) Telebiometrics System Mechanism (TSM)

- a) Study and develop biometric authentication models and procedures for the telecommunications based on Cryptographic technology such as PKI.
- b) Produce and consent new ITU-T Recommendations for biometric authentication technologies for telecommunications based on Cryptographic technology such as PKI.

3) BioAPI Interworking Protocol (BIP)

- a) Progress the BioAPI Interworking Protocol (BIP) text as a common text between ITU-T and ISO/IEC/JTC 1/SC 37 in accordance with the procedures of ITU-T Recommendation A.23 and Annex K of the JTC 1 Directives.
- b) Resolve possible issues to have this common text fully meet the requirements of Q.8/17 for communications between systems as described in the X.tsm document.

4) Telebiometrics Protection Procedures (TPP)

- a) Study and develop protecting procedures for biometric data exposed to possible threats of illegal usage in telebiometrics.
- b) Produce and consent new ITU-T Recommendations for guidelines of technical and managerial procedures for protecting telebiometric systems, including multibiometric systems.

5) Telebiometrics Authentication Infrastructure (TAI)

- a) Study and develop an infrastructure for biometric authentication to be applied in PMI.
- b) Revise the ASN.1 definitions to use Attribute Certificates defined in ITU-T Rec. X509.
- c) Create a normative Annex containing an ASN.1 module with all the definitions.

6) Telebiometrics Digital Key Framework (TDK)

- a) Study and develop the biometric digital key generation/protection/extraction frameworks based on the biometric certificate.
- b) Study and develop cryptographic requirements on the biometric digital key using biometric data in telebiometric applications.
- c) Produce and consent a new ITU-T Recommendation for biometric digital key framework to ensure security on biometric data with biometric certificate.

2.5.2 Summary of Candidate Recommendations

1) X.bip | ISO/IEC 24708, BioAPI interworking protocol

This Recommendation | International Standard specifies the syntax, semantics, and encodings of a set of messages (“BIP messages”) that enable a BioAPI-conforming application to request biometric operations in BioAPI-conforming biometric service providers (BSPs) across node or process boundaries, and to be notified of events originating in those remote BSPs. It also specifies extensions to the architecture and behaviour of the BioAPI framework (specified in ISO/IEC 19784-1) that supports the creation, processing, sending, and reception of BIP messages. This Recommendation | International Standard also describes how to use BIP with TCP/IP and SOAP/HTTP.

2) X.physiol, Telebiometrics related to human physiology

This Recommendation uses the framework defined in ITU-T Recommendation X.1081, **The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics**, for optimal safety and security in telebiometrics. It gives names and symbols for quantities and units concerned with emissions from the human body that can be detected by a sensor, and the effects on the human body produced by the telebiometric devices in his environment. It is applicable to both physiology and biometrics (the measurement of physiological, biological and behavioral characteristics). A taxonomy of Wetware and Hardware/Software interactions is defined. Thresholds are specified using the set of International System of Quantities (ISQ) and the related set of International System of Units (SI).

3) X.tai, Telebiometrics authentication infrastructure

This Recommendation describes several security requirements in authentication of identity, and proposes a security framework to provide related security service. This Recommendation includes Telebiometric Authentication Infrastructure (TAI), Biometric Certificate, Biometric Algorithm Certificate, Biometric Template in Biometric Certificate, models and procedures combining TAI with Privilege Management Infrastructure (PMI) to implement identity and privilege authentication. The framework also defines the information object, Biometric Certificate (BC) and its revoke list (Biometric Certificate Revoke List, BCRL). Referring to X.509, the document defines the BC issuance, management, usage, and revocation mechanisms. The Recommendation also defines a series of certificate extensions that can combine TAI with PKI or PMI seamlessly. The authentication scheme defined in this Recommendation is universal to be used in different applications and environments.

4) X.tpp-1, A guideline of technical and managerial countermeasures for biometric data security

This Recommendation defines weaknesses and threats in operating telebiometric systems and proposes a general guideline of security countermeasures from both technical and managerial perspectives. From the technical point of view, countermeasures are proposed to ensure the integrity, mutual authentication, and confidentiality of the transmitted data and also to protect the data capture, feature extraction, enrollment, transmission and storage of the biometric information. From the managerial perspective, measures are described that provide protection of biometric devices as related to their installation, removal, and delivery, and operational procedures; and roles and responsibilities of the personnel involved in the system are also defined.

5) X.tpp-2, A Guideline for secure and efficient transmission of multibiometric data

This Recommendation provides the procedures and methods for secure transmission of data in multibiometric systems. It adopts the concept of multibiometrics which is being provided in ISO/IEC PDTR 24722 "Multi-modal and Other Biometric Fusion". It also introduces all the possible threats during transmission in various models of multibiometrics, which then provides the guidelines for secure transmission that can be applied only in multibiometric systems and not in general biometric system, in order to avoid redundancy with X.tpp-1.

6) X.tsm-1, General biometric authentication protocol and profile on telecommunication system

This Recommendation provides biometric authentication protocols and profiles on telecommunication systems. It defines protocols of biometric authentication for unspecified end-users and service providers on open network. It clarifies nine authentication network models. It also defines communication mechanism for the protocol based on TLS extension and X.bip message components.

7) X.tsm-2, Profile of telecommunication device for Telebiometrics System Mechanism (TSM)

This Recommendation defines the requirements on client terminals for biometric authentication over the open network, based on the models defined in TSM-1. System mechanisms and security profile of the client side are specified based on Common Criteria ISO/IEC 15408 “Evaluation Criteria for IT Security”. There are outlined protocols that terminals should follow to be securely authenticated.

8) X.tdk, Telebiometrics Digital Key Framework (TDK)

This Recommendation provides biometric digital key generation, protection, and extraction models and mechanisms using the biometric template from the Biometric Certificate in order to provide cryptographic secure authentication and secure communication in open network. It also defines biometric digital key generation and protection/extraction frameworks with cryptographic mechanisms. This Recommendation further defines the security requirements in biometric digital key mechanisms for simplified authentication and secure communication.

2.6 Question 9/17: Secure Communication Services

2.6.1 Objectives

1) Mobile security and home network security

- a) Identify threats behind mobile communications or home network services, and set up technical counter-measures to handle them.
- b) Study general security policy technologies for end-to-end mobile communications or home network communication.
- c) Study general security value added services for mobile communications or home network communication.

- d) Study a security infrastructure, secure application protocols, and comprehensive security solutions in the emerging mobile network including home network or ubiquitous environment.
- e) Maintain existing mobile security-related Recommendations, produce and consent new ITU-T Recommendations for end-to-end mobile or home network communications.

2) Secure application protocols

- a) Study and recommend various secure application protocols such as PKI application protocol, end-to-end transport protocol, secure key exchange protocol, password authentication protocol, authorization protocol, notarization protocol, and time stamping protocol, et al, in a secure communication service.
- b) Standardize secure communication services to support secure and stable operation of the telecommunication network and improve the quality of security in a communication network.
- c) Standardize secure interconnectivity methods for secure application services.
- d) Standardize the security mechanisms for supporting secure application services.
- e) Produce and consent new ITU-T Recommendations for secure application protocols.

3) Web services security

- a) Investigate web services security technologies including security authentication assertion and extensible access control assertion, single-sign-on, et al.
- b) Coordinate these activities with Liberty Alliance and other groups.

- c) Clarify secure web services within telecommunications architectures; work out the usage of web-services security for telecommunication scenarios, networks, its systems and related applications.
- d) Recommend guidelines on how to best protect web-services telecommunication systems from attacks.
- e) Coordinate web services security activities with OASIS, OMA, or other groups.
- f) Produce and consent new ITU-T Recommendations for a web services security.

4) Networked RFID security

- a) Study and recommend a networked RFID-oriented security framework, security protocols, and security mechanisms for networked RFID services including authentication protocols, privacy protection framework, privacy protection guideline, etc.
- b) Standardize secure networked RFID services to support a secure end-to-end communication based on a series of networks, internetworks, and globally distributed application systems.
- c) Coordinate networked RFID security activities with ISO/IEC JTC 1, ITU-T JCA-NID or other groups.
- d) Produce and consent new ITU-T Recommendations for networked RFID security.

2.6.2 Summary of Candidate Recommendations

1) X.homesec-1, Framework of security technologies for home network

This Recommendation describes security threats and security requirements to the home network from the point of view of home user and remote user. It excludes the security requirements from the service provider's viewpoint. In addition, this Recommendation categorizes security technologies by security functions that satisfy the above security

requirements and by the place to which the security technologies are applied in the model of the home network. Finally, the security function requirements for each entity in the network and possible implementation layer for security function are also presented.

2) X.homesec-2, Device certificate profile for the home network

This Recommendation describes framework for home network device certificate. In addition, it describes a device certificate profile, certificate management protocols for device certificate in the home network, XML expression of home network device certificate, and usage scenario for device certificate.

3) X.homesec-3, User authentication mechanisms for home network service

There are some environments where it is necessary to authenticate the user, rather than a process or a device. To authenticate users, authentication system requires users to prove their uniqueness. Such uniqueness generally is based on something known, something possessed or some immutable characteristic for each user.

This Recommendation provides the user authentication mechanism in the home network, which enables various authentication means such as password, certificate, biometrics and so forth. This Recommendation also considers diverse security issues according to X.homesec-1, which is the framework of security technologies for home network. And it defines the user authentication protocol applicable to the general model of the home network defined in X.homesec-1.

4) X.msec-3, General security value added service (policy) for mobile data communication

This Recommendation provides a specification of general security service for secure mobile end-to-end data communication. One purpose of this Recommendation is to transform high level of security service as value added service. It includes a series of security levels, security policy and charging mechanism for the security service. Interfaces and negotiation process among different network entities are provided. This Recommendation also clarifies protocols used to carry out every negotiation process.

5) X.msec-4, Authentication architecture in mobile end-to-end data communication

This Recommendation constructs generic authentication architecture for mobile data communication to satisfy various requirements of application service authentication methods between mobile users and application servers. The architecture applies to mobile terminal users subscribed to different mobile networks and application service providers inside the mobile network or in open networks.

6) X.crs, Correlative reacting system in mobile network

This Recommendation describes the generic architecture of a correlative reactive system deployment which the mobile network and its user terminals can cooperate interactively to combat various security threats for secure end-to-end data communications. Such threats include, for example, virus, worms, Trojan-Horses or other network attacks etc. to both the mobile network and its mobile users. Protocol and procedures are comprehensively specified and some important application issues are addressed. For the cases that viruses or worms have already been spreading in the mobile network, the correlative reactive system also provides a mechanism to keep them from spreading in configurable scope, thus saving time for the network operator to recover, and finally to reduce the lost to the lowest possible.

7) X.sap-1, Guideline on secure password-based authentication protocol with key exchange

This Recommendation is to identify a set of requirements for password authentication protocols such as framework requirement and protocol requirement and define a selection guideline for various password authentication protocols by setting up criteria that can be used in choosing an optimum authentication protocol among various strong password authentication protocols for each application.

8) X.sap-2, Secure end-to-end data communication techniques using TTP services

This Recommendation defines the basic interfaces, basic interactions and security considerations for secure end-to-end data communication using on-line TTP (Trusted Third Party) services. This Recommendation also identifies which on-line TTP services can be used to support the secure end-to-end data communication between two applications.

9) X.p2p-1, Requirements of security for P2P communications

Although many new applications which are based on peer-to-peer (P2P) technology have been developed, these communications have several problems from the security viewpoint. This Recommendation investigates threat analysis for P2P communication services and describes security requirements for secure P2P communication services.

This Recommendation is in harmonization with X.p2p-2.

10) X.p2p-2, Security architecture and protocols for peer-to-peer network

This Recommendation defines the general architectures of peer-to-peer network, the protocol structure and the security protocols of peer-to-peer communications. For the secure peer-to-peer communication, this involves the authentication, key generation/distribution, and peer-trusting frameworks for the peer-to-peer group communication. The objective of this Recommendation is to serve as a foundation for developing the detailed protocols for the peer-to-peer security.

This Recommendation will be developed in harmonization with X.p2p-1. In addition, this Recommendation considers the security issues of X.p2p-1 which is a base of security mechanisms for peer-to-peer communications for P2P network.

11) X.websec-3, Security architecture for message security in mobile web services

This Recommendation develops a guideline on message security architecture and service scenarios for securing messages for mobile Web Services. Since SOAP messages cannot be filtered by firewalls, the message filtering mechanisms should be integrated into the architecture. This Recommendation also develops the security policy mechanisms suitable for Web Services message security. The interworking mechanisms between mobile Web Services applications and legacy non-Web Services applications are also developed.

12) X.rfidsec-1, Privacy protection framework for networked RFID services

Widespread deployment of Radio Frequency Identification (RFID) tags may cause privacy infringement worries to an ordinary person because of the abilities of RFID technology such as automated collection and processing of the RFID data from the RFID-enabled products, and possible disclosure of those data to the public. Especially, in networked RFID services based on personalized tag such as after-sale service for RFID-enabled products, healthcare-related service using RFID, etc., the privacy issue is a more serious problem. This Recommendation describes privacy infringements for networked RFID service environment and requirements for privacy protection, and develops privacy protection services based on a user privacy policy profile.

2.7 Questions 17/17: Countering Spam by Technical Means

2.7.1 Objectives

- a) Act as the lead group in ITU-T on technical means for countering spam as spam is described by Study Group 2;
- b) Establish effective cooperation with the IETF, the relevant ITU Study Groups, the ITU Strategy and Policy Unit (SPU) and appropriate consortia and fora, including private sector entities for this area;
- c) Identify and examine the telecommunication network security risks (at the edges and in the core network) introduced by the constantly changing nature of spam;
- d) Develop a comprehensive and up-to-date resource list of the existing technical measures for countering spam in a telecommunication network that are in use or under development;
- e) Determine whether new Recommendations or enhancements to existing Recommendations, including methods to combat delivery of spyware, phishing, and other malicious contents via spam, would benefit Member efforts to effectively counter spam as it relates to the stability and robustness of the telecommunication network;

- f) Provide regular updates to the Telecommunication Standardization Advisory Group and to the Director of the Telecommunication Standardization Bureau to include in the annual report to Council; and
- g) Maintain awareness of international cooperation measures on countering spam.

2.7.2 Summary of Candidate Recommendations

1) X.csreq, Requirement on countering spam

Requirements on countering spam are clarified in this recommendation. There are many types of spam, such as email spam, mobile messaging spam and IP multimedia spam. Various types of spam may have both common and specific requirements on countering it. For one type of spam, the requirement in different entities should also be clarified.

2) X.gcs, Guideline document on countering email spam

This Recommendation specifies technical issues on countering email spam. It provides the current technical solutions and related activities from various Standards Development Organizations (SDOs) and relevant organizations on countering email spam. Purpose of the Recommendation is to provide useful information to the users who want to find technical solutions on countering email spam and it will be used as a basis for further development of technical Recommendations on countering email spam.

3) X.fcs, Technical framework for countering email spam

This Recommendation specifies the technical framework for network structure for countering spam. Functions inside the framework are defined. It also provides the universal rules of distinguishing spam from other emails and the common methods of countering email spam.

4) X.ocsip, Overview of countering spam for IP Multimedia application

This Recommendation specifies basic concepts, characteristics, and effects of Spam in IP multimedia applications such as IP telephony, video on demand, IP TV, instant messaging, multimedia conference, etc. It provides technical issues, requirements for technical solutions, and various activities on countering spam for IP multimedia

applications. It provides the basis and guideline for developing further technical solutions for countering spam.

5) X.fcsip, Framework of countering IP Multimedia spam

This Recommendation specifies general architecture of countering spam system on IP multimedia applications such as IP telephony, instant messaging, multimedia conference, etc. It provides functional blocks of necessary network entities to counter spam and their functionalities, and describe interfaces among the entities. To build secure session against spam attack, user terminals and edge service entities such as proxy server or application servers will be extended to have spam control functions. We will also show interfaces between these extended peer entities, and interfaces with other network entities which can be involved in countering spam.

6) X.tcs, Technical means for countering spam

Communication network is evolving, more services are emerging, and the capability of spammers is stronger. Moreover, no single technical means has perfect performances on countering spam currently. It may be necessary to propose new technical countermeasures.

7) X.tcs-1, Interactive countering spam gateway system

This Recommendation specifies interactive countering spam gateway system as a technical means for countering various types of spam. The gateway system enables spam notification from receiver's gateway to sender's gateway, prevents spam traffic from going across the network. This specification defined architecture for the countering spam gateway system, described basic entities, protocols and functions, provided mechanisms for spam detection, countering spam information sharing, and countering spam actions of the gateway systems.

Note: The biography of the author is available at the end of the paper "Japan's Status Update - Brief Summary Of ISMS Update In Japan" on page 35.

ABSTRACT

This paper highlights issues pertaining to Cybercrime and Cybersecurity, including the adoption and lack of adoption of related laws in the Asia Pacific region to address these issues. It also highlights the challenges faced by countries, as well as law and technology professionals, when addressing such issues.

1. Introduction

The purpose of this paper is to familiarize non-law professionals with some of the issues involving Cybercrime and Cybersecurity facing the law, policy and technology communities.

A fundamental issue in this domain is the lack of consistent definitions of the terms “Cybercrime” or “Cybersecurity”. The same actions may be characterized in various terms, for example, “computer crime”, “computer intrusion”, “Internet security”, “network intrusion”, etc. in laws and policies of various nations and international organizations.

Despite the lack of consistent definitions, here are a few:

Computer crimes - also called:

- a) “computer-related crime” - “the use of a computer is integral to committing the offense; examples are offenses such as computer-related forgery (where false data are put forward as authentic) and computer-related fraud (the fraudulent interference with or manipulation of data to cause property loss)”;
- b) “computer crime” - “a general label for offenses in which a computer is the object or the offense or the tool for its commission”;
- c) “Internet crime” - “crimes in which the use of the Internet is a key feature and includes content-related offenses such as possession of child pornography, or in some countries, the dissemination of hate or racist material”; and

¹ This paper was presented at the 5th RAISS Forum Meeting, on 4 October 2006 and has been updated with new information as of 25 January 2007.

- d) “e-crime” - “a general label for offenses committed using an electronic data storage or communications device”.²

Cybercrime is defined both in statutes adopted by countries and economies, and at times at state or commonwealth levels, but not in the Council of Europe Convention on Cybercrime, which, as has been pointed out by commentators, has a broader meaning at the international level. It is then “an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copyright offenses. This wide definition of Cybercrime overlaps in part with general offense categories that need not be ICT-dependent, such as white-collar crime and economic crime.”³

As if these terms are not confusing enough to absorb, there is also the label of “high tech crime” used in places such as the United Kingdom and Australia. Agencies in both countries “deal with crimes that rely on the use of Information and Communications Technology (ICT), or which target ICT equipment, data and services. Their focus is on the complex networking capacity of ICT, which creates a previously unimaginable platform for committing and investigating criminal activity.” According to the same crime brief, “the distinction between the use of ICT as either the object or as a tool of offending... has been adopted by Statistics Canada (2002)...”. This two part division of high tech crime has been used for the analysis of such crimes in Australia.⁴

For some additional definitions, the reader may want to consult Wikipedia⁵, and laws from various jurisdictions⁶, and those who are more ambitious may wish to read some law journal articles and books discussing the lack of consistent or universal definitions.⁷

² Australian Institute of Criminology, High Tech Crime Brief, Concepts and Terms, New Crimes and Old Crimes Committed in New Ways, 1/05, <http://www.aic.gov.au>.

³ Id.

⁴ Id.

⁵ <http://www.en.wikipedia.org>.

⁶ These will be discussed later on in this paper.

⁷ See, e.g. Susan Brenner, “Cybercrime Law and Policy in the United States”, in Pauline C. Reich, Ed., CYBERCRIME AND SECURITY (Oceana, a division of Oxford University Press).

Cybersecurity - also called "Internet security", but may also include Distributed Denial of Service (DDOS) attack, cyberterrorism, attacks on critical information infrastructure, cyberwar.

A simple definition:

Cybersecurity - "Ensuring the safety and security of networked information systems".⁸

2. Laws Addressing Cybercrime and Cybersecurity

- Many, Some, None in Various Countries and Economies

Some countries and economies have multiple laws for addressing the actions we have described above⁹. Other countries have not yet adopted laws¹⁰ or may have to use existing criminal and other types of laws, e.g. intellectual property laws, telecommunications laws, etc., while proposed laws are stalled in their legislative bodies.¹¹

In most countries, there are inadequate numbers of police trained in computer forensics, and thus very few arrests, prosecutions or convictions, although there are some.¹²

3. Collaboration, Cooperation and Why

The problems of Cybercrime and Cybersecurity, due to the cross-border nature of the Internet in particular, require international cooperation and collaboration in order to prosecute the perpetrators of criminal activities such as identity theft, fraud, spamming, hacking, fund raising for terrorist groups, teaching terrorist tactics online, and online money laundering.

⁸ Miriam F. Miquelon Weismann, "International Cybercrime: Recent Developments in the Law", in Ralph D. Clifford, Ed., CYBERCRIME: THE INVESTIGATION, PROSECUTION AND DEFENSE OF A COMPUTER-RELATED CRIME, 2ND Ed., Carolina Academic Press (North Carolina) p. 243.

⁹ For example, the United States, the EU countries, the Republic of Korea, Japan, Australia, others.

¹⁰ India is an example. Amendment of its 2000 law is under consideration.

¹¹ For example, Thailand.

¹² See the U.S. Department of Justice Computer Crime & Intellectual Property Section website, <http://www.cybercrime.gov/intl.html> for information about the international aspects of "computer crime" and <http://www.cybercrime.gov> for news releases about U.S. prosecutions at the Federal level under the Federal statutes enforced by the Department of Justice. See also coverage of the Winny cases in Japan, e.g. Takato Natsui, "Winny Case", (2004) at <http://www.isc.meiji.ac.jp/~sumwel-h/doc/Winny%20Case%20Natsui%20rel%204/pdf>; "Winny developer guilty of copyright violations", THE ASAHI SHIMBUN, http://www.asahi.com/english/Herald_asahi/TKY200612140146.html; "Winny", Wikipedia, <http://en.wikipedia.org/wiki/Winny>.

The Council of Europe Cybercrime Convention can be used as a model for national legislation, however, some countries are concerned about such issues as violations of personal privacy in the name of national security, or just plain invasions of privacy by governments in nations in which privacy is thought to be an important constitutional right.¹³

Cybercrime and Cybersecurity issues also require domestic collaboration among the various players - the technology professionals, the law professions¹⁴, policy makers, legislators in each nation or economy, as well as cross-border cooperation.

On the international level, there is a need for all of us to “be on the same page” with respect to what the various criminal and national security issues are, how to develop legislation with knowledge of the nature of computers, computer networks, the Internet, etc., how to investigate, how to present digital evidence, how to interpret digital evidence and apply law to it, the severity of infractions, etc. The bottom line is that there is a need for an interdisciplinary dialogue among the various players and their communities - but instead, most of us often do not meet with others from different fields to exchange knowledge, whether domestically or internationally.

Do you know, for example, what laws are in place in your country or economy to combat Cybercrime and Cybersecurity issues? Are the existing laws effective in enabling police to investigate and arrest persons or crime rings engaged in some of the activities listed above? Do the laws take into account the technology available in your economy? Are there adequate numbers of police and national security professionals trained in the technology areas needed, e.g. computer forensics?

For many developing countries, even more so than in developed countries, there is a severe shortage of trained police and national security professionals. This inhibits the application and enforcement of laws even when they are adopted.

¹³ See, e.g., John Morris and Jon Peterson, “Who’s Watching You Now?”, IEEE Security and Privacy Magazine, Vol. 5, Issue 1, January/February 2007; Jerry Berman, “Security, Privacy and Government Access to Commercial Data”, in Clayton Northouse, Editor, PROTECTING WHAT MATTERS; TECHNOLOGY, SECURITY AND LIBERTY SINCE 9/11, Brookings Institution Press and the Computer Ethics Institute, 2006; Nancy Liben, “The anxious new dawn of cybersnooping”, CNET News, 3 May 2006.

¹⁴ For example, police, prosecutors, judges, defense attorneys.

4. The Council of Europe Cybercrime Convention

The Convention is a model developed to address the legal aspects of Cybercrime prevention and prosecution. It entered into force on 1 July 2004.

As of 27 September 2006, 15 countries had ratified the Convention, and thus became parties to it, and 43 countries had signed the convention.

The difference between signing and ratification is that signing means that a country will undertake a review of its laws and policies and undertake to adopt legislation that will put it into compliance with the Convention. Japan, for example, is a country that is still a signer, as all the laws necessary to align with the Convention have not yet been adopted.¹⁵

In the Asia-Pacific region, only Japan, Canada and the United States have signed the Convention (other non-EU signatories were Montenegro and South Africa). The United States ratified it on 22 September 2006, but with some controversy and expressions of concern.¹⁶

5. Where do other countries in the Asia-Pacific/Oceania Region stand with respect to the adoption of laws to address these issues?

A review of the Asia Pacific region indicates the following legislation to be pending or in place:

- a) Bangladesh - June 2006 - A draft bill on Information and Communication Technology was introduced in the Parliament.
- b) Brunei - March 2006 - New laws dealing with Cybercrime were "under serious consideration".

¹⁵ See Takato Natsui, "Cybercrime Legislation and Cases in Japan - Update", and Japan Federation of Bar Associations, "Crime Prevention and Criminal Justice", in Pauline C. Reich, Ed., CYBERCRIME AND SECURITY.

¹⁶ Kristin Archick, CRS Report for Congress, updated 9/28/06, <http://italy.usembassy.gov/pdf/other/RS21208.pdf>.

- c) Australia - the following laws are available to deal with Cybercrimes:
- Cybercrime Act 2001;¹⁷
 - Crimes Act 1900 (New South Wales);
 - Criminal Code (Western Australia);¹⁸ and
 - Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) (2004) (came into force on 1 March 2005).¹⁹
- d) Canada - Canadian Criminal Code Section 342, Unauthorized Use of Computer and Section 184, Interception of Communications.²⁰
- e) China -Criminal Law provisions are applied.²¹
- f) Hong Kong - A provision of the Crimes Ordinance, Section 161, Access to Computer with Criminal or Dishonest Intent, can be applied to Cybercrimes.²²
- g) India - The Information Technology Act, 2000 is applied to some crimes and the government has convened a committee to address amendment of that law. Discussions have been ongoing for some time.²³
- h) Indonesia -July 2005 - the Electronic Transaction and Information Law was submitted to the House.

17 See <http://www.cybercrimelaw.net/laws/countries/australia.html>.

18 Computer crime, Wikipedia, http://en.wikipedia.org/wiki/Computer_crime.

19 This added a new part to the Criminal Code Act 1995 containing offenses prohibiting the misuse of telecommunications networks. See Gregor Urbas and Peter Grabosky, "Cybercrime and Jurisdiction in Australia", in Koops and Brenner, Eds., CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY (2005), p. 52.

20 See <http://www.cybercrimelaw.net/laws/countries/canada.html> and "Computer crime", Wikipedia, http://en.wikipedia.org/wiki/Computer_crime.

21 See <http://www.cybercrimelaw.net/laws/countries/china.html>.

22 See <http://www.hkii.org/cgi-hkii/disp.pl/hk/legis/en/ord/200/s161.html?query=22computer%22+and+%22crime%22>.

23 See <http://www.cybercrimelaw.net/laws.countries/india.html> and Asian School of Cyber Laws analysis, "Unauthorised Access", http://www.asianlaws.org/cyberlaw/library/india/cc/un_access.htm.

- i) Japan - The Unauthorized Computer Access Law No. 128 of 1999 (Prohibition of acts of unauthorized computer access) is one of the laws in place²⁴. The other major legislation is found in provisions of the Penal Code.
- j) Republic of Korea - There are three laws in place addressing Cybercrime issues:
- Criminal Law;
 - Act on Promotion of Information and Communications Network Utilization and Information Protection; and
 - Information Infrastructure Protection Act.²⁵
- k) Malaysia - The Computer Crimes Act 1997 has been adopted²⁶, however, according to one lawyer in Malaysia, there have been few cases brought under the law.
- l) New Zealand - The Crimes Amendment Act 2003, No. 39 Part 1 s15 of July 7th has been adopted.²⁷
- m) Pakistan - The Federal Cabinet approved the adoption of the Prevention of Electronic Crimes Bill 2007 on 17 January 2007.²⁸

²⁴ See <http://www.cybercrimelaw.net/laws.countries/japan.html> and Takato Natsui, "Cybercrime Legislation and Cases in Japan: Update" in Pauline C. Reich, Ed., CYBERCRIME AND SECURITY, for full coverage as of 2005.

²⁵ See <http://www.cybercrimelaw.net/laws.countries/korea.html>.

²⁶ See <http://www.cybercrimelaw.net/laws.countries/malaysia.html>.

²⁷ See <http://www.cybercrimelaw.net/laws.countries/newzealand.html>.

²⁸ Pakistan's Cybercrime Bill 2007, 20 January 2007, <http://southasiaic4d.wordpress.com/2007/01/20/pakistans-cyber-crime-bill-2007/> <accessed 1/26/07>. According to the report, the bill includes penalties ranging from six months' imprisonment to capital punishment for 17 types of cybercrimes including cyberterrorism, hacking of websites and criminal access to secure data. Electronic crimes addressed in the bill include cyberterrorism, criminal access, criminal data access, data damage electronic fraud, electronic forgery, misuse of electronic system or electronic device, unauthorized access to code, misuse of encryption, misuse of code, cyber stalking. If the bill becomes law, it would "require the Internet companies maintain their traffic data for at least six months to enable the agencies to investigate cases involving data stored by them" and the law "would enable the government to seek extradition of foreign nationals through Interpol for their involvement in criminal activities punishable under the law".

- n) Philippines - The Philippines Republic Act No. 8792, An Act for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions, Penalties for Unlawful Use Thereof, and Other Purposes has been adopted.²⁹
- o) Singapore - Singapore has adopted the Computer Misuse Act (Ch. 50A).³⁰
- p) Thailand - Since the coup d'etat a few months ago, the Constitution has been suspended and a new Constitution is being written. Existing criminal law has been reported to be inadequate to address such issues as hacking³¹. Cybercrime-specific legislation has been stalled in the legislature for some time.
- q) United States -
- Access device fraud - 18 U.S.C. Section 1029;
 - Computer Fraud and Abuse Act, 18 U.S.C. Section 1030;
 - CAN-SPAM Act 18 U.S.C. Section 1037;
 - Extortion and threats, 18 U.S.C. Section 875;
 - Identity theft and assumption deterrence Act of 1998, 18 U.S.C. Section 1028;
 - Wire Fraud, 18 U.S.C. Section 1343;
 - No Electronic Theft Act, 17 U.S.C. Section 506;
 - Digital Millennium Copyright Act of 1998, 17 U.S.C. Section 1201;
 - Electronic Communications Privacy Act, 18 U.S.C. Section 2701 et seq;
 - Trade Secrets Act, 18 U.S.C. Section 1832;
 - Economic Espionage Act, 18 U.S.C. Section 1831; and
 - U.S. Computer Crime Laws by State.³²

²⁹ See <http://www.cybercrimelaw.net/laws/countries/philippines.html> and Abraham A. Purugganan, "Philippine Cybersecurity Update: Laws, Cases and Other Legal Issues", in Pauline C. Reich, Ed. CYBERCRIME AND SECURITY.

³⁰ <http://www.cybercrimelaw.net/laws/countries/singapore.html>. Author's note: The reader should check this website regularly, as new laws are added when they have been passed.

³¹ Police Major Dr Kissana Phathanacharoen, "Thailand Cybercrime and Security Issues", and "The Application of Existing Thai Criminal Law Dealing with Computer Hacking", in Pauline C. Reich, Ed., CYBERCRIME AND SECURITY.

³² Computer Crime, Wikipedia, http://en.wikipedia.org/wiki/Computer_crime.

6. The Need for Adequate Laws and Agreements for Prevention, Investigation and Prosecution

When countries adopt laws, they not only enable the legal professions to deal with domestic Cybercrime issues, but also, if they are consistent in prohibiting the same laws as those prohibited in other countries around the world, there is the possibility of country-to-country adoption of multilateral assistance treaties so that those committing Cybercrimes outside the country can be extradited and tried under other countries' laws. For example, if Country A (from which the Cybercriminal has released a virus which cripples computers in Country B) has no law with respect to the release of computer viruses and has no agreement with Country B, Country B cannot officially request that the perpetrator be extradited and tried under Country B's Cybercrime law. There are two problems here - lack of extradition power and lack of a crime in Country A so that Country A would not recognize the act affecting Country B as a crime.

The Cybercrime Convention, used as a model for the development of Cybercrime laws by individual countries and economies, would enable official cooperation in fighting such crimes as computer hacking, child pornography, online financial fraud, online extortion, and illegal copying of software, because all ratifying countries and economies would have similar domestic laws and would then be able to cooperate in investigation, extradition, etc.

The Convention is intended to harmonize computer crime and other such laws, so that countries that have joined the Convention are able to have up to date and similar kinds of domestic legislation.

7. Not all countries agree on adopting laws incorporating all the provisions of the Council of Europe Cybercrime Convention

Although the Council of Europe wants to take the lead in developing a model for legislation adopted in countries worldwide, there are some reservations that have been articulated in various countries about issues such as the following:

- a) Internet providers must cooperate with electronic searches and seizures without reimbursement;
- b) Governments must conduct electronic surveillance in “real time” on behalf of other governments;
- c) Businesses can be slapped with “expedited preservation orders” preventing them from routinely deleting logs or other data; and
- d) The Convention requirements do not require “dual criminality” in mutual legal assistance provisions, which is what happened when the Love Bug Virus arose and the perpetrator could not be prosecuted under existing law in the Philippines or be extradited.³³

8. The Optional Protocol on Hate Speech and Websites, etc.

Countries that have signed or ratified the main portion of the Cybercrime Convention may not have signed or ratified the Optional Protocol of the Convention. For example, the United States did not ratify it because some of the provisions are interpreted to be a violation of the First Amendment of the United States Constitution, which protects freedom of speech, even if that speech is unpopular or hateful to some members of the community.³⁴

³³ See Abraham A. Puruggannan, “Philippine Cybersecurity Update: Laws Cases and Other Legal Issues”, in Pauline C. Reich, Editor, CYBERCRIME AND SECURITY.

³⁴ See Kristin Archick, note 17 supra.

9. Other Controversial Aspects of the Cybercrime Convention

Civil liberties advocates in the United States have raised concerns about the government conducting wiretapping of phones and emails without search warrants. Recently, the Bush administration retreated a few steps on this issue and agreed to have a secret court issue search warrants in such instances.³⁵

This raises another question of whether government monitoring of the general population is overly broad.

10. The Need for an Interdisciplinary Dialogue between Law and Technology Communities

Why are many countries stalled in adopting adequate legislation to address first Cybercrime and then Cybersecurity issues? Here are some reasons:

- a) Laws must be designed to take into account technology use;
- b) Legislators must understand the nature of the technology and the cross-border nature of the Internet before being able to draft legislation;
- c) Governments must understand technology before issuing policy;
- d) Police, prosecutors, judges and defense attorneys must understand technology in order to carry out their respective roles;
- e) National security agency personnel must also understand technology in order to address Cybersecurity issues, although these may have to be addressed in part by technological defense strategies rather than law;
- f) Police in particular need hands-on training, adequate staffing, funds to pursue investigations and prosecutions; and

³⁵ Dan Eggen, "Court Will Oversee Wiretap Program", THE WASHINGTON POST, 1/18/07, page A01, <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/17/AR2007011701256.html>.

- g) Countries and economies may need to establish a Computer Emergency Response Team (CERT) organization, and to decide whether or not to have the CERT coordinate its activities with domestic law enforcement officials.

11. Conclusion

This brief overview of the law aspects of Cybercrime and Cybersecurity issues is designed to begin the dialogue between the technology side and the law side about how to collaborate by being familiar with issues in each other's fields. Both communities need to meet regularly in various fora to ensure that they are not talking past each other, but to each other. Having attended several APEC meetings related to these topics, my concern is that developing countries may not fully understand the issues involved and that is why they are stalled in designing, adopting and implementing laws. In addition, there may not be adequate training offered to the law and technology sides in the respective economies, whether in workshops, conferences and seminars, or in ongoing university and continuing education programs.

The dialogue has to continue, for example, by building law standards into the security standards adopted in each country, by creating interdisciplinary courses taught by law and technology professionals together in university undergraduate and graduate programs, professional schools, as continuing education for members of the public, as in-service training for police, prosecutors, judges, and legislators.

Take a look around you. What resources do you have in your country? What are the needs of the law and technology communities, the legislators, and even the general public to understand the issues described here and to address them?

12. Reference and Resources for Further Information about these Topics

- a) Australian Institute of Criminology, "Concepts and terms: New crimes and old crimes committed in new ways", 1/05, <http://www.aic.gov.au>.
- b) Susan W. Brenner, "Is there such a thing as 'virtual crime'?" (2001), 4 Cal. Criminal Law Review 1 [4], <http://www.boalt.org/bjcl/v4/v4brenner.htm>.

- c) Center for Democracy and Technology, International Issues: Cybercrime, <http://www.cdt.org.international/cybercrime>.
- d) James X. Dempsey and Ira Rubinstein, "Lawyers and Technologies: Joined at the Hip?" IEEE SECURITY AND PRIVACY, May/June 2006, <http://www.computer.org/security/>, pages 15-19.
- e) Richard W. Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime", 43 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 705 (2005).
- f) Tom Espiner, "Yahoo calls for 'effective' cybercrime laws", ZDNet UK, 31 March 2006, <http://www.zdnet.co.uk/>.
- g) Sarah Gordon and Richard Ford, "On the definition and classification of Cybercrime", JOURNAL IN COMPUTER VIROLOGY, Vol. 2, No. 1, August 2006.
- h) Beryl Howell, "Ambiguities in U.S. law for investigators", Digital Investigation (2004), 1, 106-111.
- i) ITU global portal, Cybersecurity Gateway, http://www.itu.int/cybersecurity.laws_legislation.html.
- j) ITU Guide de la cybersécurité pour les pays en développement (Cybersecurity Handbook for Developing Countries), 2006 (available in French only at this time), http://www.itu.int/ITU-D/e-strategies/publications-articles/pdf/CyberSecurity/Cyber-Security_F.pdf (Includes a chapter on Cybercrime).
- k) Bert Jaap Koops and Susan W. Brenner, Editors, CYBERCRIME AND JURISDICTION; A GLOBAL SURVEY, T.M.C. Asser Press, The Hague, 2006.
- l) Declan McCullagh, "Senate ratifies controversial cybercrime treaty", 7 August 2006, http://news.com/cm/Senate+ratifies+controversial+cybercrime+treaty/2100-7348_3-6102354.html.

- m) RAND Europe and Lawfort, HANDBOOK OF LEGAL PROCEDURES OF COMPUTER AND NETWORK MISUSE IN EU COUNTRIES FOR ASSISTING COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTS), http://www.csirt_handbook.org.uk/ (Note: Discusses EU only).
- n) Pauline C. Reich, General Editor, CYBERCRIME AND SECURITY, Oceana Publications, a division of Oxford University Press, about 3000 pages, looseleaf series updated regularly.
- o) Ryan Singel, "Judge: NSA Case Can Proceed", Wired News, 20 July 2006, <http://www.wired.com/news/technology/1,71432-0.html>.
- p) U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, NIJ Special Reports, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER NETWORKS, January 2007, <http://www.ncjrs.gov/pdffiles1/nij/210798.pdf>.
- q) Matthew Williams, "Cybercrime" in J. Mitchell Miller, Ed., ENCYCLOPAEDIA OF CRIMINOLOGY, London: Routledge, 2005?
<http://www.cf.ac.uk/socsi/williamsm/Williams,%20M%20-%20Encyclopedia%20of%20Criminology.pdf>.
- r) Mark Williams, "The Total Information Awareness Project Lives On", TECHNOLOGY REVIEW, 26 August 2006,
http://www.technologyreview.com/read_article.aspx?ch=infotech&sc=&id=16741&pg=1#.
- s) Wm. A. Wulf and Anita K. Jones, Cybersecurity, THE BRIDGE, National Academy of Engineering of the National Academies, Vol. 32, No. 1, Spring 2002,
<http://www.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-58NLKV?OpenDocument>.

Prof Pauline C. Reich

J.D., M.A.

Professor, Waseda University School of Law, Tokyo, Japan

*Vice Chair, E-payments Subcommittee
American Bar Association Section of Science and Technology*

*General Editor, CYBERCRIME AND SECURITY
(Oceana Publications, a division of Oxford University Press)*

*Director
Asia-Pacific Cyberlaw, Cybercrime and Internet Research Institute
Waseda University, Tokyo, Japan*



Professor Pauline C. Reich is a Professor with the Waseda University School of Law in Japan. She is also an American Lawyer and Professor, and the Director for Asia-Pacific Cybercrime and Internet Security Institute. She conducts research, publishes publications, provide technical assistance, provide training for lawyers, judges, prosecutors, police, legislators, businesses and the governments in the Asia-Pacific region and worldwide.

Prof Reich is also the General Editor, Cybersecurity and Security (Oceana Publications, New York), a 3-volume series on law and Cybersecurity issues worldwide. This publication covers 25 countries worldwide, and it is being updated quarterly.

Prof Reich aims to create an interdisciplinary dialogue among law, business, government and the technology sectors, and to establish international dialogues for global cooperation.

Her current planned projects are research and training, Cybercrime/Security issues; translation, materials for training in developing countries; and also ongoing publications on emerging issues from legal and security perspectives.