Technical measures to fight cybercrime

Asia-Pacific Regional Workshop on Fighting Cybercrime
Seoul, Republic of Korea, 21-23 September 2011

Heung Youl Youm
Vice-chairman of ITU-T Study Group 17
Chairman of ITU-T Study Group 17 Working Party 2
hyyoum@sch.ac.kr

International Telecommunication Union
Committed to connecting the world

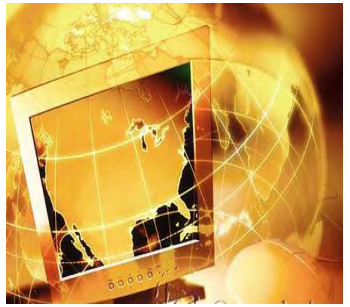
Contents - Overview

- Part 1 – introduction
  - Cybersecurity Threats and Challenges
  - Glowing cybersecurity threats
  - Key cybersecurity challenges
  - Cybercrimes
  - Technical measure to fight cybercrimes
- Part 2 - ITU-T cybersecurity standardization activities
  - Security activities in other ITU-T Study Groups
  - ITU-T SG 17 cybersecurity activities and results
  - CYBEX basics, model, and overview of CYBEX clusters
  - Identity Management Collaboration
  - Security aspect for ubiquitous telecommunication service
  - Secure application service
  - ITU SG 17's Child Online Protection
  - ITU-T SG 17's response to Memorandum of Understanding (MoU) between the ITU and the United Nations Office on Drugs and Crime (UNODC)

Part 1 - Introduction

Growing Cybersecurity Threats

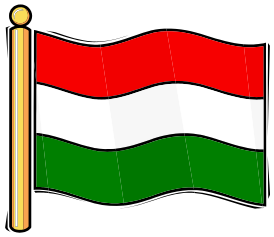
- ICTs have become an integral part of information society.
- ICT networks are regarded as basic national infrastructure.
- ICTs are also exposing our societies to the threat of cyber war/cyber attacks/cyber crimes.
- Vulnerability of national infrastructures increases as the use of ICTs take root.
- Cyber attacks on ICTs are borderless and can be launched from virtually across the frontiers anywhere.
- As global reliance on ICTs grows, so does vulnerability to attacks on critical infrastructures through cyberspace.



No geographical borders, no boundaries and tremendous destructive power

Cybercrimes

- Computer crime, or *cybercrime*, refers to any crime that involves a computer and a network.
- According to the Budapest Convention on cybercrime, the following are types of cybercrimes:
  - Offences against the confidentiality, integrity and availability of computer data and systems, such as Illegal access, Illegal interception, Data interference, System interference (DDoS), Misuse of devices;
  - Computer-related offences such as Computer-related forgery, Computer-related fraud;
  - Content-related offences such as Offences related to child pornography;
  - Offences related to infringements of copyright and related rights such as Offences related to infringements of copyright and related rights;
  - Ancillary liability and sanctions such as Attempt and aiding or abetting , Corporate liability.



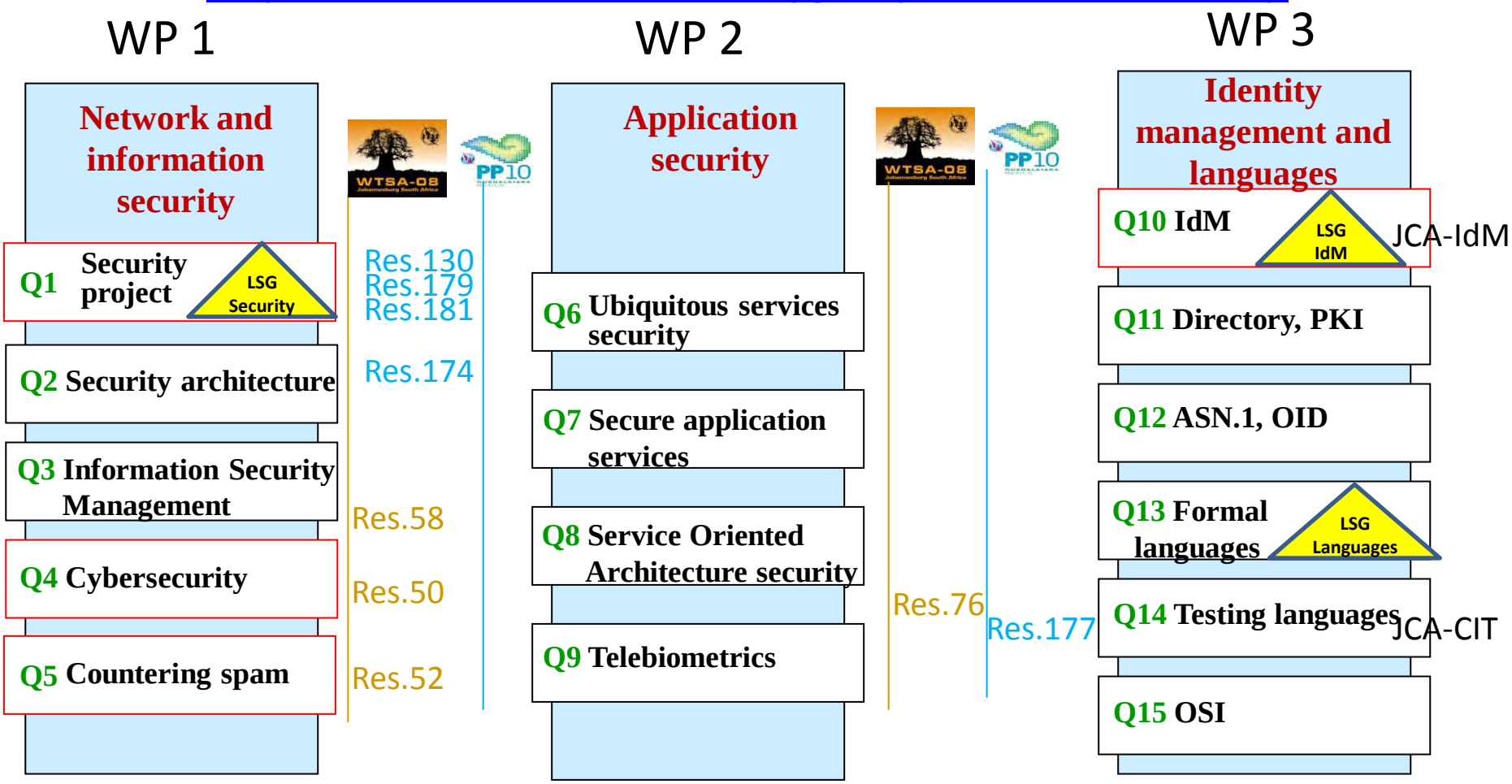
Technical standards to fight cybercrimes

- **Cyber attacks** continue to be widespread; they cause a complex range of problems to users, service providers, operators and networks.
- **Spam** has become a widespread problem causing potential loss of revenue to Internet service providers, telecommunication operators, mobile telecommunication operators and business users around the globe.
- **Due to wide deployment of ubiquitous sensor networks application,** security threats have received a lot of attention to provide services in a secure and trust manner.
- **Identity theft** continues to increase in cyber space. It is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Countering identity theft and fraud by technical means is needed urgently.
- **Countering cyber attacks, spam, and identity theft by technical means** requires development of frameworks and requirements for: detecting and protecting against them; and mitigating and recovering from their effects through exchanging cybersecurity information.
- Therefore, **technical standards** could be used to prevent, detect, and respond to the cybercrimes.

Part 2 -
ITU-T Cybersecurity standardization activities

ITU-T Study Group 17 “Security”

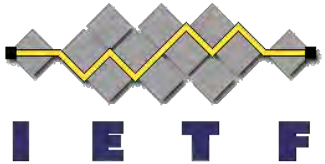
http://www.itu.int/ITU-T/studygroups/com17/index.asp



Res.50: Cybersecurity
Res.52: Anti-SPAM
Res.58: National CIRTs
Res.76: Conformance & Interoperability

Res.130: Security & Confidence in ICT
Res.174: Illicit use of ICT
Res.177: Conformance & Interoperability
Res.179: Child Online Protection
Res.181: Defs & Terms on ICT security, confidence

Coordination with other bodies



ITU-D, ITU-R, xyz…

Definition of Cybersecurity

(ref. Recommendation ITU-T X.1205, Overview of cybersecurity)

- Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
  Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
- Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.
  The general security objectives comprise the following:
  - Availability
  - Integrity, which may include authenticity and non-repudiation
  - Confidentiality.

Major accomplishments (1)

X.1200 – X.1229 allocated to Cybersecurity

❑ Cybersecurity

- **X.1205** Overview of cybersecurity

New

- **X Suppl. 8** to ITU-T X.1205 – Supplement on best practices against botnet threats

New

- **X Suppl.9** to ITU-T X.1205 - Supplement on guidelines for reducing malware in ICT networks

New

- **X Supple.10 to ITU-T X.1205-**Usability of network traceback
- **X.1206** A vendor-neutral framework for automatic notification of security related information and dissemination of updates
- **X.1207** Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software
- **X.1209** Capabilities and their context scenarios for cybersecurity information sharing and exchange
- **X.dexf** digital forensics exchange format

Major accomplishments (2)

X.1500-series Recommendations allocated to Cybersecurity information exchange (CYBEX)

- **Cybersecurity information exchange**
  - **X.1500** Overview of cybersecurity information exchange (CYBEX) — New
- **Vulnerability/state exchange**
  - **X.1520** Common vulnerabilities and exposures (CVE) — New
  - **X.1521** Common vulnerability scoring system (CVSS) — New
  - **X.1524 (X.cwe)** Common weakness enumeration (CWE) — Determined
- **Identification and discovery**
  - **X.1570** Discovery mechanisms in the exchange of cybersecurity information — New
  - **X.1500.1 (X.cybex.1),** Procedures for the registration of arcs under the object identifier (OID) arc for cybersecurity information exchange — Determined
- **Data Representation**
  - **X.1541 (X.iodef),** Incident object description exchange format — Determined

- 34 active work items on cybersecurity are in the Q4/17 pipeline and are being progressed towards Recommendations.

Question 4/17 “Cybersecurity” activities

- Security assurance mechanisms in telecommunication networks for service providers
- Development and sharing of best practices in the cyber environment
- Sharing of vulnerabilities information
- Framework for security information sharing; enhancements and refinements of cybersecurity information exchange techniques
- Malware attribute, vulnerability, weakness, misuse, attack pattern enumeration and classification
- Assessment result format, Common event expression, Digital forensics exchange format, Incident object description exchange, Extensible configuration checklist description format
- Discovery mechanisms in the exchange of cybersecurity information
- Guideline for reducing malware in ICT networks
- Guideline on cybersecurity index
- Abnormal traffic detection
- Framework for Botnet detection and response
- Traceback scenarios, capabilities, mechanisms
- Techniques for preventing web-based attacks
- Requirements and solutions for telecommunications/ICT using digital forensics, trace-back, to counter cyber stalking and fraud.
- Cybersecurity index computation from usage and measurement of indicators
- Distributing policies for network security
- Usage of networks to provide critical services in a secure fashion during national emergency.

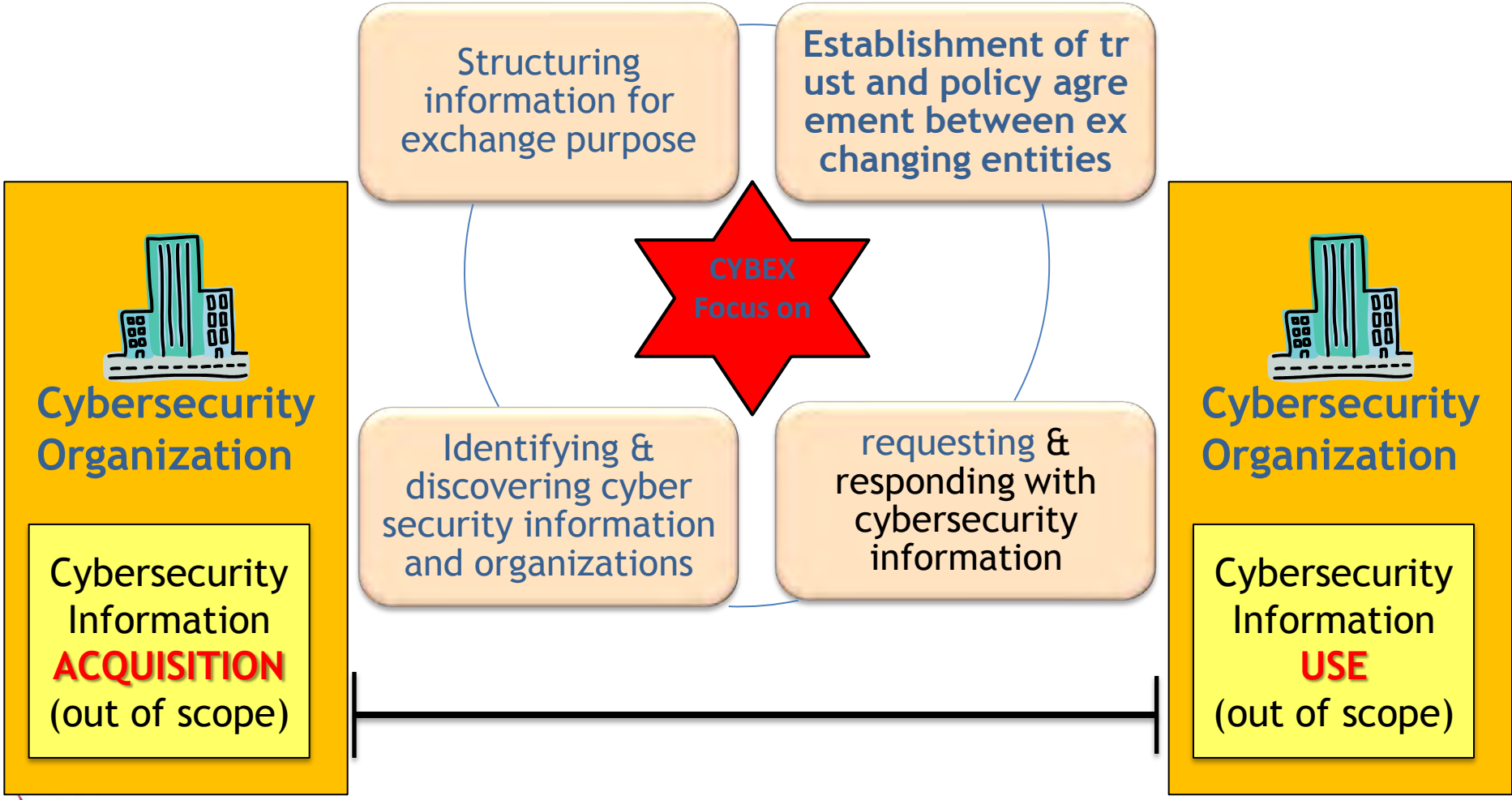
CYBEX Basics

(CYBEX = Cybersecurity information exchange)

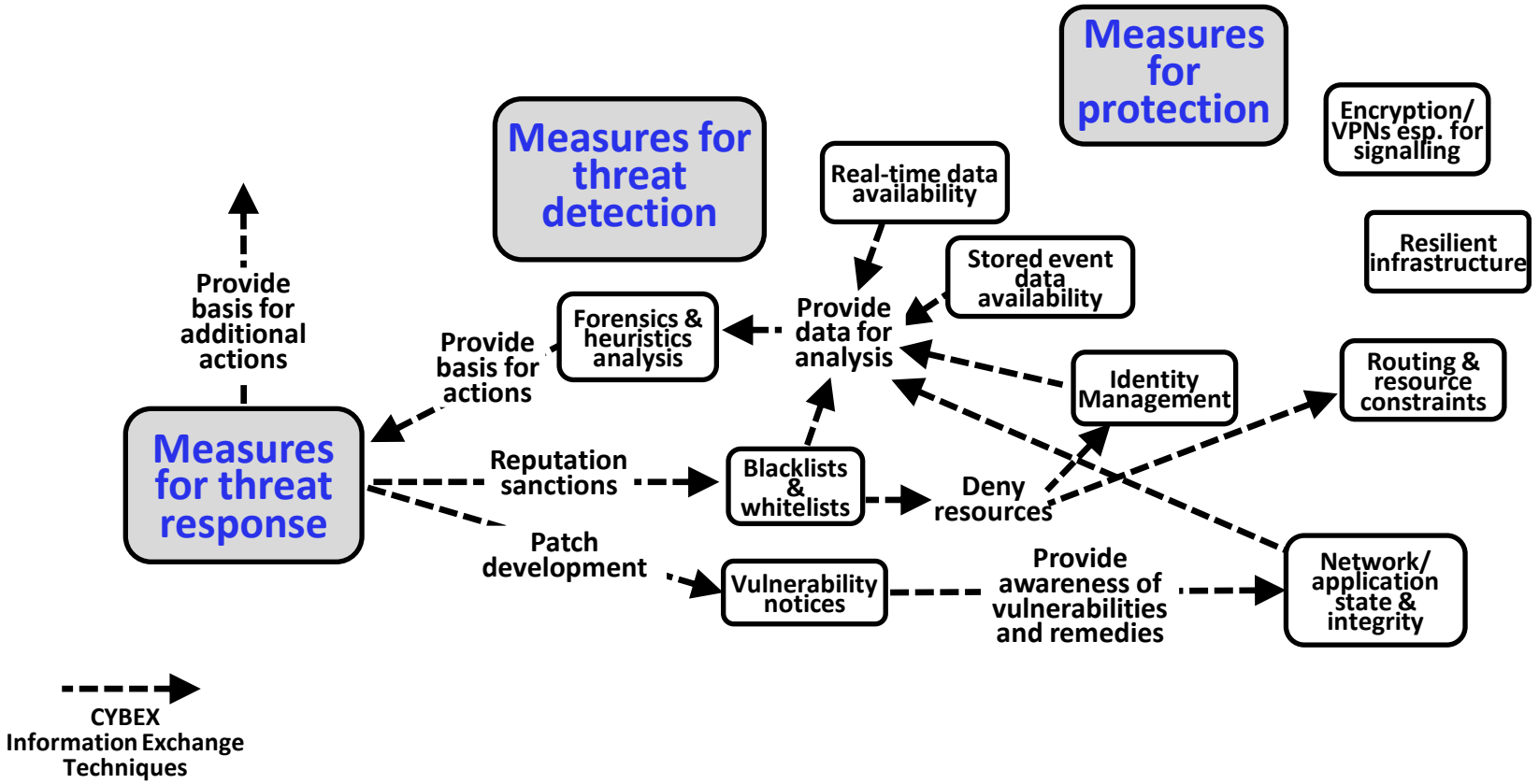
- The new cybersecurity paradigm
  - know your weaknesses
    - minimize the vulnerabilities
  - know your attacks
    - share the heuristics within trust communities
- CYBEX – techniques for the new paradigm
  - Weakness, vulnerability and state
  - Event, incident, and heuristics
  - Information exchange policy
  - Identification, discovery, and query
  - Identity assurance
  - Exchange protocols
  - Evidence of incidents
- X.1500 completes a broadly supported 2-year effort
- Consists of a non-prescriptive, extensible, complementary "collection of tools" that can be used as needed

The CYBEX Initiative:

basic model for information exchange



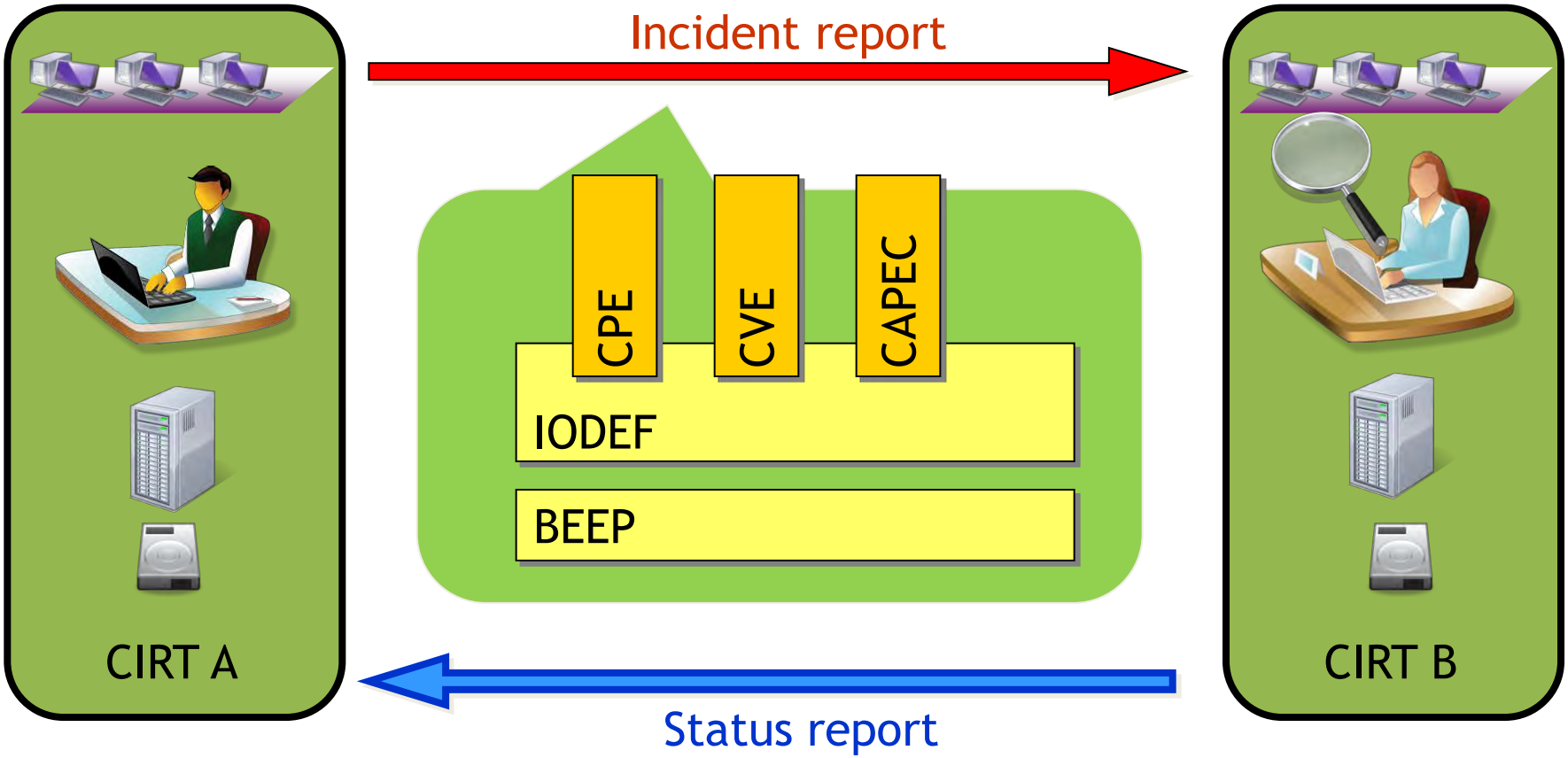
CYBEX Facilitates a Global Cybersecurity Model



Global standardization activity

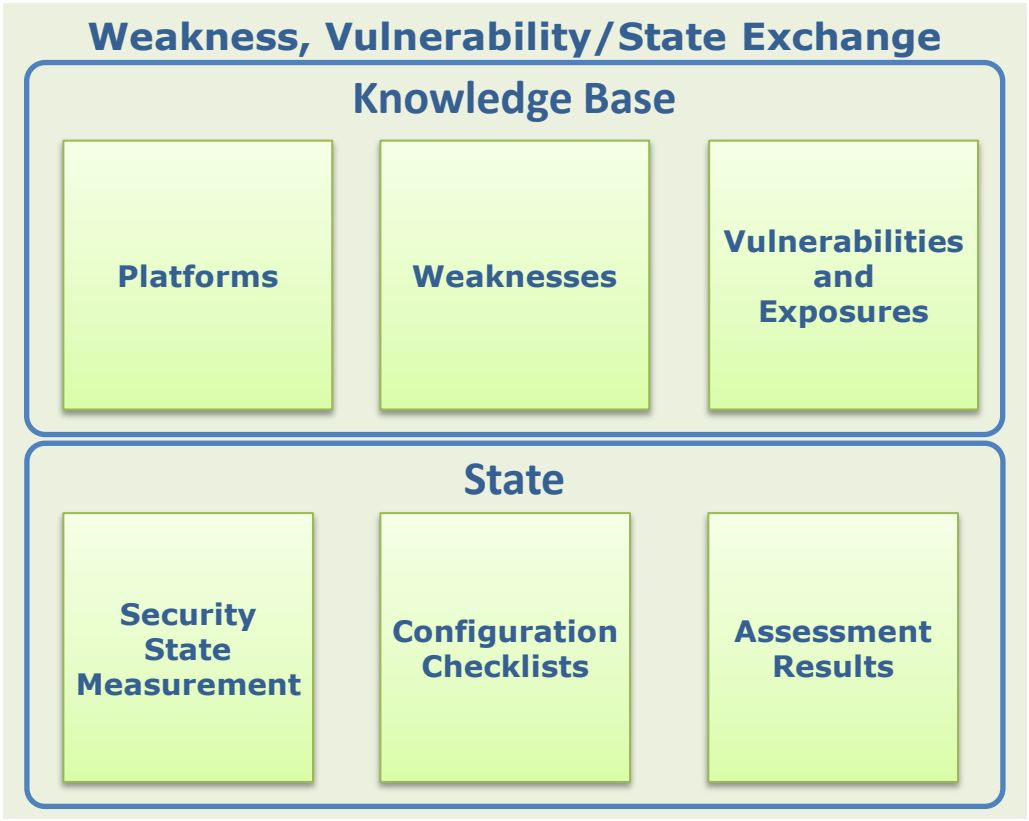
- Activity for cybersecurity information exchange (CYBEX) framework
  - initiated from September, 2009 at ITU-T SG 17 Question 4, Cybersecurity
  - Recommendation ITU-T X.1500, Overview of cyber security information exchange (approved)
- A Global initiative(CYBEX) to
  - Identify a set of platform specifications to facilitate the trusted exchange of information among responsible parties worldwide supporting cybersecurity for Infrastructure protection, Incident analysis and response, and Law enforcement and judicial forensics
  - Enhance the availability, interoperability, and usefulness of these platforms

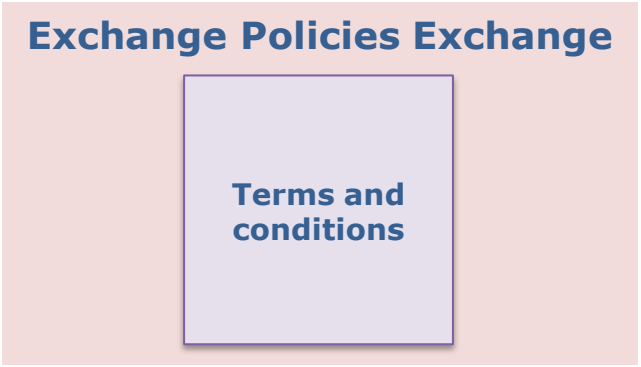
Concept of Cybersecurity Information Exchange



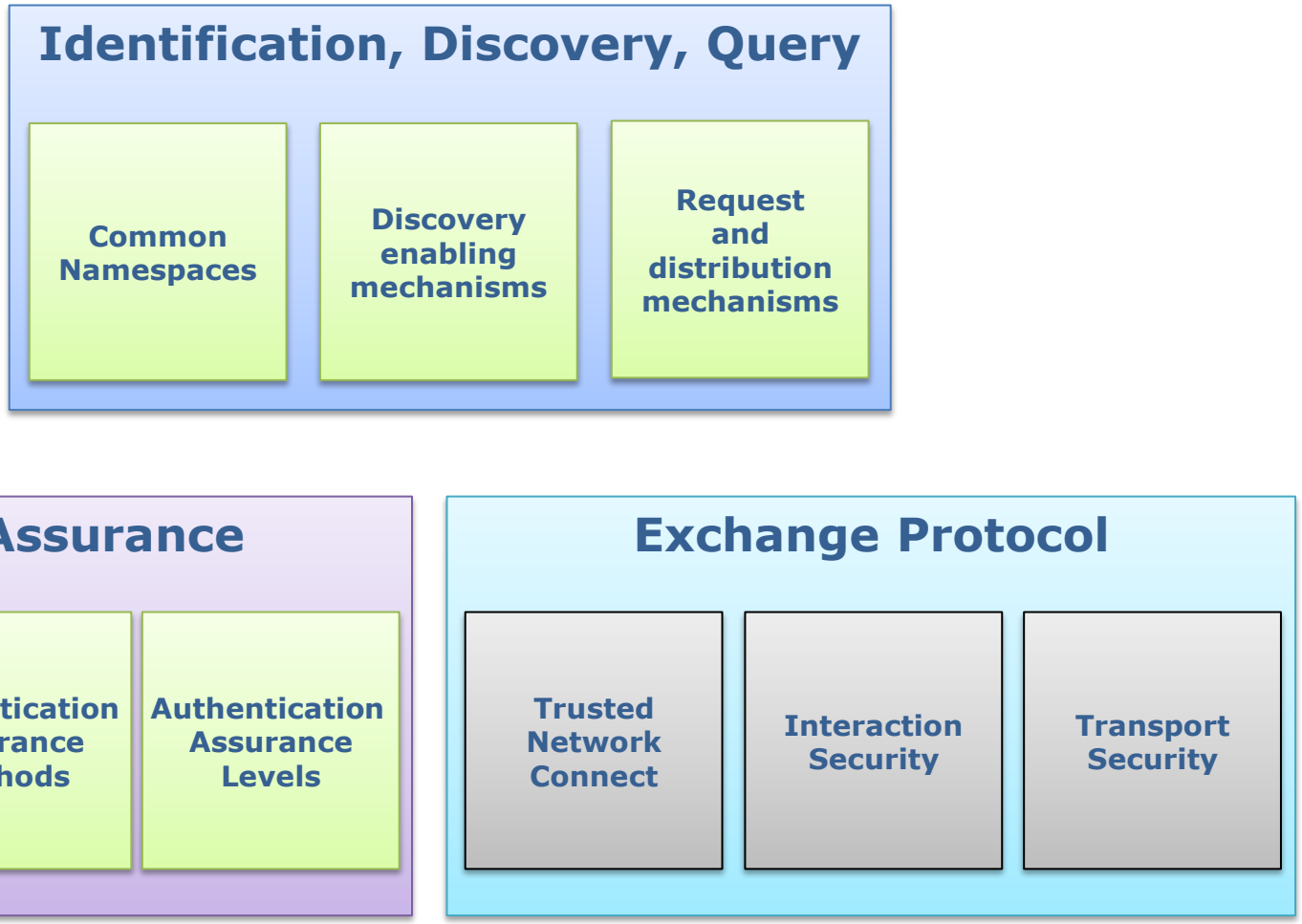
- IODEF: Incident Object Description and Exchange Format, CPE: Common Platform Enumeration
- CVE : Common Vulnerabilities and Exposures , CAPEC : Common Attack Pattern Enumeration and Classification

CYBEX Technique Clusters: Structured Information





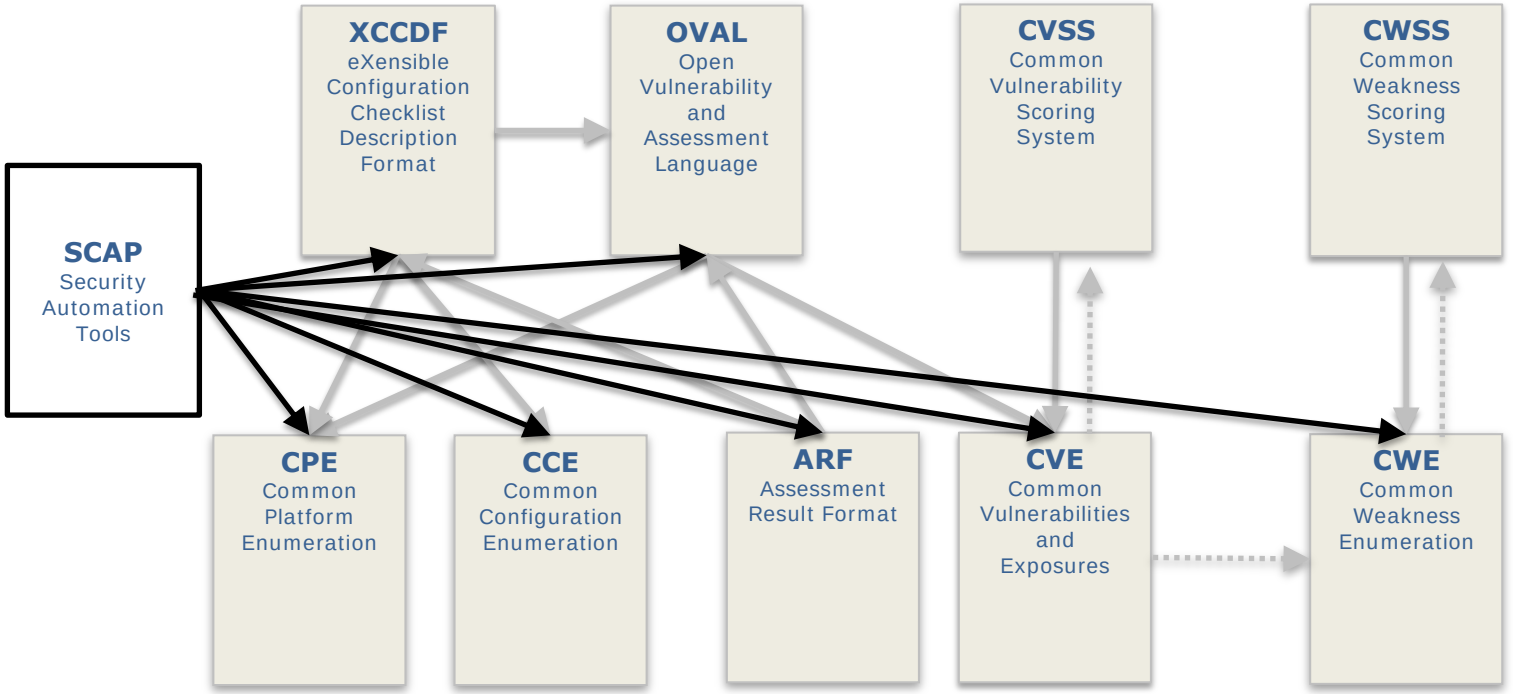
CYBEX Technique Clusters: Utilities



International Telecommunication Union

Committed to connecting the world

Toward Network Security Planes: Security Automation Schemas Everywhere



Major accomplishments (3)

X.1230 – X.1249 allocated to Countering spam

- **Countering spam**
  - **X.1231** Technical strategies on countering spam
  - **X.1240** Technologies involved in countering e-mail spam
  - **X.1241** Technical framework for countering e-mail spam
  - **X.1242** Short message service (SMS) spam filtering system based on user-specified rules
  - **X.1243** Interactive gateway system for countering spam
  - New **X.1244** Overall aspects of countering spam in IP-based multimedia applications
  - New **X.1245** Framework for countering spam in IP-based multimedia applications
  - New **Draft X Suppl. 11 To X.1245** Real time-blocking list (RBL)-based framework for countering VoIP spam

Major accomplishments (4)

Security aspects of ubiquitous telecommunication services

- **Multicast security**
  - X.1101, Security requirements and framework for multicast communication
- **Mobile security**
  - X.1121, Framework of security technologies for mobile end-to-end data communications
  - X.1122, Guideline for implementing secure mobile systems based on PKI
  - X.1123, Differentiated security service for secure mobile end-to-end data communication
  - X.1124, Authentication architecture for mobile end-to-end data communication
  - X.1125, Correlative reacting system in mobile data communication
- **Networked ID security**
  - X.1171, Threats and requirements for protection of personally identifiable information in applications using tag-based identification
- **IPTV security**

New
- X.1191, Functional requirements and architecture for IPTV security aspects

Consent
- X.1192, Functional requirements and mechanisms for secure transcodable scheme of IPTV

New
- X.1193, Key management framework for secure IPTV services
- X.1195, Service and content protection (SCP) interoperability scheme

- **Ubiquitous sensor network security**

New
- X.1311, Information technology – Security framework for ubiquitous sensor network
- X.1312, Ubiquitous sensor network (USN) middleware security guidelines

Major accomplishments (5)

Secure application services

- **Web security**
  - **X.1141**, Security Assertion Markup Language (SAML 2.0)
  - **X.1142**, eXtensible Access Control Markup Language (XACML 2.0)
  - **X.1143**, Security architecture for message security in mobile web services
- **Security protocols**
  - **X.1151**, Guideline on secure password-based authentication protocol with key exchange
  - **X.1152**, Secure end-to-end data communication techniques using trusted third party services
  - New **X.1153,** A management framework of an one time password-based authentication service
- **Peer-to-peer security**
  - **X.1161**, Framework for secure peer-to-peer communications
  - **X.1162**, Security architecture and operations for peer-to-peer networks

Major accomplishments (6)

X.1250 – X.1279 allocated to Identity Management

- **Identity Management**
  - **X.1250** Baseline capabilities for enhanced global identity management and interoperability
  - **X Suppl. 7** to ITU-T X.1250 series – Supplement on overview of identity management in the context of cybersecurity
  - **X.1251** A framework for user control of digital identity
  - New **X.1252** Baseline identity management terms and definitions
  - **X.1253** Security guidelines for identity management systems
  - **X.1261** Extended validation certificate framework (EVcert)
  - New **X.1275** Guidelines on protection of personally identifiable information in the application of RFID technology
  - Draft **X.1261** Extended validation certificate framework (EVcert)

Misc.:

- New **X.674** Procedures for the registration of arcs under the Alerting object identifier arc
- **X.1303** Common alerting protocol (CAP 1.1)

Coordination and Collaboration on Identity Management

ITU-T Joint coordination activity in IdM JCA-IdM

International Telecommunication Union

Committed to connecting the world

MoU between the ITU and the UNODC

Announced (19 May 2011) MoU between UNODC (United Nations Office on Drugs and Crime) and ITU!

- A fundamental role of ITU is to build confidence and security in the use of information and communication technologies (ICTs).
- The UNODC is a global leader in the fight against illicit drugs and international crime.
- A Memorandum of Understanding signed between ITU and the United Nations Office on Drugs and Crime (UNODC) will allow the two organizations to collaborate in assisting ITU and UN Member States mitigate the risks posed by cybercrime.
- The objective is to establish a general framework for collaboration between the Parties, on a non-exclusive basis, and in accordance with the commonly-agreed goals in the areas of cybersecurity and cybercrime.
- Areas of cooperation
  - Legal measures
  - Capacity building and technical assistance
  - Intergovernmental and expert meetings
  - Comprehensive study on cybercrime
  - Organizational Structures, etc

International Telecommunication Union

Committed to connecting the world

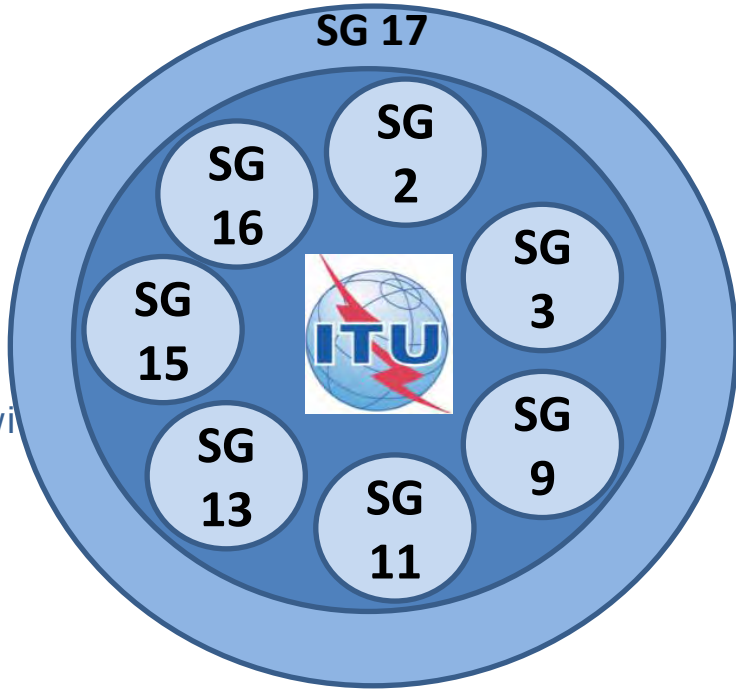
Child Online Protection (COP) New study topic within SG 17

- TSAG has acknowledged (Feb 2011) that SG 17 can study and coordinate Child Online Protection.
- SG 17's foreseen activities on COP are a logical next step in continuing the ITU COP initiative in the area of technical measures.
- SG 17 could be active on technical and procedural security measures concerning COP, where SG 17 members and Member States are expected to develop technical procedural criteria for telecom operators and/or service providers and related technical measures to combat new and emerging threats to children.
  - The objectives would be to identify best practices on technical measures for child online protection and to develop interoperable standards and related Recommendations (i.e., identity management, authentication) to protect children online.
- A Correspondence Group identifies the role of SG 17 on COP
  - To identify technical issues (e.g., identity management and authentication)

International Telecommunication Union
Committed to connecting the world

Security activities in other ITU-T Study Groups

- ITU-T SG 2 Operation aspects & TMN
  - Q3 International Emergency Preference Scheme , ETS/TDR
  - Q5 Network and service operations and maintenance procedures , E.408
  - Q11 TMN security, TMN PKI
- ITU-T SG 9 Integrated broadband cable and TV
  - Q3 Conditional access, copy protection, HDLC privacy,
  - Q7, Q8 DOCSIS privacy/security
  - Q9 IPCablecom 2 (IMS w. security), MediaHomeNet security gateway, DRM
- ITU-T SG 11 Signaling Protocols
  - Q7 EAP-AKA for NGN
- ITU-T SG 13 Future network
  - Q16 Security and identity management for NGN
  - Q17 Deep Packet Inspection
- ITU-T SG 15 Optical Transport & Access
  - Reliability, availability, Ethernet/MPLS protection swi
- ITU-T SG 16 Multimedia
  - Secure VoIP and Multimedia security (H.233, H.234, H.235, H.323, secure JPEG2000)



International Telecommunication Union
Committed to connecting the world

THANK YOU

For further information

www.itu.int/cybersecurity

cybersecurity@itu.int

http://www.itu.int/ITU-T/studygroups/com17/index.asp

International Telecommunication Union

Committed to connecting the world