V1.0

World Class Standards

ETSI Workshop
19-20 January 2011
Sophia Antipolis, France

Enhancing Security for Next Generation Networks and Cloud Computing

Tony Rutkowski
Yaana Technologies
Georgia Tech
ITU-T Q.4/17 Rapporteur

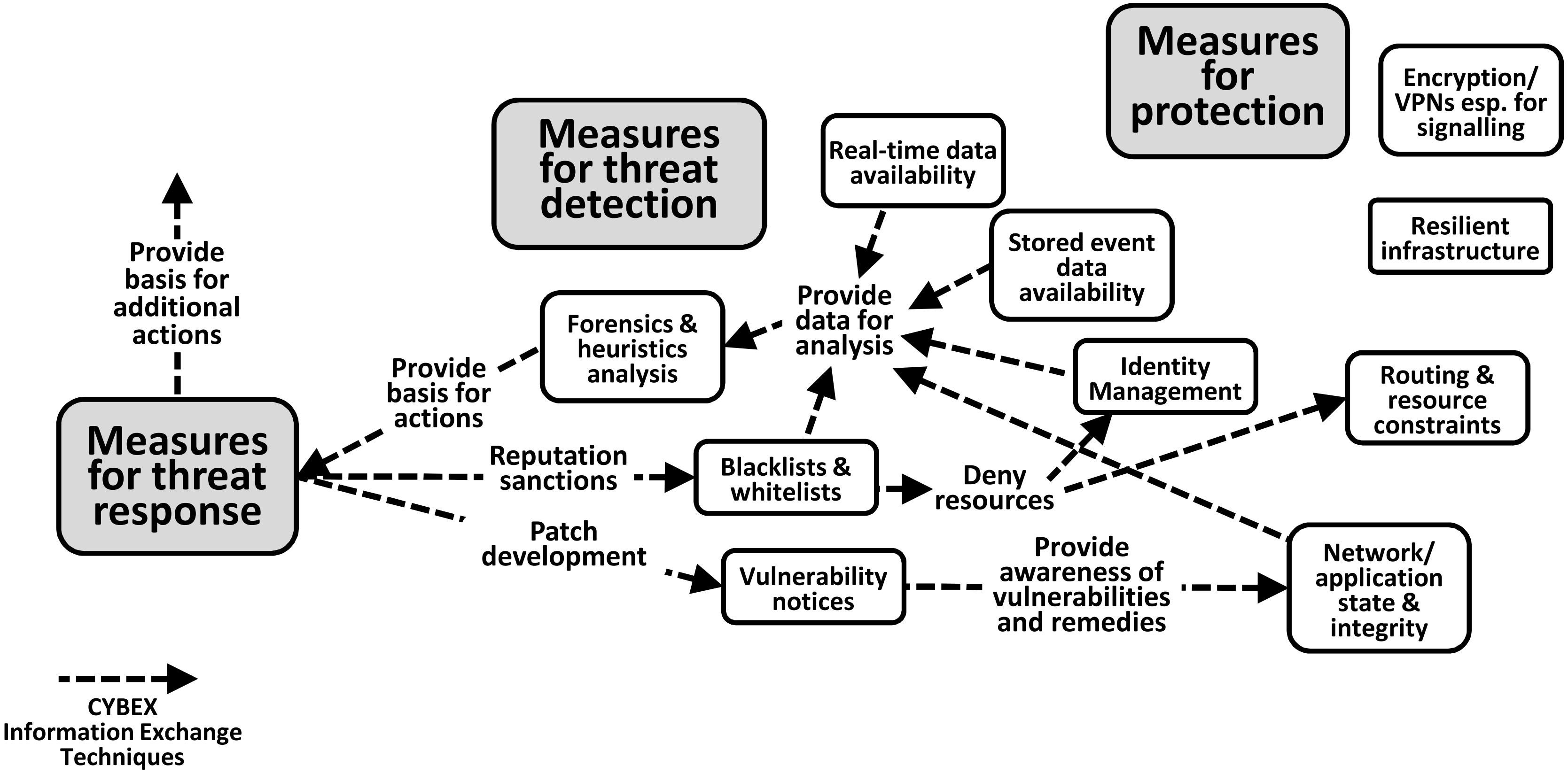
CYBEX Basics

- 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
- Rec. ITU-T 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

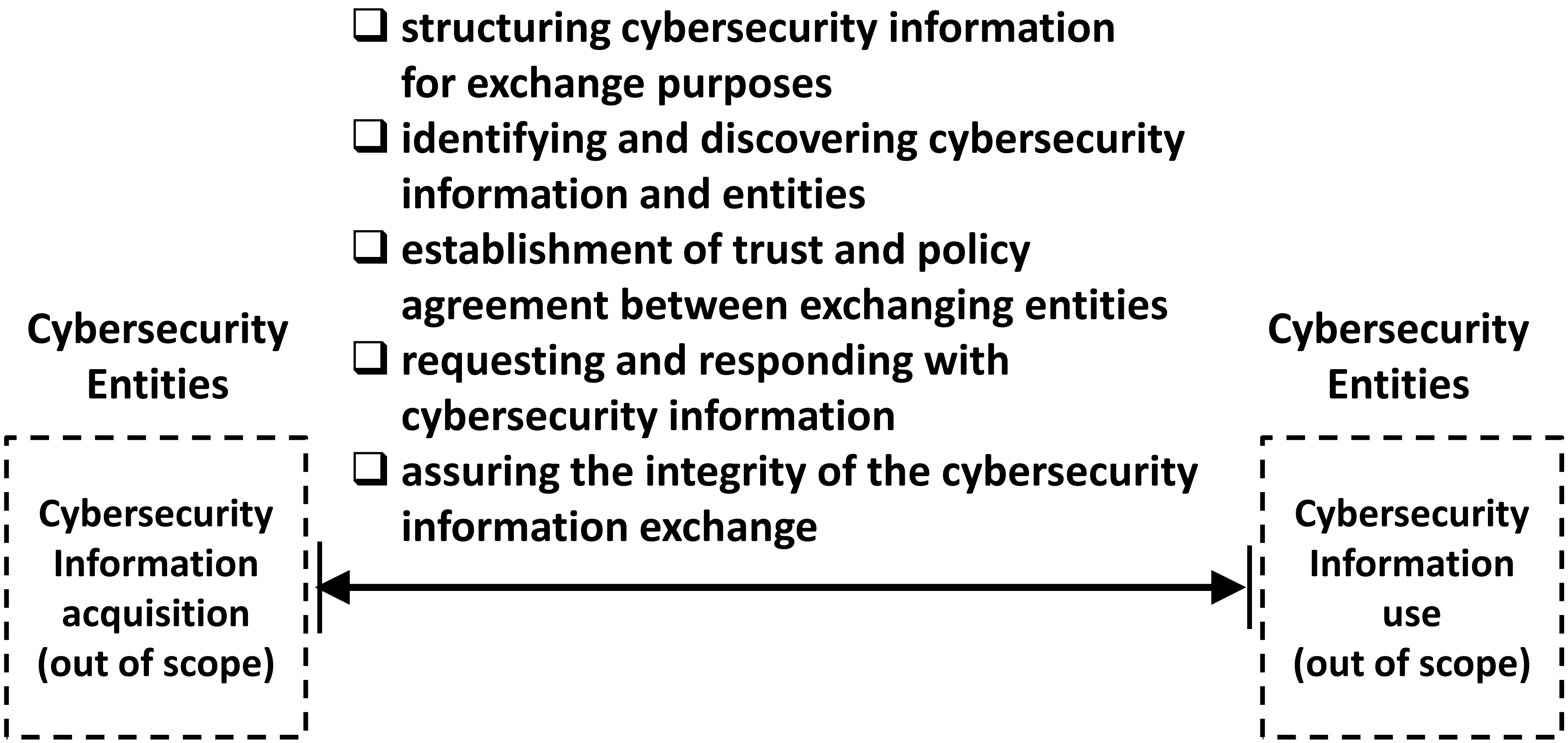
Today’s Reality

- “Security by design” is not a reasonable objective today
  - The code/systems are too complex, distributed, autonomous, dynamic, and threatened
  - Security today requires continuously knowing weaknesses, attacks, and responsive actions
- Common global protocol platforms for the trusted exchange of this knowledge are essential
- A distributed, “security management” network plane that supports autonomy is emerging
  - Single “national centres” for this purpose are not feasible and would represent a massive vulnerability
- Cloud Computing is especially challenging

CYBEX Facilitates a Global Cybersecurity Model


Measures for protection
Encryption/ VPNs esp. for signalling
Measures for threat detection
Real-time data availability
Resilient infrastructure
Stored event data availability
Provide basis for additional actions
Provide data for analysis
Forensics & heuristics analysis
Identity Management
Provide basis for actions
Routing & resource constraints
Measures for threat response
Reputation sanctions
Blacklists & whitelists
Deny resources
Patch development
Network/ application state & integrity
Vulnerability notices
Provide awareness of vulnerabilities and remedies
CYBEX Information Exchange Techniques

The CYBEX Model



Cybersecurity Entities

Cybersecurity Information acquisition (out of scope)

□ structuring cybersecurity information for exchange purposes

□ identifying and discovering cybersecurity information and entities

□ establishment of trust and policy agreement between exchanging entities

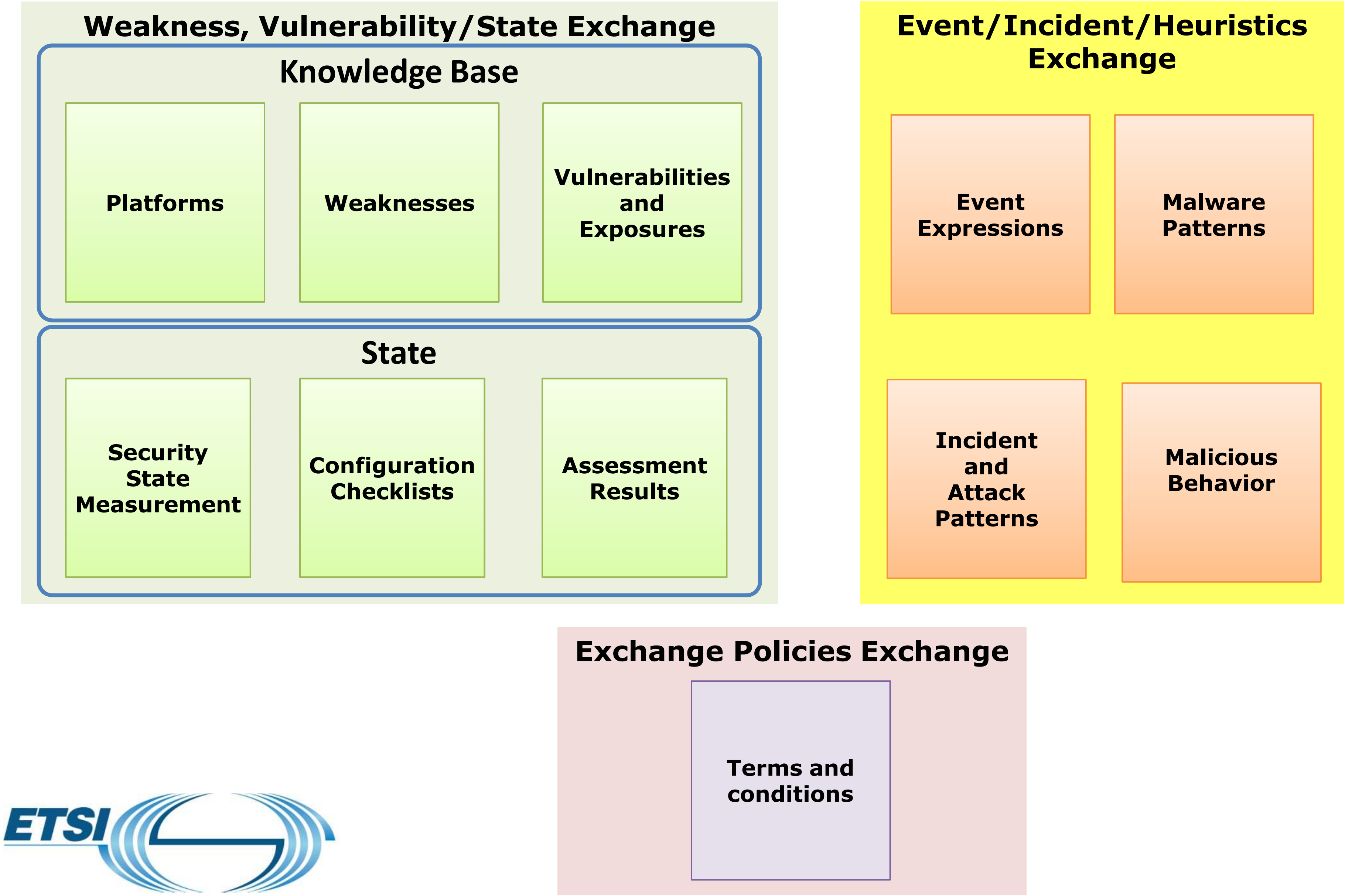
□ requesting and responding with cybersecurity information

□ assuring the integrity of the cybersecurity information exchange

Cybersecurity Entities

Cybersecurity Information use (out of scope)

CYBEX Technique Clusters: Structured Information



Weakness, Vulnerability/State Exchange

Knowledge Base

Platforms

Weaknesses

Vulnerabilities and Exposures

State

Security State Measurement

Configuration Checklists

Assessment Results

Event/Incident/Heuristics Exchange

Event Expressions

Malware Patterns

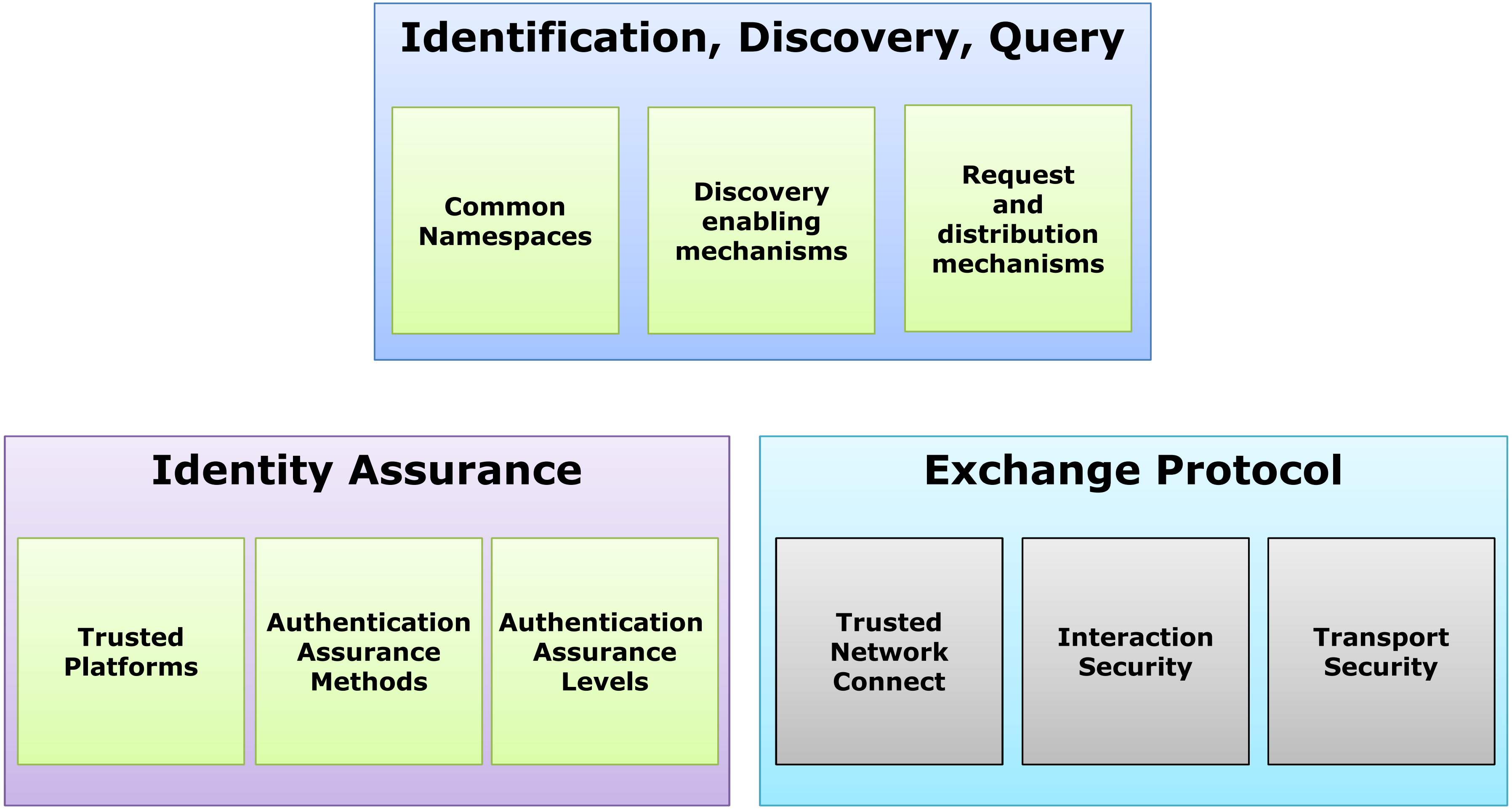
Incident and Attack Patterns

Malicious Behavior

Exchange Policies Exchange

Terms and conditions

CYBEX Technique Clusters: Utilities



Identification, Discovery, Query

Common Namespaces

Discovery enabling mechanisms

Request and distribution mechanisms

Identity Assurance

Trusted Platforms

Authentication Assurance Methods

Authentication Assurance Levels

Exchange Protocol

Trusted Network Connect

Interaction Security

Transport Security

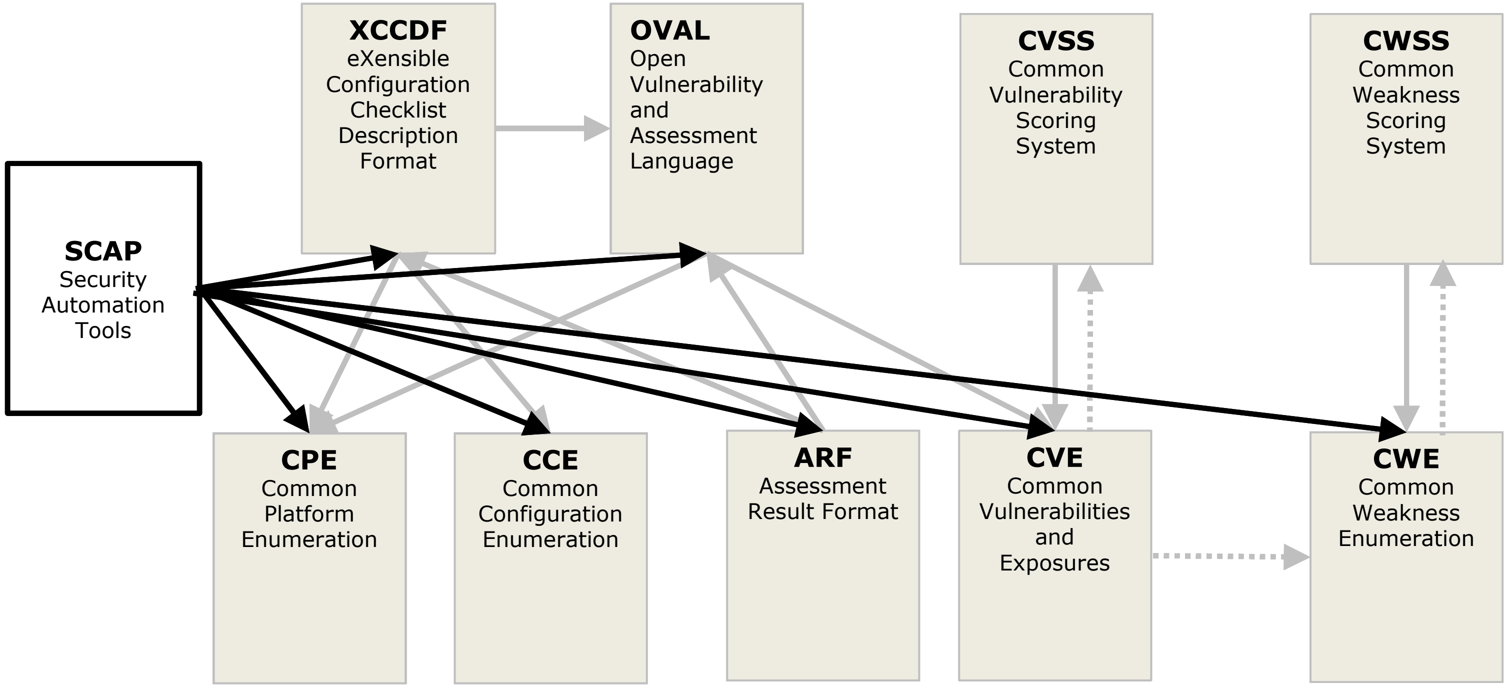
Today’s Use Cases

- Your computer
  - Patch Tuesday
  - Open “Windows Update”
- X.1500 Appendices
  - NICT CYBEX Ontology
  - Japan Vulnerability Notes (JVN) portal
  - USA Federal Desktop Core Configuration/ US Government Configuration Baseline

Significant adoption rate

- SG17 Dec 2010 Geneva Cybersecurity Workshop CYBEX session
  - Robert A. Martin of MITRE described the essentials for Vendor Neutral Security Measurement & Management with Standards
  - Ian Bryant of the EU NEISAS Project described the challenges in sharing security information for infrastructure protection
  - Takeshi Takahashi of NICT described an ontological approach for cybersecurity information haring, especially for Cloud Computing
  - Thomas Millar of the US-CERT presented an operational model of CIRT processes for improved collaboration and capability development
  - Luc Dandurand of NATO described his organizations new initiative for cyber defence data exchange and collaboration infrastructure (CDXI)
  - Damir Rajnovic of FIRST described the structure and mechanisms of the principal global organization of cybersecurity incident centers
- 2010 adoption by Common Criteria Control Board
- IETF October 2010 Beijing Meeting
  - CYBEX conceptualized as a security management layer

Knowing your weaknesses: Security Automation Schemas Everywhere



SCAP Security Automation Tools

XCCDF eXensible Configuration Checklist Description Format

OVAL Open Vulnerability and Assessment Language

CVSS Common Vulnerability Scoring System

CWSS Common Weakness Scoring System

CPE Common Platform Enumeration

CCE Common Configuration Enumeration

ARF Assessment Result Format

CVE Common Vulnerabilities and Exposures

CWE Common Weakness Enumeration

A CYBEX security plane for NGNs

- A CYBEX reference model for NGNs can be created
  - SCAP should be ubiquitous in the models
  - Requires a “CYBEX” plane
  - Approach is adapted from NGN Identity Management plane
  - NGN providers would play a substantial CYBEX framework-support function
    - with understood assurance levels among themselves and all network devices and capabilities within their domain
    - with services offered to customers
  - CYBEX techniques would be adapted as necessary
    - through the use of extensions
    - reflected in a new extensible Y-series Recommendation
- ETSI TISPAN is already working on a related model

CYBEX applied to Future Network Strata and Functions

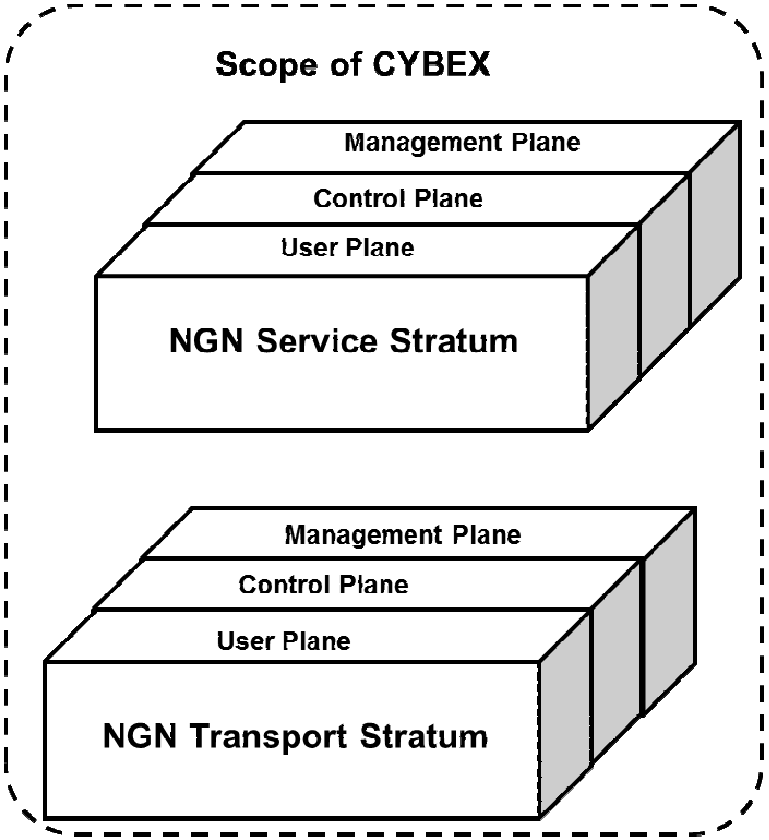


Figure 2/Y.2011

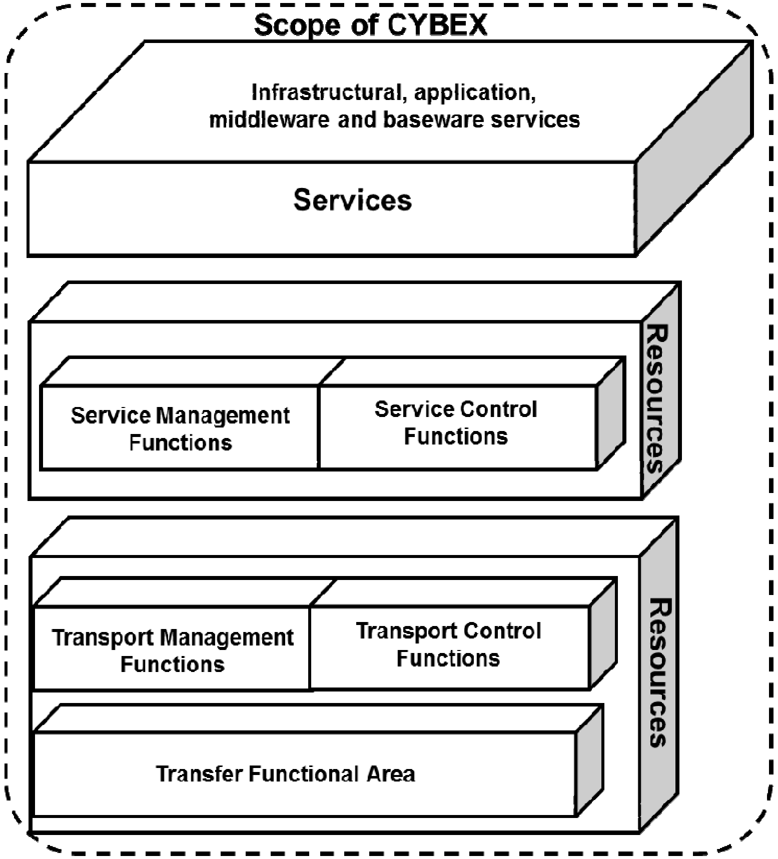
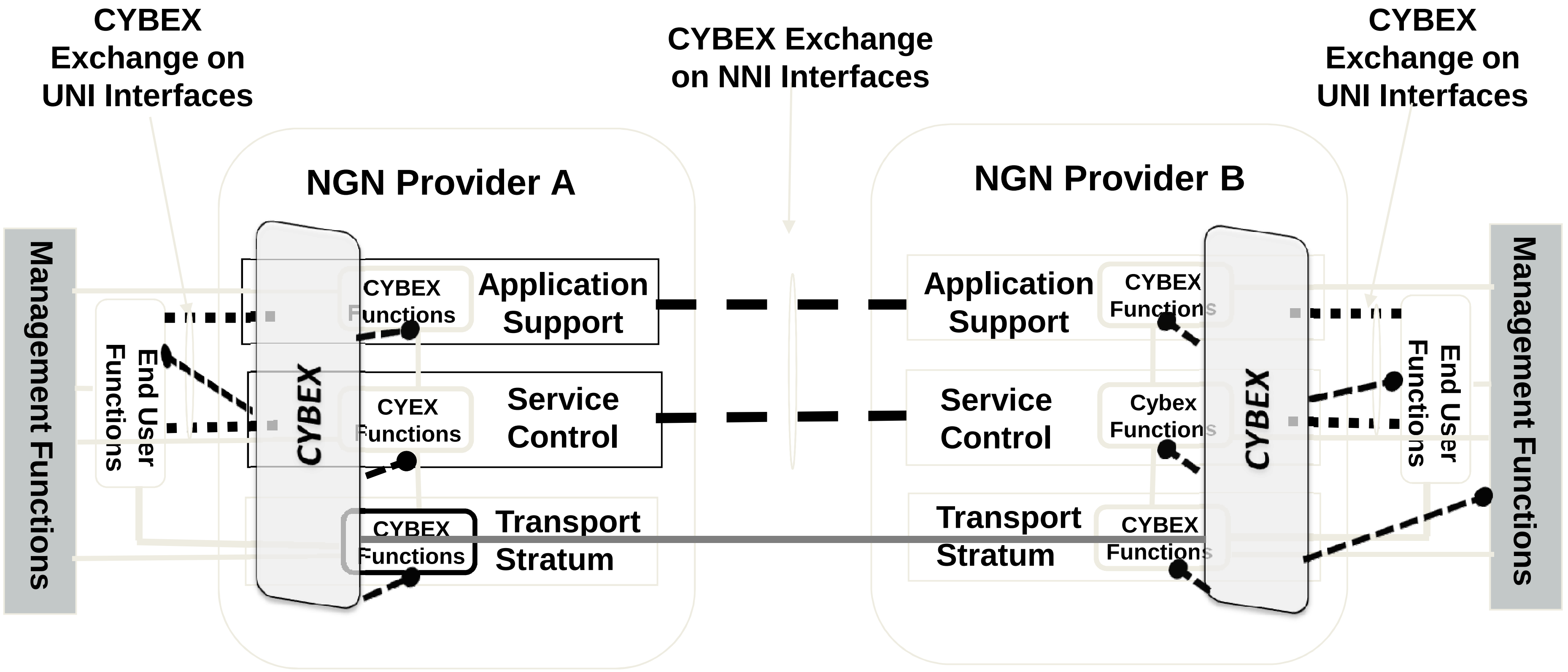

Scope of CYBEX
Infrastructural, application, middleware and baseware services
Services
Service Management Functions
Service Control Functions
Resources
Transport Management Functions
Transport Control Functions
Transfer Functional Area
Resources

Figure 3/Y.2011

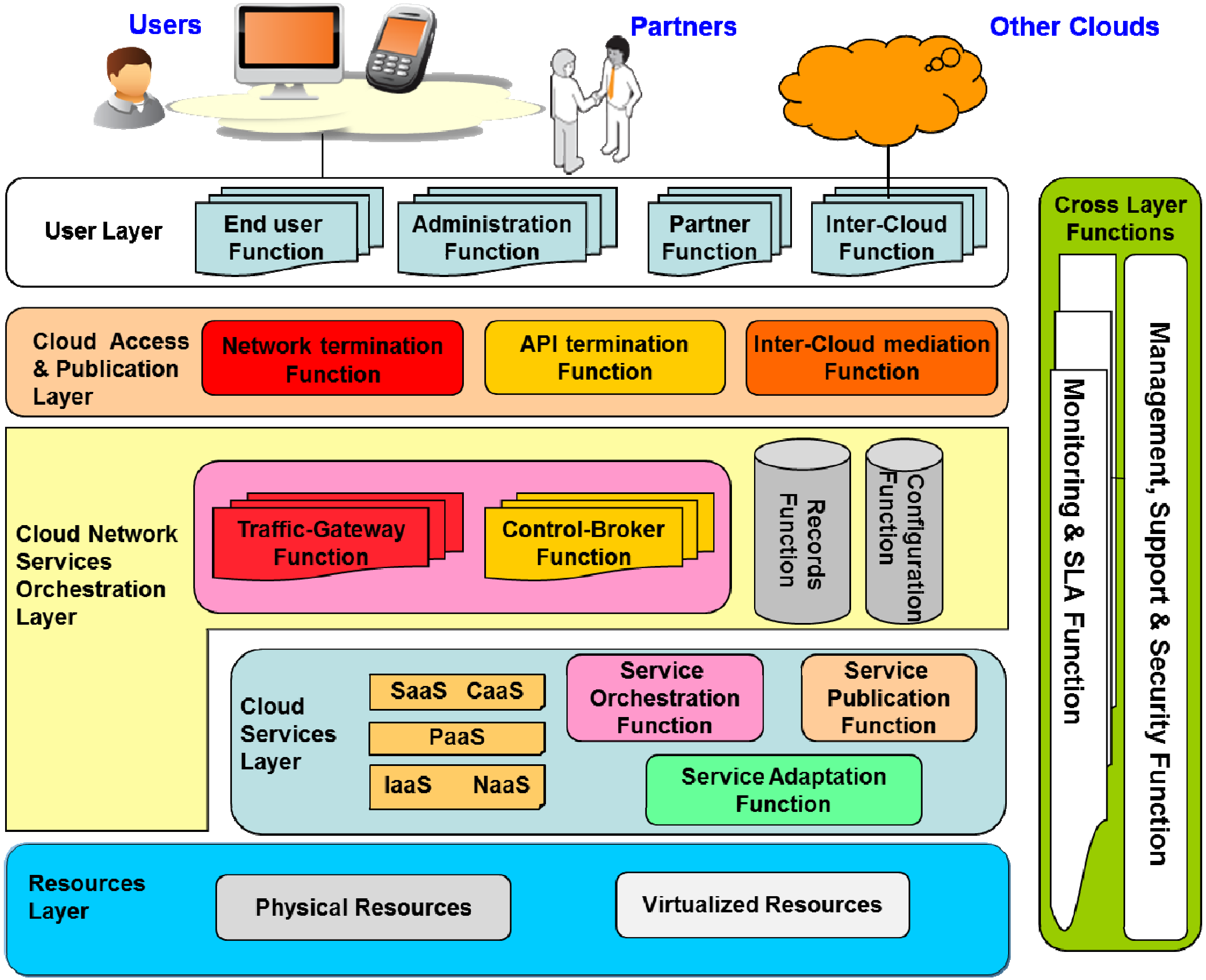
CYBEX applied to Future Network Models toward a NGN/FN security plane



Cloud Computing Ecosystem Taxonomies

- NIST taxonomy
  - Cloud Software as a Service (SaaS)
  - Cloud Platform as a Service (PaaS)
  - Cloud Infrastructure as a Service (IaaS)
- FG-CLOUD taxonomy
  - Application services (SaaS)
  - Resource services (IaaS)
  - Platform services (PaaS)
  - Network services (NaaS)
  - Communication services (CaaS)
- Emerging market
  - Personal clouds

Cloud Reference Architecture



See *Draft deliverable on Functional Requirements and Reference Architecture*, Nanjing, 10–13 January 2011

Cloud Computing security standards embrace new paradigm and CYBEX

- Cloud security conceptualized as mitigating threats
  - Threats to cloud users
  - Threats to cloud service providers
- Transformed into requirements for Cloud Computing security
  - Cloud user requirements
  - Cloud service provider requirements
- Includes new ENISA Common assurance maturity model
- Requirements met using CYBEX techniques

See *Draft deliverable on Cloud Computing Security – Output of the FG Cloud #4 meeting*, Nanjing, 10–13 January 2011