ITU standardization for Cybersecurity

(focus on ITU-T Study Group 17)

12 November 2007

Xiaoya Yang

International Telecommunication Union (ITU)

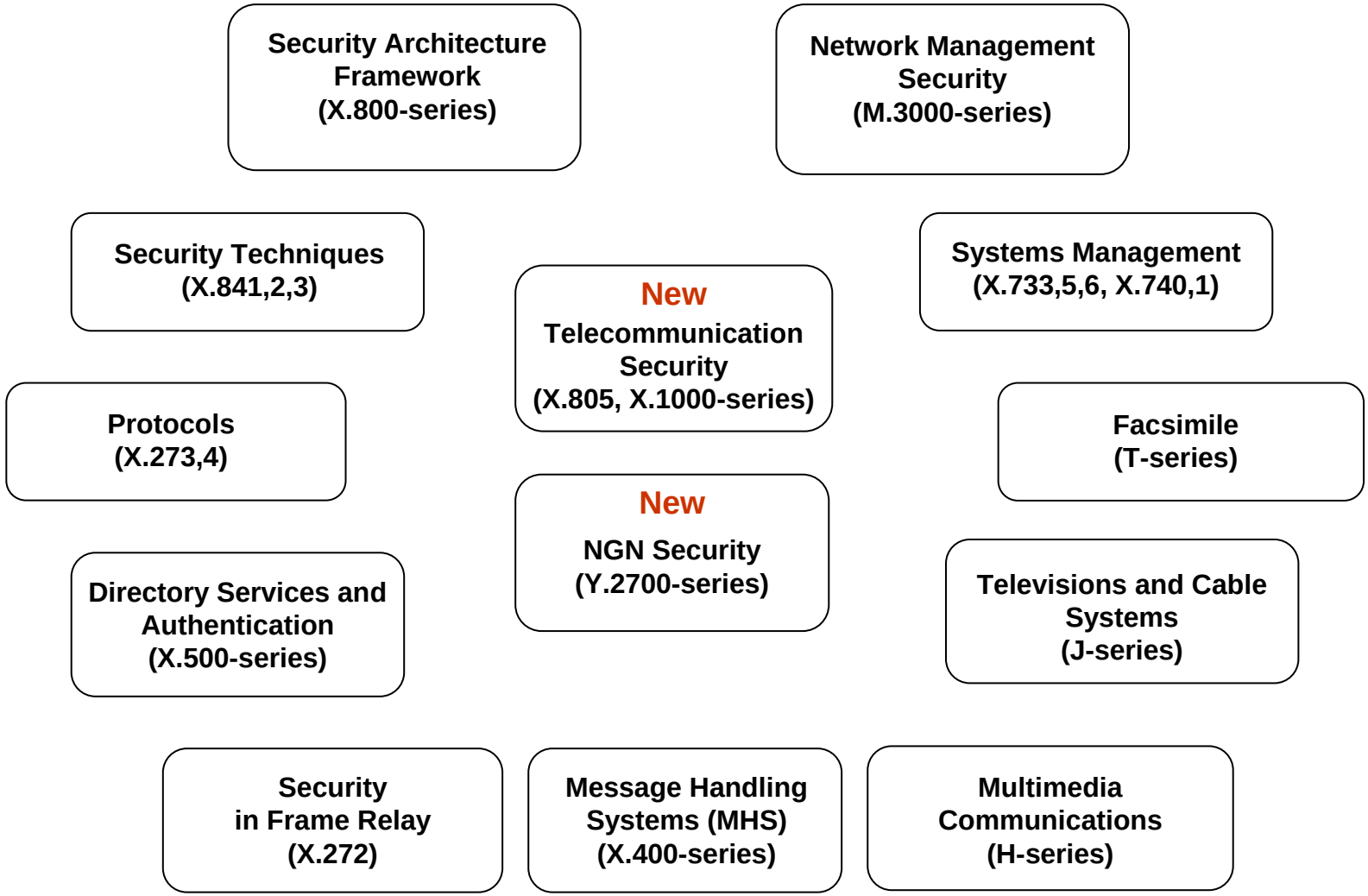
International Telecommunication Union

Every time someone, somewhere:

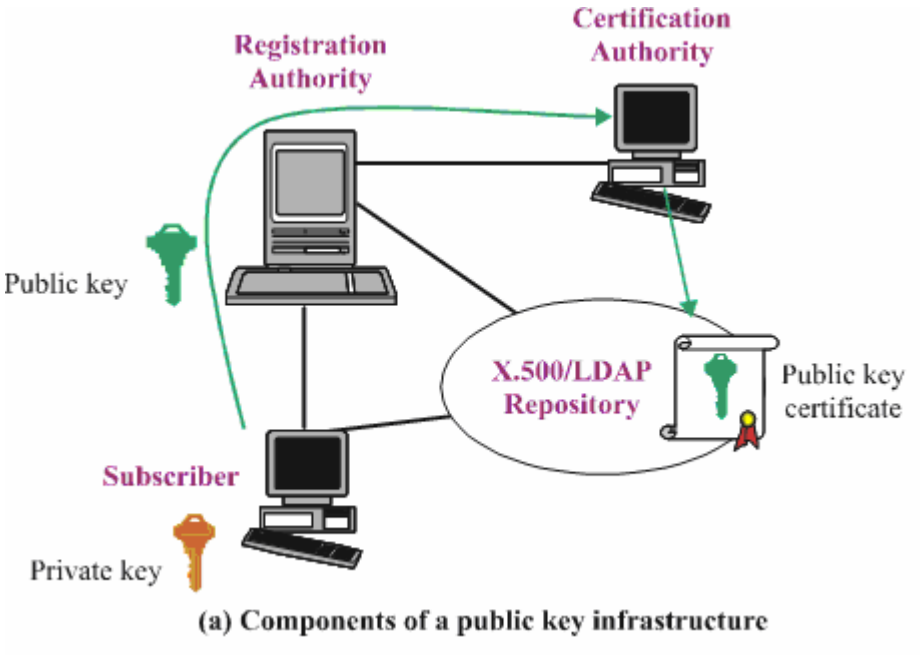
- picks up a telephone and dials a number,
- answers a call on a mobile phone,
- sends a fax or receives an e-mail,
- takes a plane or a ship,
- listens to the radio,
- watches a favorite television programme,
- helps a small child master the latest radio-controlled toy,
- access the services of the network,
- is alerted about emergencies

he benefits from the work of the ITU.

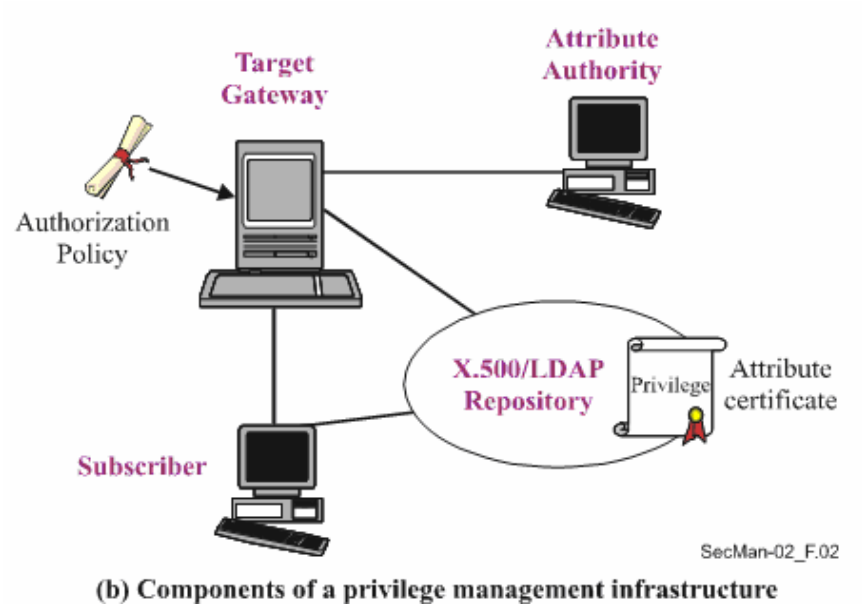
ITU-T Security Building Blocks



ITU-T Recommendation X.509 (PKI and PMI)

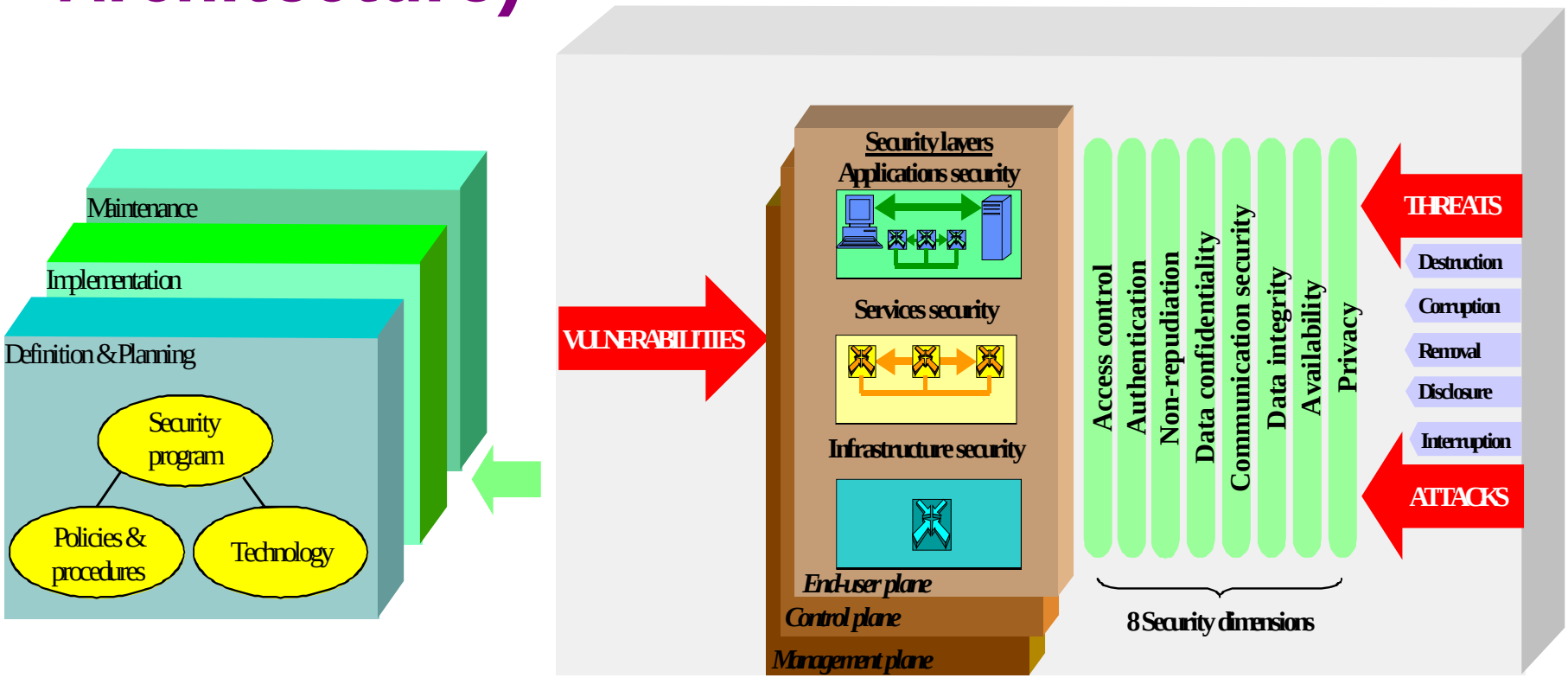


(a) Components of a public key infrastructure



(b) Components of a privilege management infrastructure

ITU-T Recommendation X.805 (Security Architecture)



X.805_F4

Study Group 17: Lead Study Group on Telecommunication Security

Specific Systems, Services, Applications Security in ITU-T are developed by SG 2, 3, 4, 5, 6, 9, 11, 13, 15, 16, 19

Core Technology and Common Security Techniques in ITU-T are developed by SG 17



ISO/IEC SC 27, 37 | IETF | ANSI, ETSI, OASIS, etc.

Study Group 17 products

- 100+ Recommendations approved on security for communications; 50+ work items of draft new or revised Recommendations underway
- Security Manual: *Security in Telecommunications and Information Technology* – an overview of existing ITU-T Recommendations for secure telecommunications
- Security Compendium
  - catalogue of approved ITU-T security Recommendations
  - extract of ITU-T approved security definitions
  - listing of ITU-T security related Questions

Telecom Systems Users

Telecom Systems

Telebiometrics
Q.8/17

* Multimodal model framework
* System mechanism
* Protection procedure

Security Management
Q.7/17

* ISMS-T
* Incident management
* Risk assessment methodology

Q.4/17

Secure Communication Services
Q.9/17

* Secure mobile communications
* Home network security
* Web services security

Cyber Security
Q.6/17

* Vulnerability information sharing…
* Incident handling operations
* Identity management

Countering spam by technical means
Q.17/17

* Technical anti-spam measures

Security Architecture and Framework
Q.5/17

* Architecture,
* Model,
* Concepts,
* Frameworks

Communications System Security Project *Vision, Project, Roadmap, …

Recently approved security Recommendations (Free online!)

M.3016.0, 1, 2, 3, 4	Security for the management plane: Overview, Security requirements, Security services, Security mechanism, Profile proforma
X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
X.805	Security Architecture for Systems Providing End-to-End Communications
X.893	Information technology – Generic applications of ASN.1: Fast Infoset security
X.1035	Password-authenticated key exchange (PAK) protocol
X.1051	Information security management system - Requirements for telecommunications (ISMS-T)
X.1081	The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics
X.1111	Framework for security technologies for home network
X.1121	Framework of security technologies for mobile end-to-end communications
X.1122	Guideline for implementing secure mobile systems based on PKI
X.1141	Security Assertion Markup Language (SAML 2.0)
X.1142	eXtensible Access Control Markup Language (XACML 2.0)
X.1303	Common Alerting Protocol (CAP 1.1)
Y.2701	Security requirements for NGN release 1

Work in progress: Extract from the current SG 17 security work

Q.	Acronym	Title or Subject
5	X.akm	Framework for EAP-based authentication and key management
6	X.1205	Overview of cybersecurity
6	X.idmf	Identity management framework
6	X.gopw	Guideline on preventing worm spreading in a data communication network
7	X.1051 (Revised)	Information security management guidelines for telecommunications based on ISO/IEC 27002
7	X.rmg	Risk management guidelines for telecommunications
8	X.bip	BioAPI interworking protocol
8	X.tai	Telebiometrics authentication infrastructure
9	X.homesec-2, 3, 4	Certificate profile for the device in the home network, User authentication mechanisms for home network service, Authorization framework for home network
9	X.msec-3	General security value added service (policy) for mobile data communication
9	X.p2p-1	Requirements of security for peer-to-peer and peer-to-multi peer communications
9	X.websec-3	Security architecture for message security in mobile web services
17	X.csreq	Requirement on countering spam
17	X.fcsip	Framework of countering IP multimedia spam

Many more in SG 17 work plan … 53 x items (Summaries available online)

Work in progress:

NGN, Multimedia, IPTV, digital satellite Security

Y.IdMsec	NGN identity management security
Y.NGN AAA	AAA application for implementation of network and service security requirements over NGN
Y.NGN Authentication	NGN Authentication
Y.NGN Certificate Management	NGN certificate management
Y.SecMechanisms	NGN Security mechanisms and procedures
Y.SecReqR2	Security requirements for NGN release 2
H.235	Security and encryption for H-series multimedia systems
J.170	IPCablecom Security Specification
S.1250	Network management architecture for digital satellite systems
S.1711	Performance enhancements of transmission control protocol over satellite networks

Identity management standards: emerging importance

THE PROBLEM:

- Identity theft… security breaches… malware attacks…insider threats… synthetic identities… phishing…data leakage… Whatever label is attached to the problem, identity management and information protection are huge issues with which all of society must grapple. And no one is exempt-- from government, law enforcement, business, health care, academe, non profit to citizens. The problem is ubiquitous.

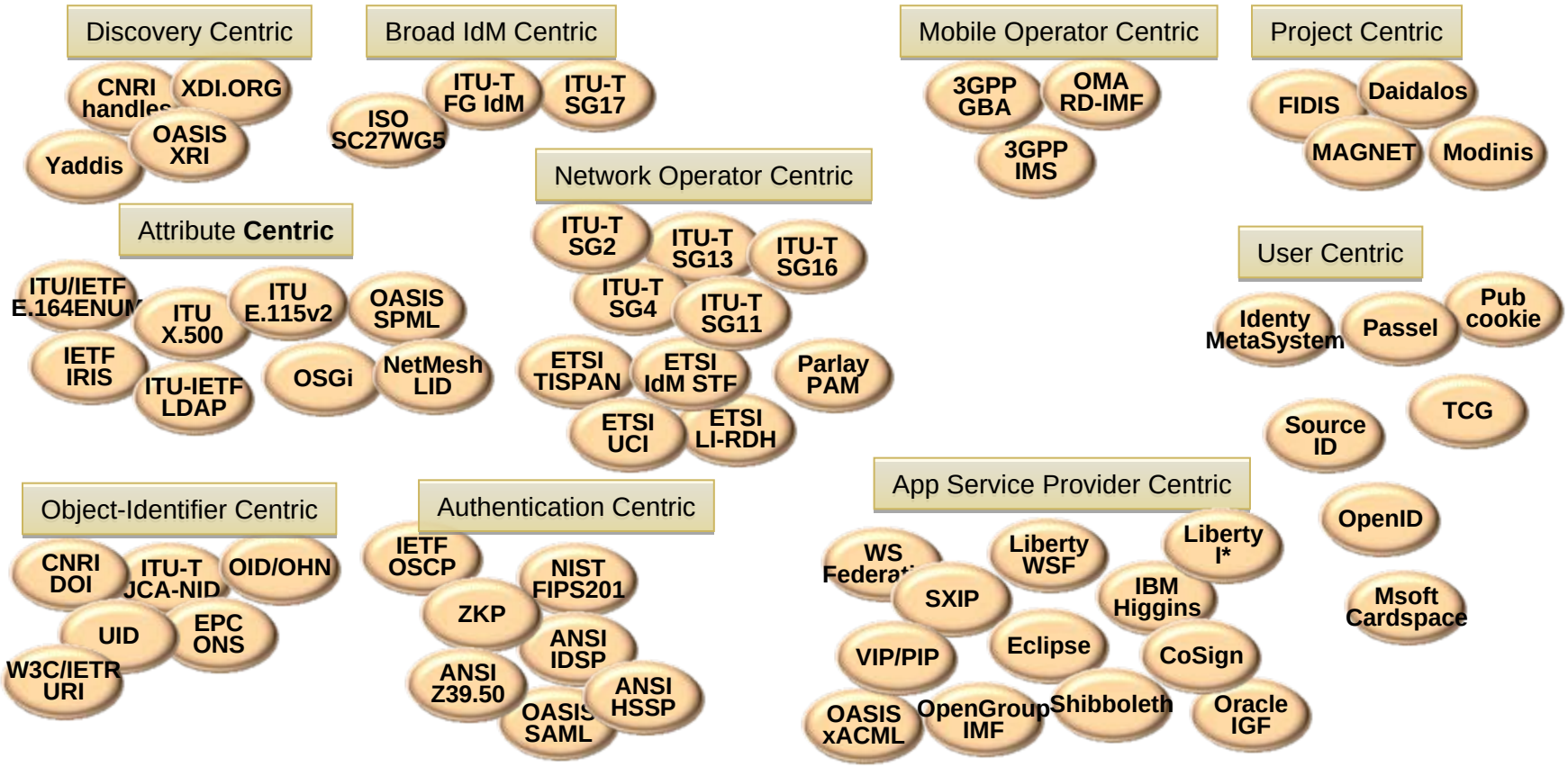
ADDRESSED TO:

- Fraud investigators…information officers…security officers…fraud managers…law enforcement…corporate security…internal auditors…information managers…management consultants…standards organizations

FOR:

- Managing data, storage, register, authorize, individuate,…

Expansive ecosystem on IdM standardization



Collaboration is key factor for standardization

- Identity Management:
  - Focus Group on Identity Management (Dec 06- Sept 07)
  - Work continues in SG 17; New phase of cooperation will start Jan 08
- World Standards Cooperation (WSC) **ISO, IEC, ITU**
  - **ISO IEC ITU-T** Strategic Advisory Group on Security
- Global Standards Collaboration (GSC) **Regional, National SDOs and ITU-T, ITU-R**

ICT security standards roadmap: a collaboration tool

- Part 1 contains information about organizations working on ICT security standards
- Part 2 is a searchable database of existing security standards, currently includes ITU-T, ISO/IEC JTC 1, IETF, IEEE, ATIS, ETSI and OASIS security standards
- Part 3 will be a list of standards in development
- Part 4 will identify future needs and proposed new standards
- Part 5 is now being built and includes Security Best Practices

ENISA and Network and Information Security Steering Group (NISSG) are now collaborating with ITU-T in the development of the Roadmap

Conclusions

- Security is **everybody's business, and an ongoing effort**
- Standards are **key building blocks for cybersecurity**
- Security needs to be **designed in upfront**
- ITU is uniquely positioned to lead the security standardization work:
  - Industry-government partnership
  - Taking into account the needs of developing countries
  - Collaboration with other SDOs

Some useful web resources

- ITU-T Home page www.itu.int/ITU-T
- Study Group 17 www.itu.int/ITU-T/studygroups/com17
  e-mail: tsbsg17@itu.int
- Recommendations www.itu.int/ITU-T/publications/recs.html
- ITU-T Lighthouse www.itu.int/ITU-T/lighthouse
- ITU-T Workshops www.itu.int/ITU-T/worksem
- Security Roadmap www.itu.int/ITU-T/studygroups/com17/index
- Contribution to IGF

http://www.intgovforum.org/Substantive_2nd_IGF/ITU_TSB_4_Security%20initiatives.pdf

Thank you

杨晓雅 (Xiaoya Yang)
Telecommunication Standardization Bureau
International Telecommunication Union

xiaoya.yang@itu.int