ICT Security – Cybersecurity – CYBEX
Overview of activities in ITU-T with focus on Study Group 17

TSB Briefing to the Regional Offices, 28 Feb 2011

Martin Euchner

Advisor of ITU-T Study Group 17

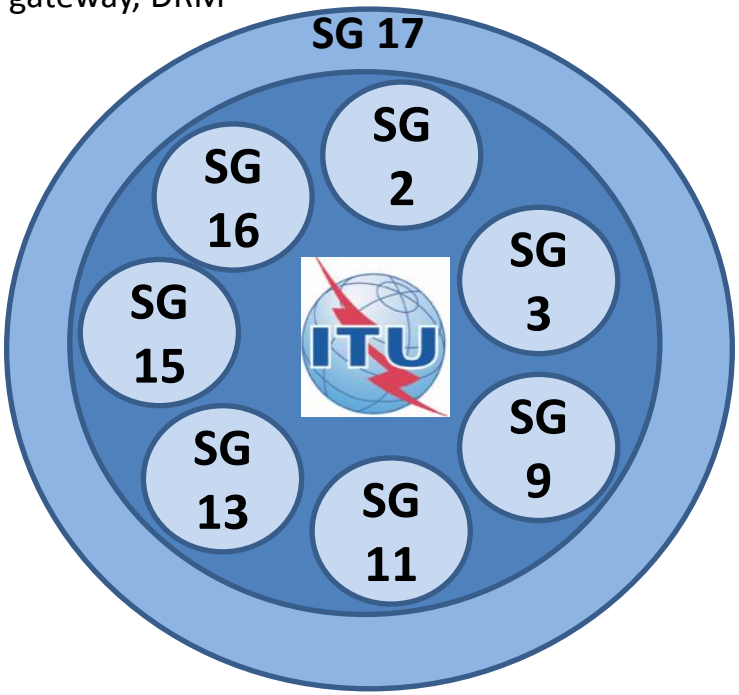
Martin.Euchner@itu.int

International Telecommunication Union

Committed to connecting the world

Security activities in other ITU-T Study Groups

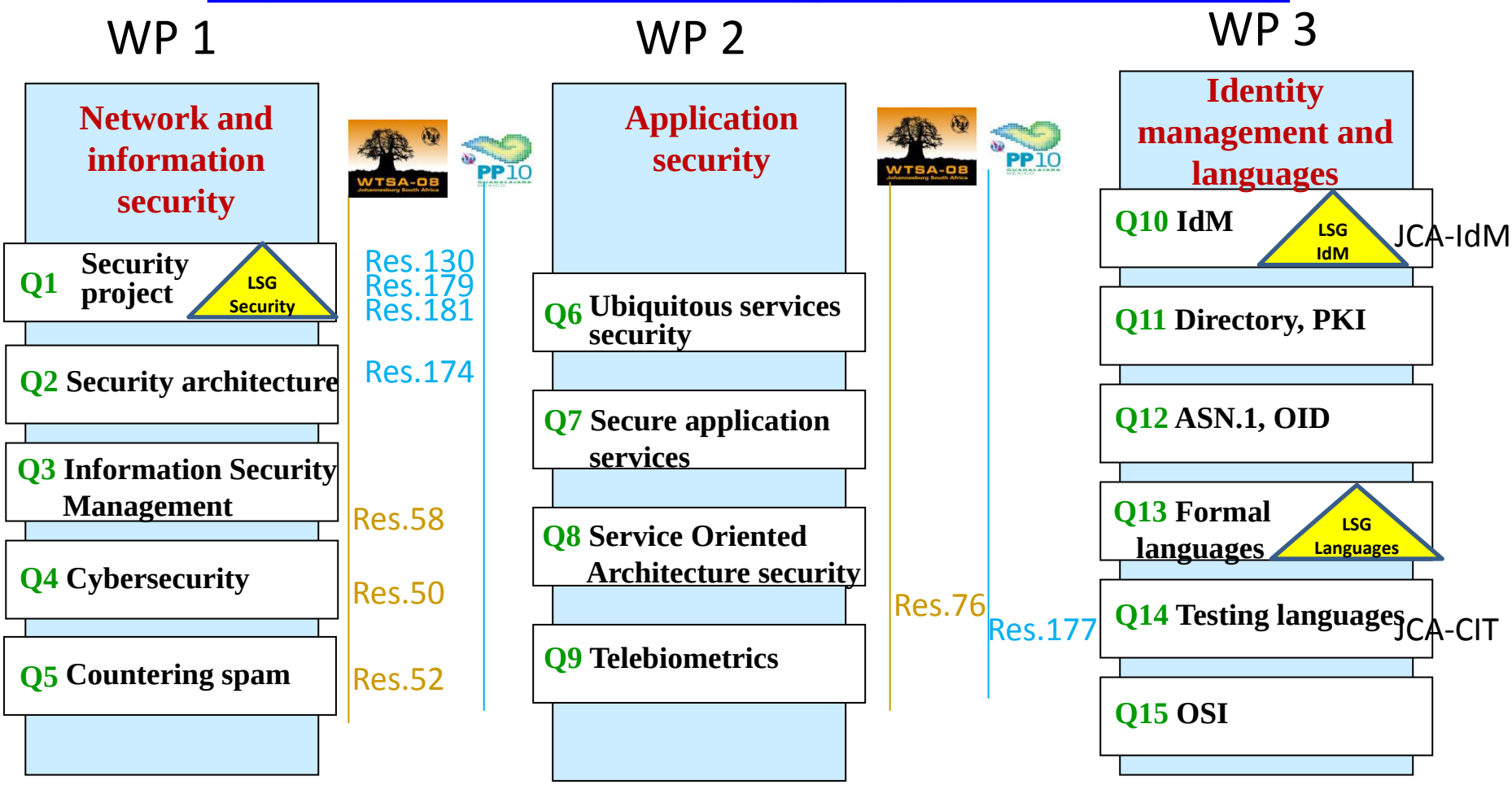
- **ITU-T SG 2 Operation aspects & TMN**
  - **Q3** International Emergency Preference Scheme , ETS/TDR
  - **Q5** Network and service operations and maintenance procedures , E.408
  - **Q11** TMN security, TMN PKI
- **ITU-T SG 9 Integrated broadband cable and TV**
  - **Q3** Conditional access, copy 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 switching
- **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

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

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-series Recommendations allocated to Cyberspace security

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
  - **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
  - New – **X.1209** Capabilities and their context scenarios for cybersecurity information sharing and exchange.

Major accomplishments (2)

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
  - New – **X.1243** Interactive gateway system for countering spam
  - **X.1244** Overall aspects of countering spam in IP-based multimedia applications
  - New – **X.1245** Framework for countering spam in IP-based multimedia applications

Major accomplishments (3)

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
  - **X.1252** Baseline identity management terms and definitions
  - New – **X.1261** Extended validation certificate framework (EVcert)
  - New – **X.1275** Guidelines on protection of personally identifiable information in the application of RFID technology

Misc.:

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

Question 4/17 “Cybersecurity”
Some activities

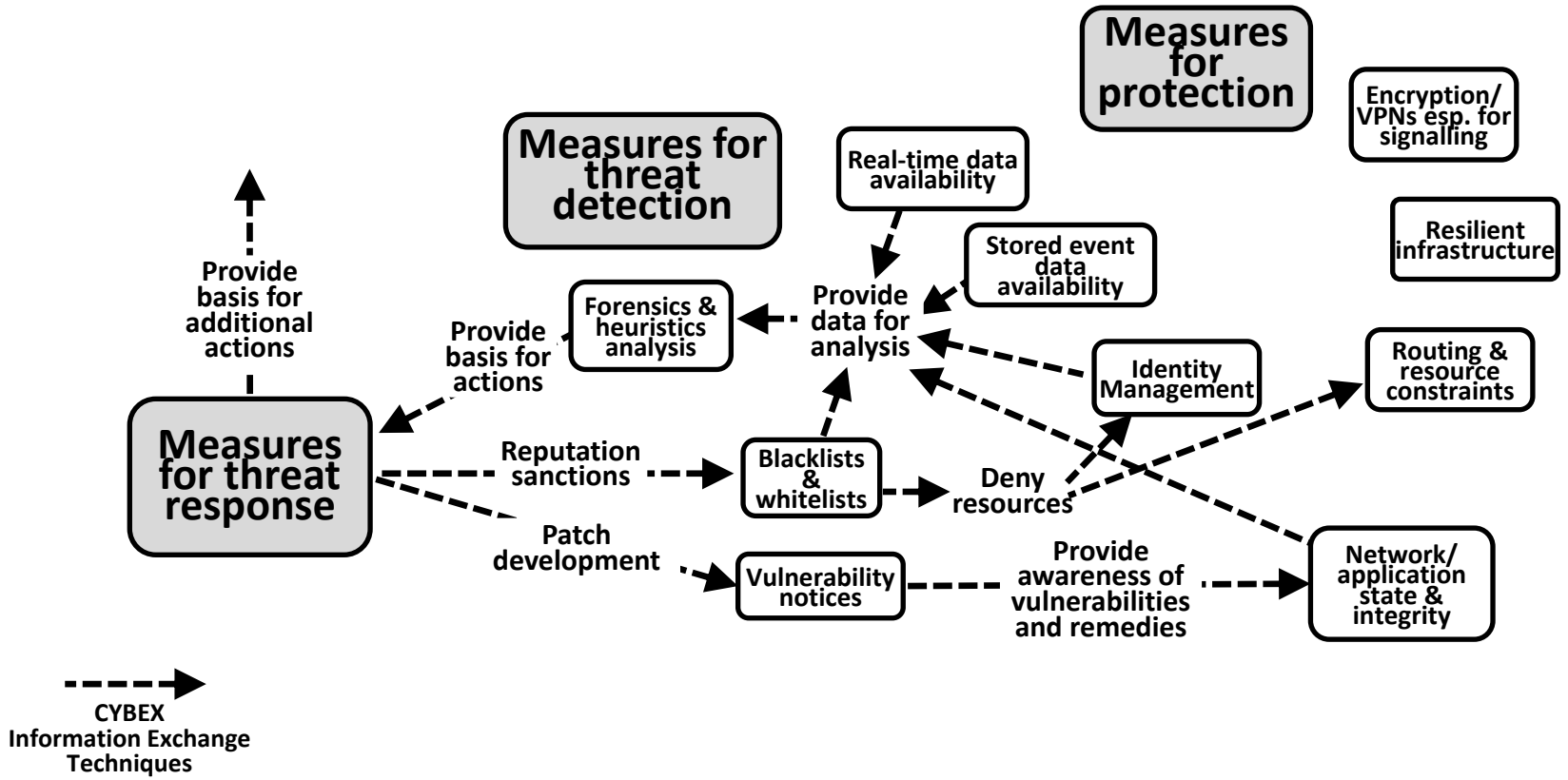
- Security assurance mechanisms in telecommunication networks for service providers
- Development and sharing of best practices in the cyber environment
- Sharing of vulnerabilities information
- Framework for security information sharing; enhancements and refinements of cybersecurity information exchange 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 on preventing malicious code spreading in ICT networks
- 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)

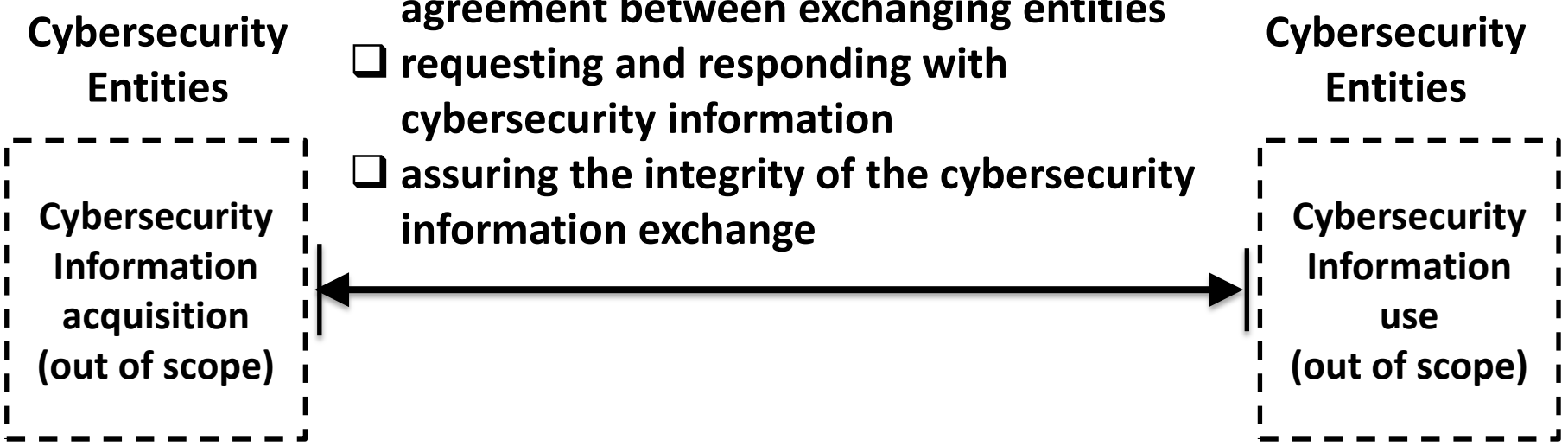
- The new cybersecurity paradigm
  - know your weaknesses
    - minimize the vulnerabilities
  - know your attacks
    - share the heuristics within trust communities
- CYBEX – techniques for the new paradigm
  - Weakness, vulnerability and state
  - Event, incident, and heuristics
  - Information exchange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

CYBEX Facilitates a Global Cybersecurity Model

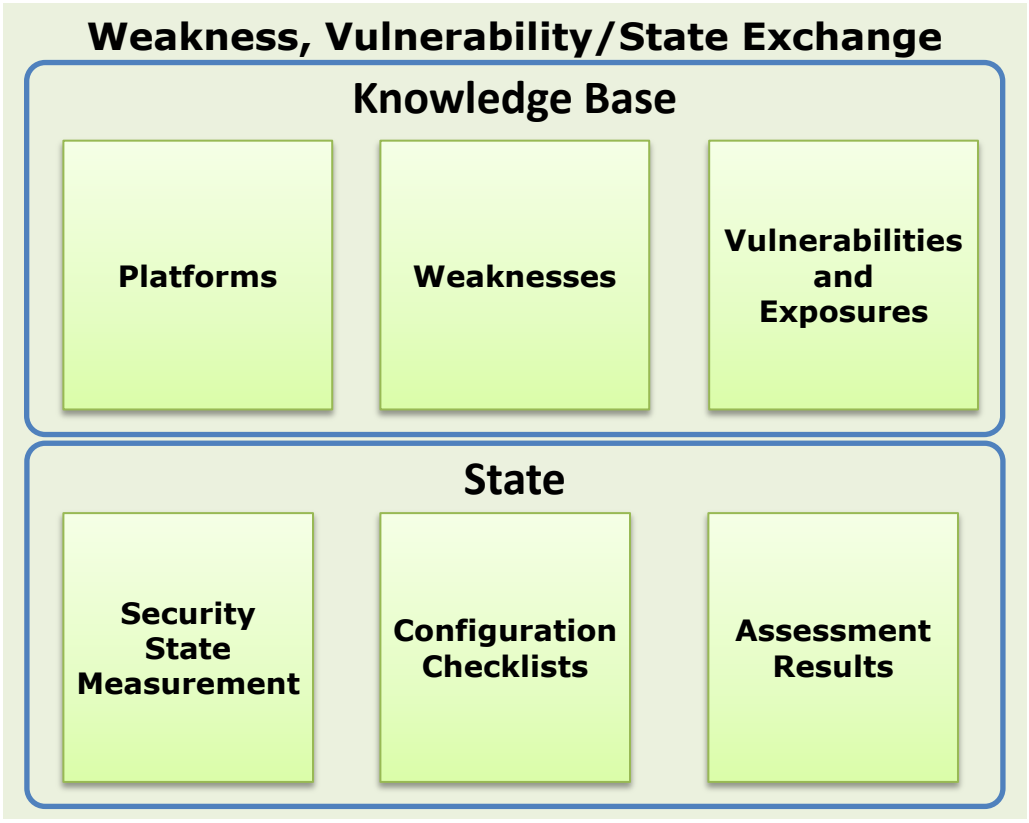


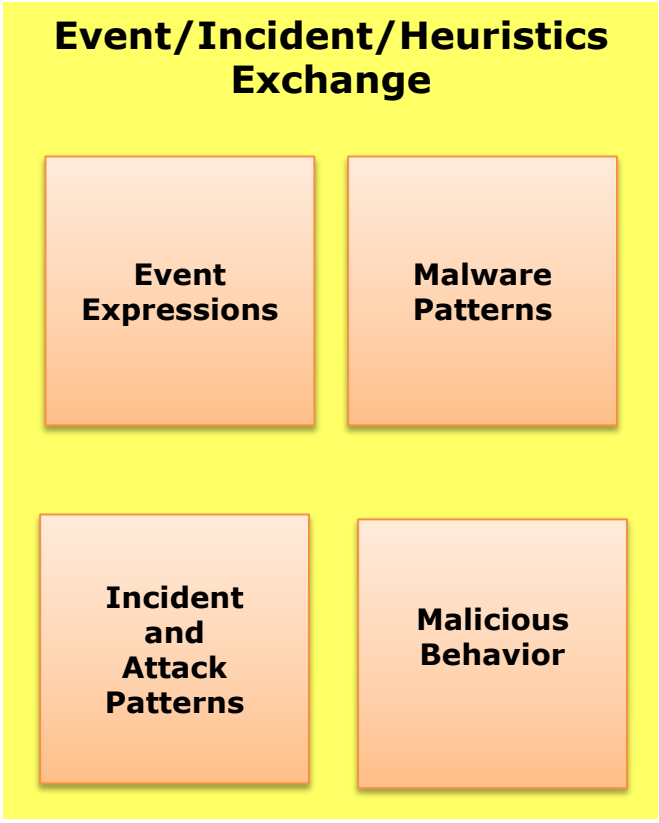
The CYBEX Model

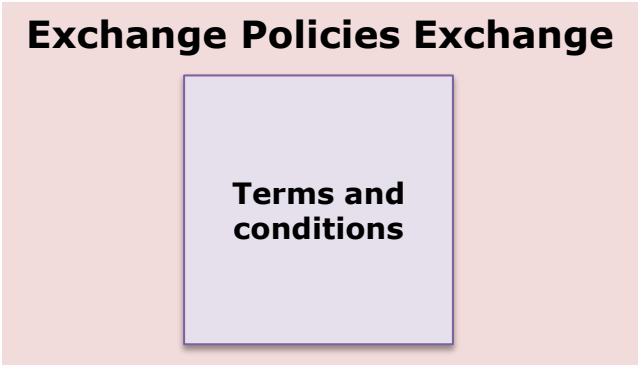
- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- establishment of trust and policy agreement between exchanging entities
- requesting and responding with cybersecurity information
- assuring the integrity of the cybersecurity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



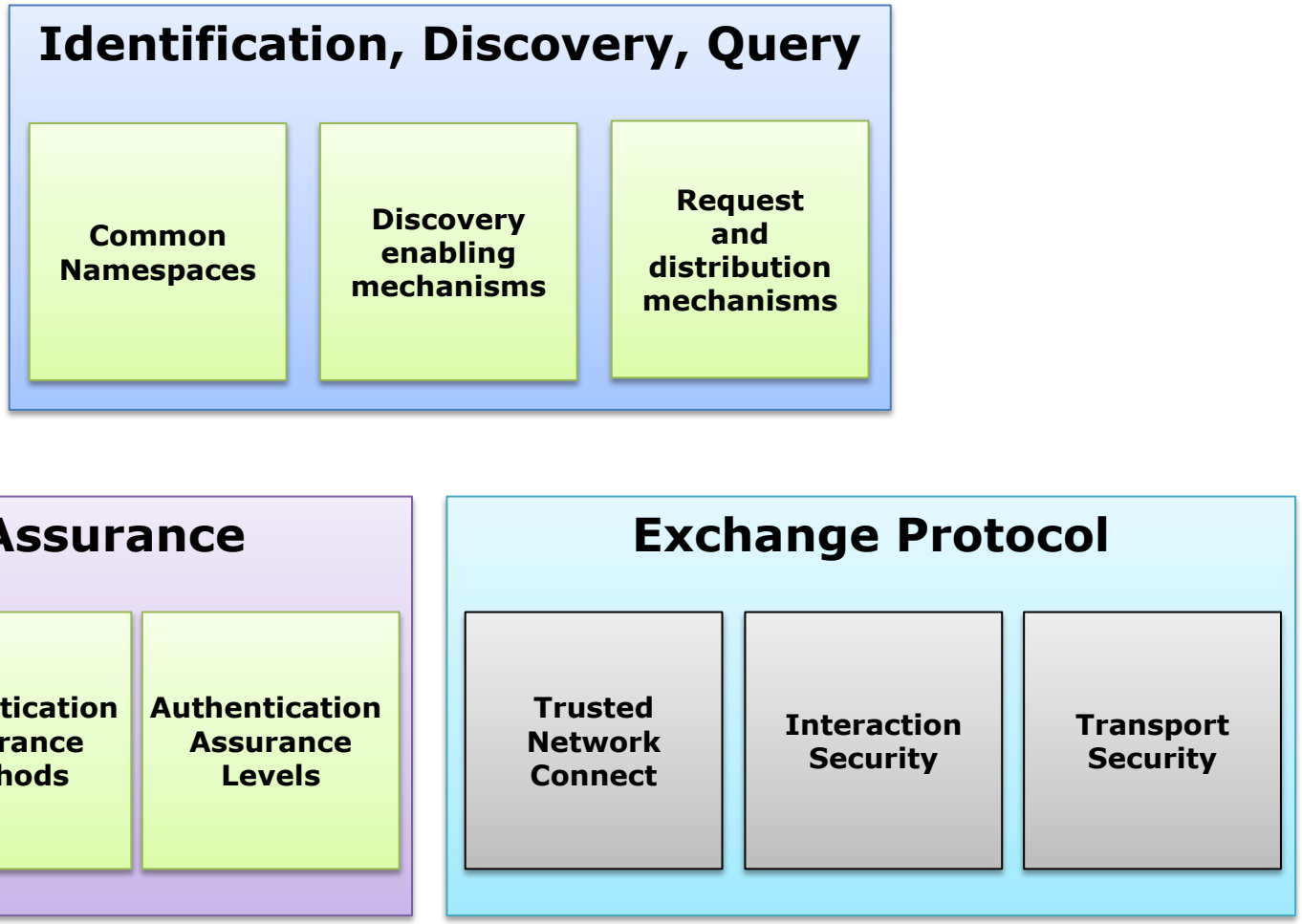
CYBEX Technique Clusters: Structured Information







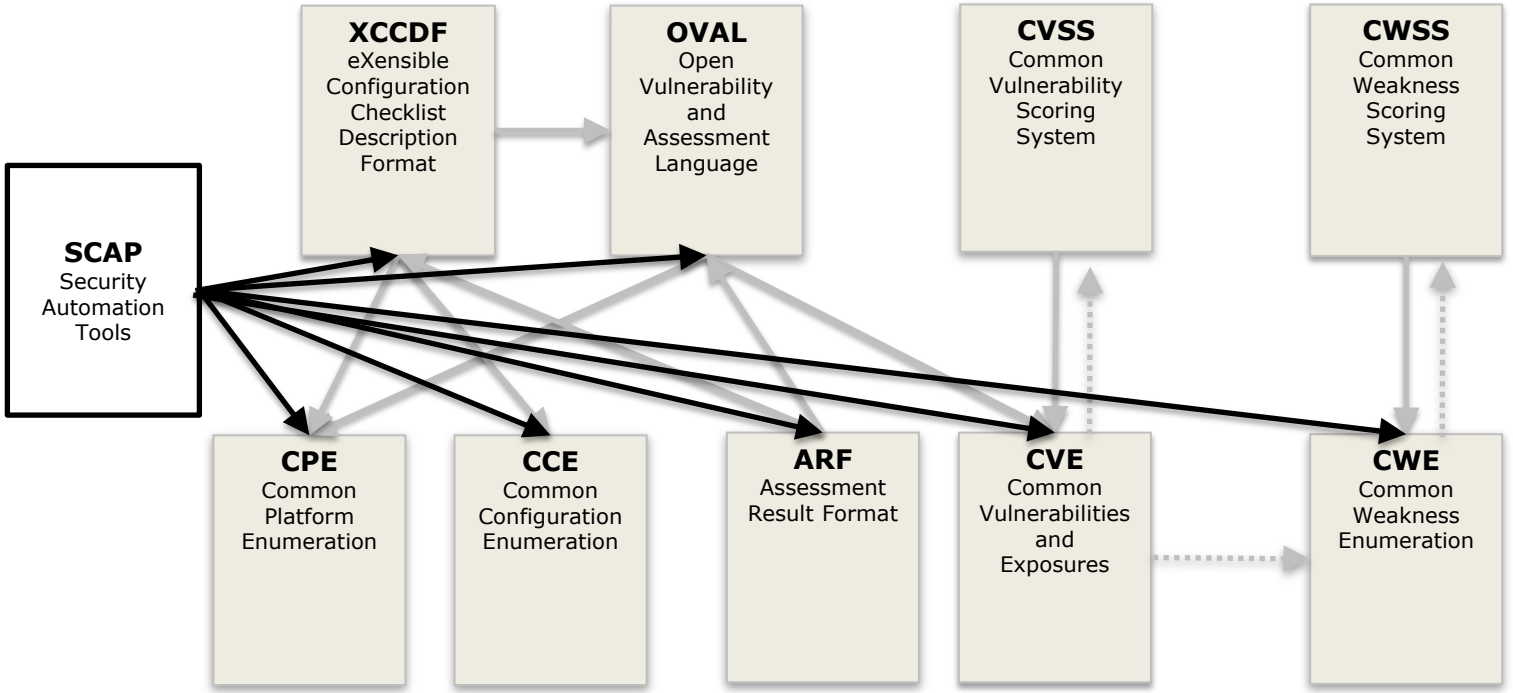
CYBEX Technique Clusters: Utilities



International Telecommunication Union

Committed to connecting the world

Toward Network Security Planes: Security Automation Schemas Everywhere

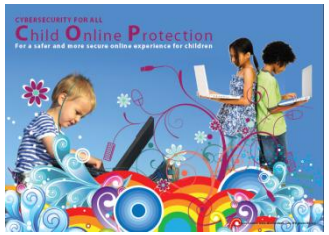


Future direction
Cybersecurity

- **X.1500-series Recommendations allocated to Cybersecurity information exchange**
- **Cybersecurity Information Exchange (CYBEX)**
  - Facilitate standardized global exchange of vulnerability and incident information
  - making security measurable
  - http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx

Draft X.1500	**Cybersecurity information exchange framework**
Draft X.1520	**Common vulnerabilities and exposures (CVE)**
Draft X.1521	**Common vulnerability scoring system (CVSS)**
Draft X.gopw	**Guideline on preventing malicious code spreading in a data communication network**

- **Approx. 30 active work items on cybersecurity are in the Q4/17 pipeline and re being progressed towards Recommendations.**



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

- COP aims to tackle cybersecurity holistically, addressing legal, technical, organizational and procedural issues as well as capacity building and international cooperation.
- 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.
  - In the technical domain, the objectives would be to identify best practices on technical measures for child online protection and to develop interoperable standards and related recommendations to protect children online. The aim would be to develop a widely shared approach which could be promoted across the whole telecommunication industry.
  - Several SG 17 Questions might study technical aspects on COP.

- SG 17 might also want to study a Code of Conduct on COP (e.g. for service providers).