ITU-T Security Manual - 4th edition

- Security requirements and architectures
- Aspects of security management
- Directory, authentication and identity management
- Securing the network infrastructure
- Specific approaches to network security
- Application security
- Counteracting common network threats
- The future of ICT/telecommunications security standardization future

ICT Security Standards Roadmap

Part 1: ICT Standards Development Organizations and their work

Part 2: Approved ICT security standards (database with direct links)

Part 3: Security standards under development

Part 4: Future needs and proposed new security standards proposed, and

Part 5: Best practices.

Part 6: Identity Management (IdM) landscape.

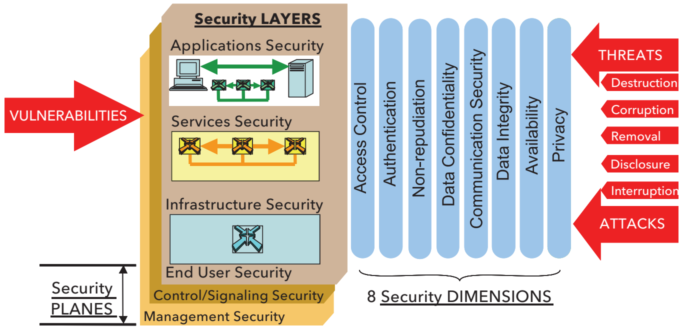
Security Compendia

- Catalogue of approved Recommendations related to telecommunication security
- List of security definitions extracted from approved ITU-T Recommendations
- Summary of ITU-T Study Groups with security-related activities
- Summary of Recommendations under review for security considerations
- Summary of other ITU security activities.

Security Architectures

Rec. ITU-T X.805 "Security Architecture for Systems Providing End-to-End Communications", as well as a number of application-specific architectures, were developed to address areas such as network management, peer-to-peer communications and mobile web servers.

The X.805 architecture, illustrated above, is defined in terms of three major concepts for an end-to-end network: Security Layers, Security Planes and Security Dimensions. A hierarchical approach is taken in dividing the security requirements across the layers and planes, ensuring end-to-end security is achieved.



This architecture can be used as the basis of a security assessment or to guide the development of security policy, incident response and recovery plans, and technology architectures, by taking into account the applicable security dimension at each security layer and plane during the definition and planning phase.

www.itu.int/itu-t/studygroups

International Telecommunication Union

Security

Building confidence and security in the use of ICTs (WSIS – Action Line C.5)

01.2012 tsbpromo@itu.int

ITU-T

ICT/telecommunications security

The ITU-T work on ICT/telecommunications security has been underway for over two decades. Several Study Groups have developed recommendations and guidance in a number of key areas. Study Group 17 has primary responsibility for the ITU-T security work and has been designated the Lead Study Group on security.

Assets Protection

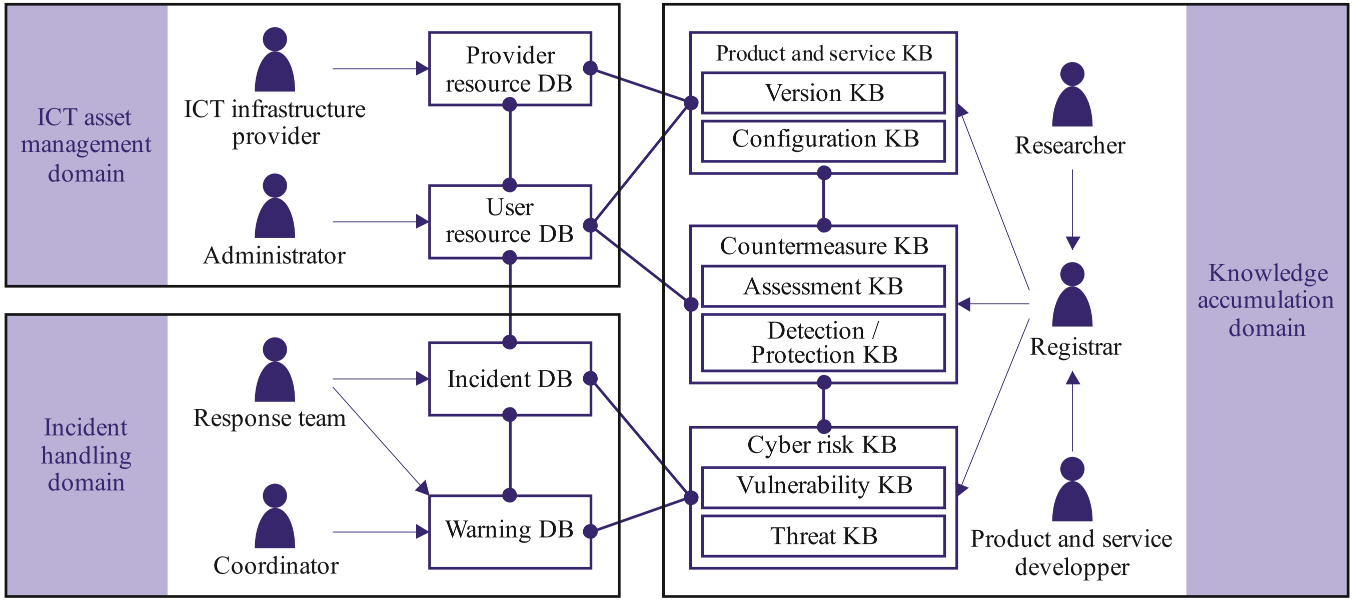
In general terms, we need to protect assets for the following parties:

- Customers/subscribers who need confidence in the network and the services offered, including availability of services (especially emergency services);
- Public community/authorities who demand security by directives and/or legislation, in order to ensure availability of services, fair competition and privacy protection; and
- Network operators/service providers themselves which need security to safeguard their operation and business interests and to meet their obligations to customers and the public, at the national and international level.

ITU-T Rec. Series X.1500 – Global exchange of cybersecurity information

CYBEX series present techniques for exchanging cybersecurity information, by means of the following basic functions, that can be used separately or together, as appropriate:

- structuring cybersecurity information for exchange purposes;
- identifying and discovering cybersecurity information and entities;
- establishment of trust and policy agreement between exchanging entities;
- requesting and responding with cybersecurity information;
- assuring the integrity of the cybersecurity information exchange.



DB = Database, KB = Knowledge Base

X.1500(11)_F01a

The figure above illustrates CYBEX ontology, presented under the form of an operational context. Cybersecurity operations principally consist of three domains: Incident handling, ICT asset management and knowledge accumulation.