ISOG-J Seminar
Tokyo
13 Oct 2010
V1.1

Cybersecurity information security exchange framework (CYBEX): importance and current developments

Tony Rutkowski, tony@yaanatech.com

Rapporteur for Cybersecurity Group, ITU-T Q4/17

Additional roles include: global eWarrant Rapporteur, ETSI TCLI; U.S. NSTAC Cybersecurity Expert; Distinguished Senior Research Fellow, Georgia Institute of Technology

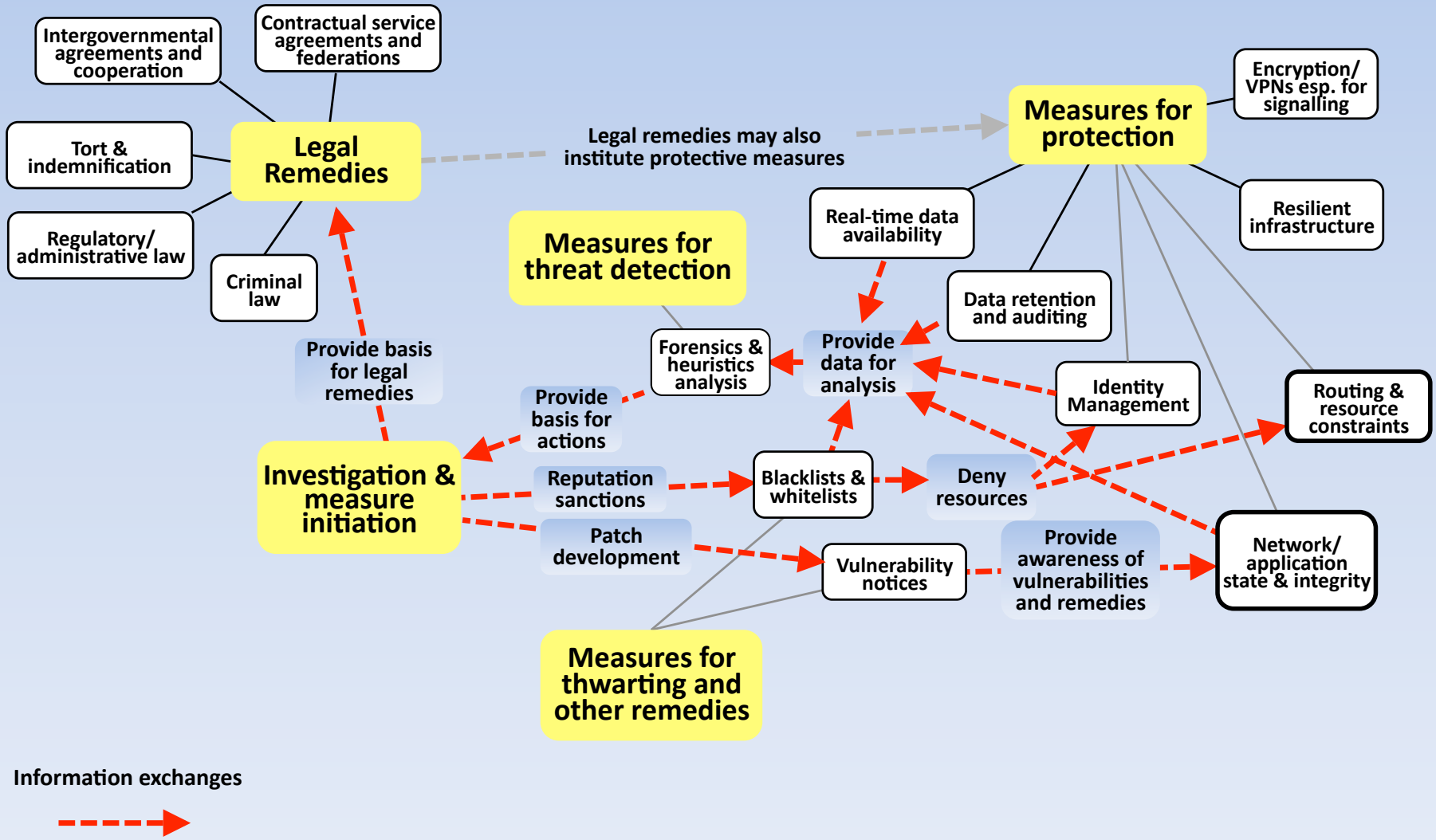
Outline

- Why the CYBEX initiative is important
- Major developments shaping the work
- Specific capabilities
  - Systems Assurance and Incident Response
  - Cybersecurity Information Exchange Framework
  - Identity Management
- Major implementation challenges
  - Extent and evolution of the standards
  - Discovery and trust capabilities
  - Achieving implementations and widespread use

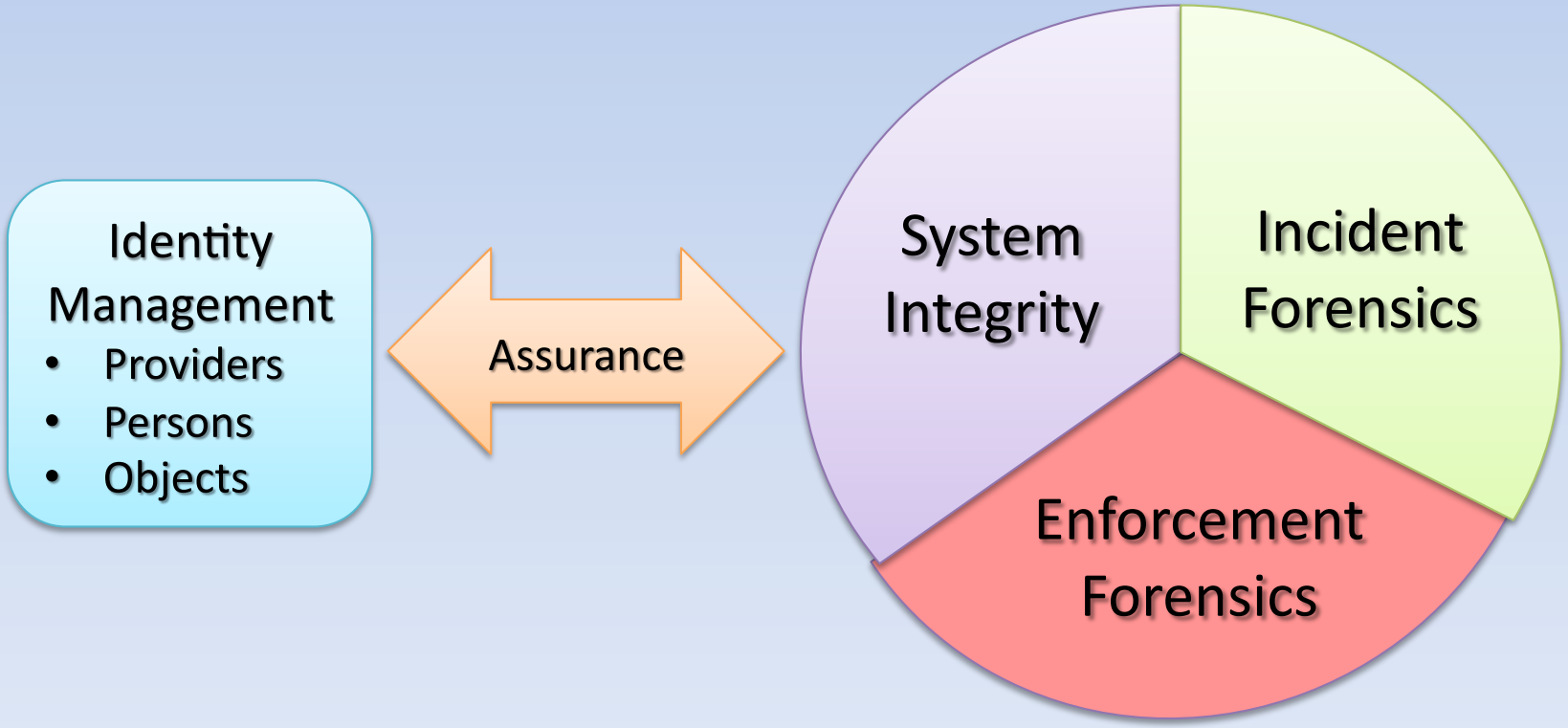
CYBEX: origins

- A common realization that
  - Talking about cybersecurity accomplished nothing
  - The incidents were scaling exponentially
  - Trusted exchange of cybersecurity information was essential to any/all capabilities
  - Many different communities were developing cybersecurity information exchange schema
  - No global framework and consensus existed to bring together communities and schema
- Institutional triggers
  - ITU-T began a new 4 year cycle with a mandate to do something about cybersecurity
  - Participants found there were common global interests in tackling cybersecurity information exchange challenges
    - LAC, NICT, and other Japanese experts and organizations
    - Government and industry entities in APEC region, U.S., and Europe

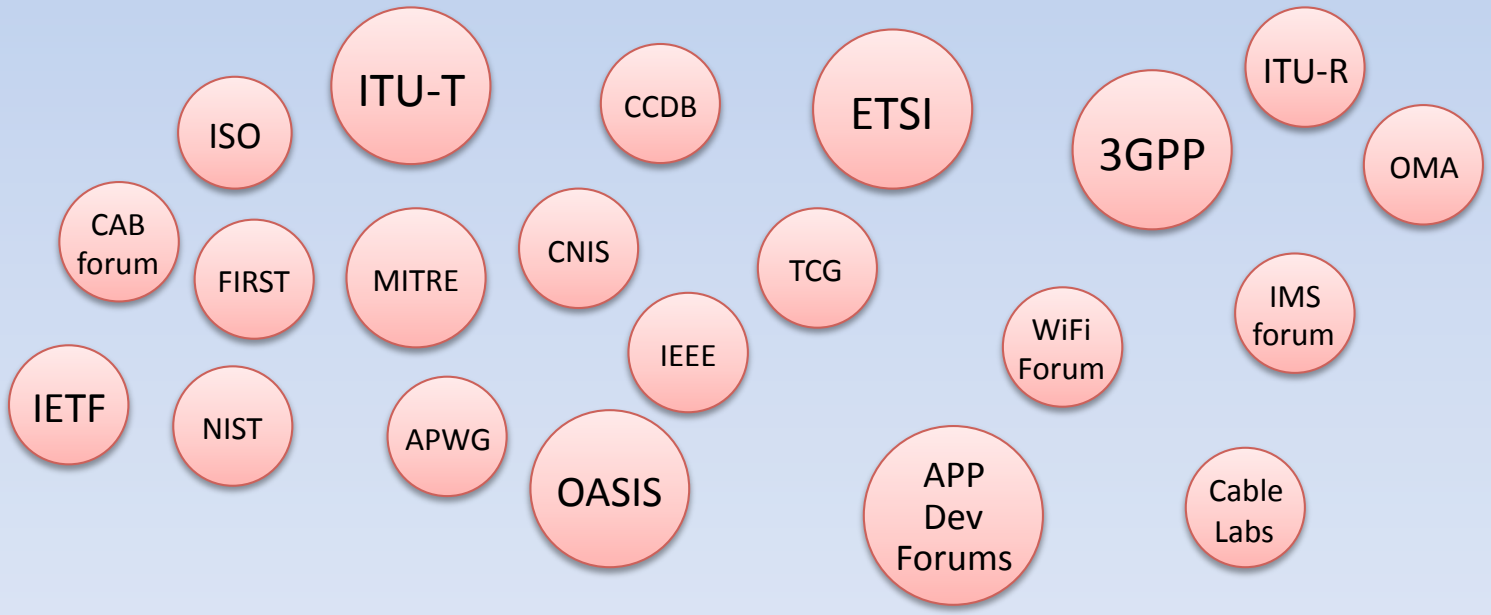
Agreement on a cybersecurity model: information sharing dependencies



Platform coherency appeared possible



Providing outreach among standards bodies seemed possible



Major related institutional developments

- U.N. 15 July document among 15 major powers on reducing "ICT conflict" (a/k/a cyberwar)
- Exercise of cybersecurity authority by regulatory bodies
  - e.g., Korea, FCC in U.S.
- High Level Cybersecurity Strategies (USTIC, Japan, UK, China, Korea)
- Cybersecurity as an issue at ongoing ITU Plenipotentiary Conference
- Enhanced Common Criteria Development Board (CCDB)/NATO activity
- New real-time, data retention, and mobile forensics mandates offshore
- Judicial eDiscovery mandates (e.g., FRCP Rule 26) in US and offshore

Major related infrastructure developments

- Application based infrastructure
  - Mobile platforms driving a world of a million applications
  - Poses major challenges (what is a good application versus malware)
- Locator/ID Separation Protocol (LISP)
  - Re-architects IP based public infrastructures
  - Should solve significant ICT security related challenges, especially attribution
- Asia-Pacific-centricity
  - Region has world's largest and fastest growing infrastructure and strong economies
  - Pursuing technology implementations, network innovations, venue leadership
- Mobile/nomadic-centricity
  - Stressing mobile standards/collaborative forums
  - Include multiple IdM/cyber security challenges

CYBEX is a substantive ongoing global Cyber/ICT security initiative

- Aimed at achieving meaningful security
  - "lock down" the integrity of ICT systems,
  - watch for undesired incidents, and
  - capture, analyze, and process the forensics from those incidents to reduce vulnerabilities, thwart attacks, and institute legal action if appropriate
- The trusted exchange of information is essential to accomplish these three tasks.
- The Cybersecurity Information Exchange Framework (CYBEX) initiative aimed at identifying the emerging set of specifications for the global platforms for achieving these trusted exchanges
- Most of the work has been accomplished within existing systems assurance, incident response, and intelligence/surveillance communities
- Pro-active outreach is part of the initiative
  - Constant attempt to survey what is occurring in all other forums and bringing important capabilities into the framework
  - Constant analysis of what is missing or needed
- Unique – no comparable activity exists

CYBEX Exchange Model

Cybersecurity Entities

Cybersecurity Information acquisition (out of scope*)

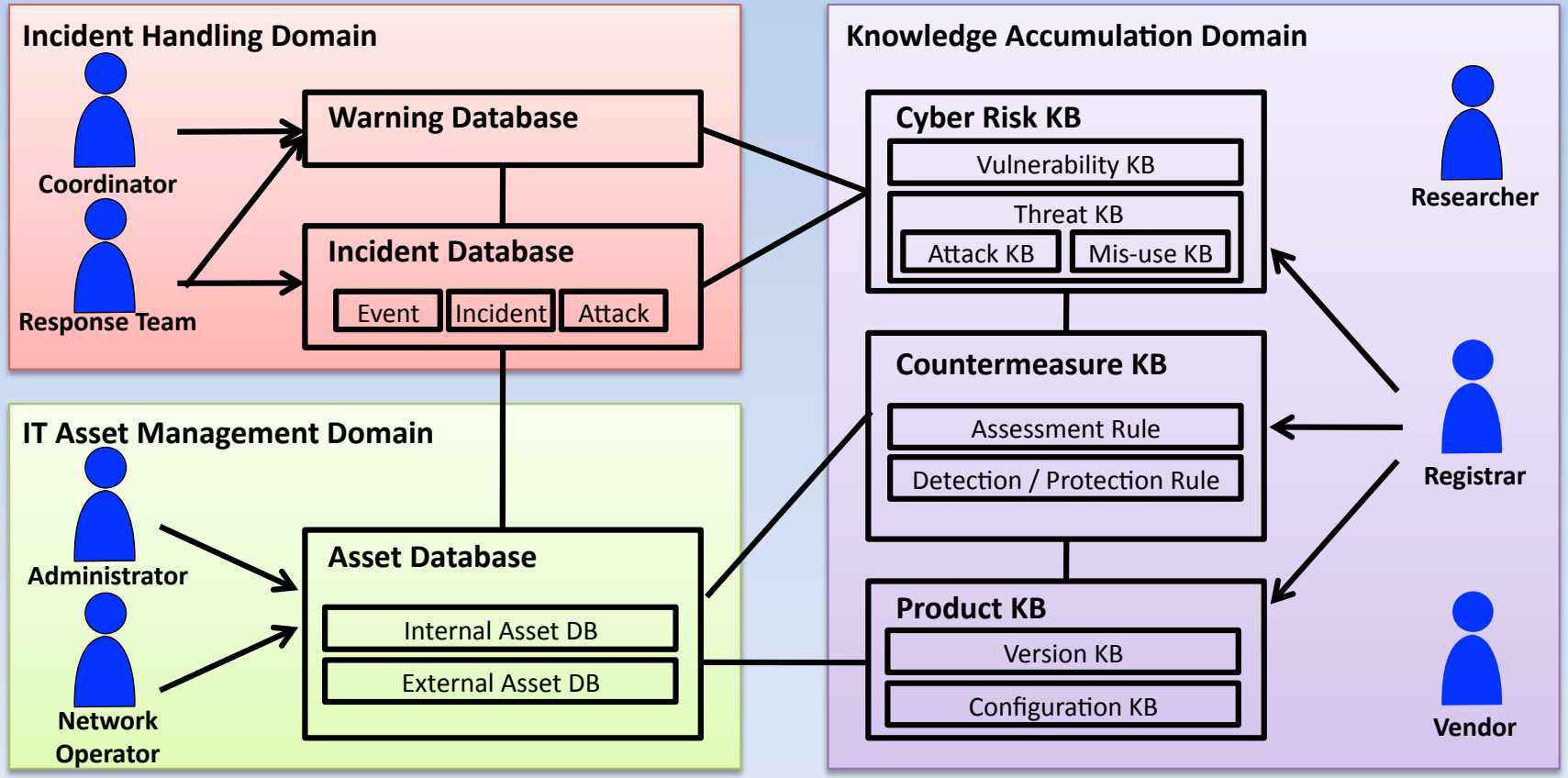
- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- requesting and responding with cybersecurity information
- exchanging of cybersecurity information over networks
- assuring cybersecurity information exchanges

Cybersecurity Entities

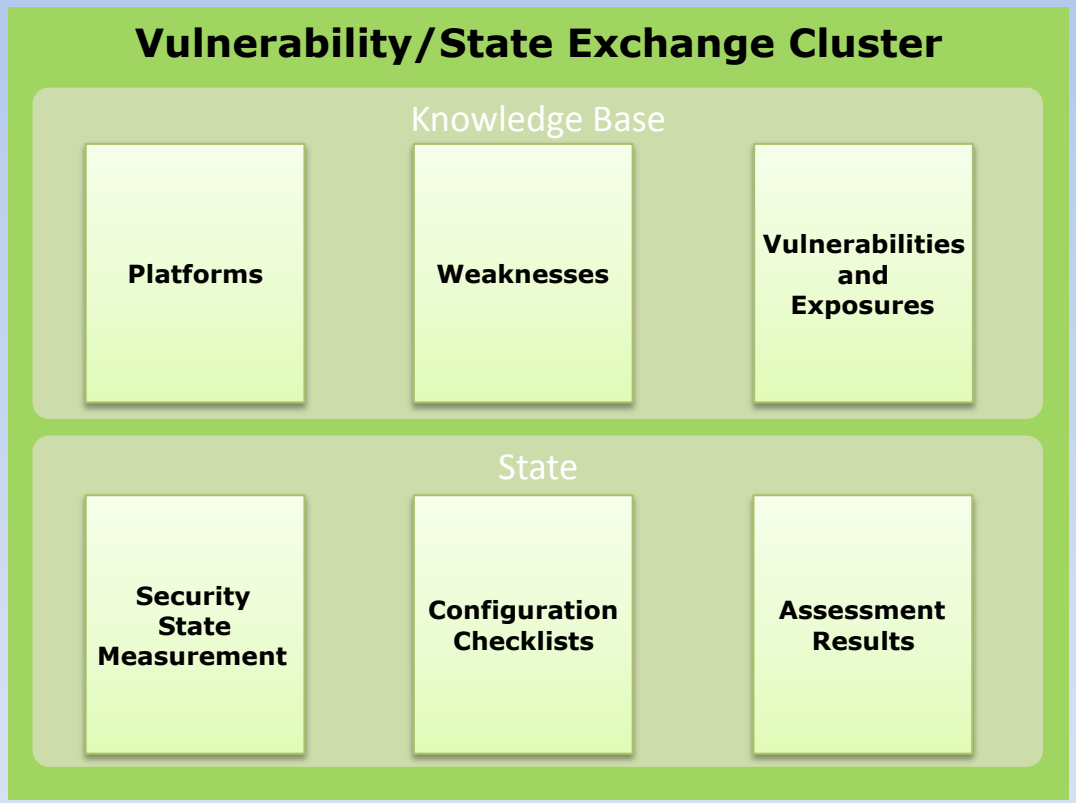
Cybersecurity Information use (out of scope*)

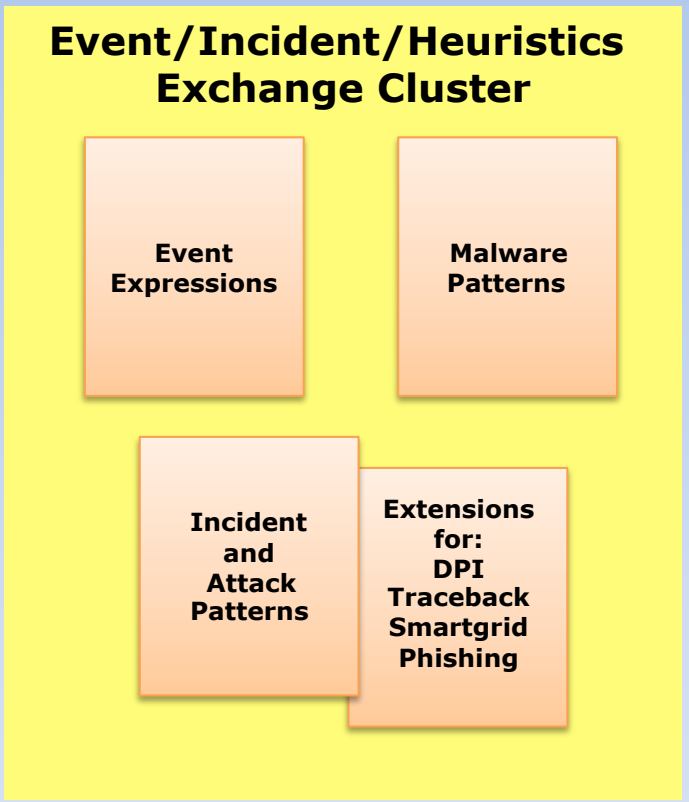
* Some specialized cybersecurity exchange implementations may require application specific frameworks specifying acquisition and use capabilities

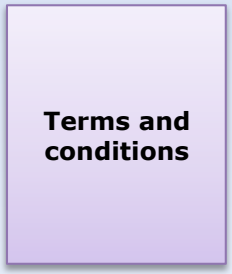
CYBEX Ontology

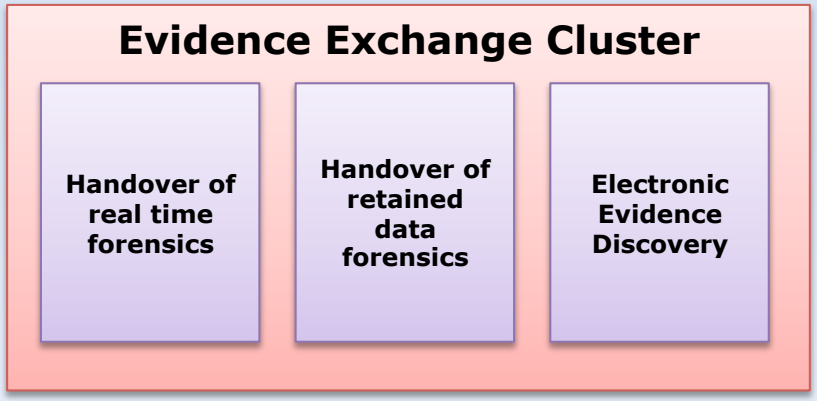


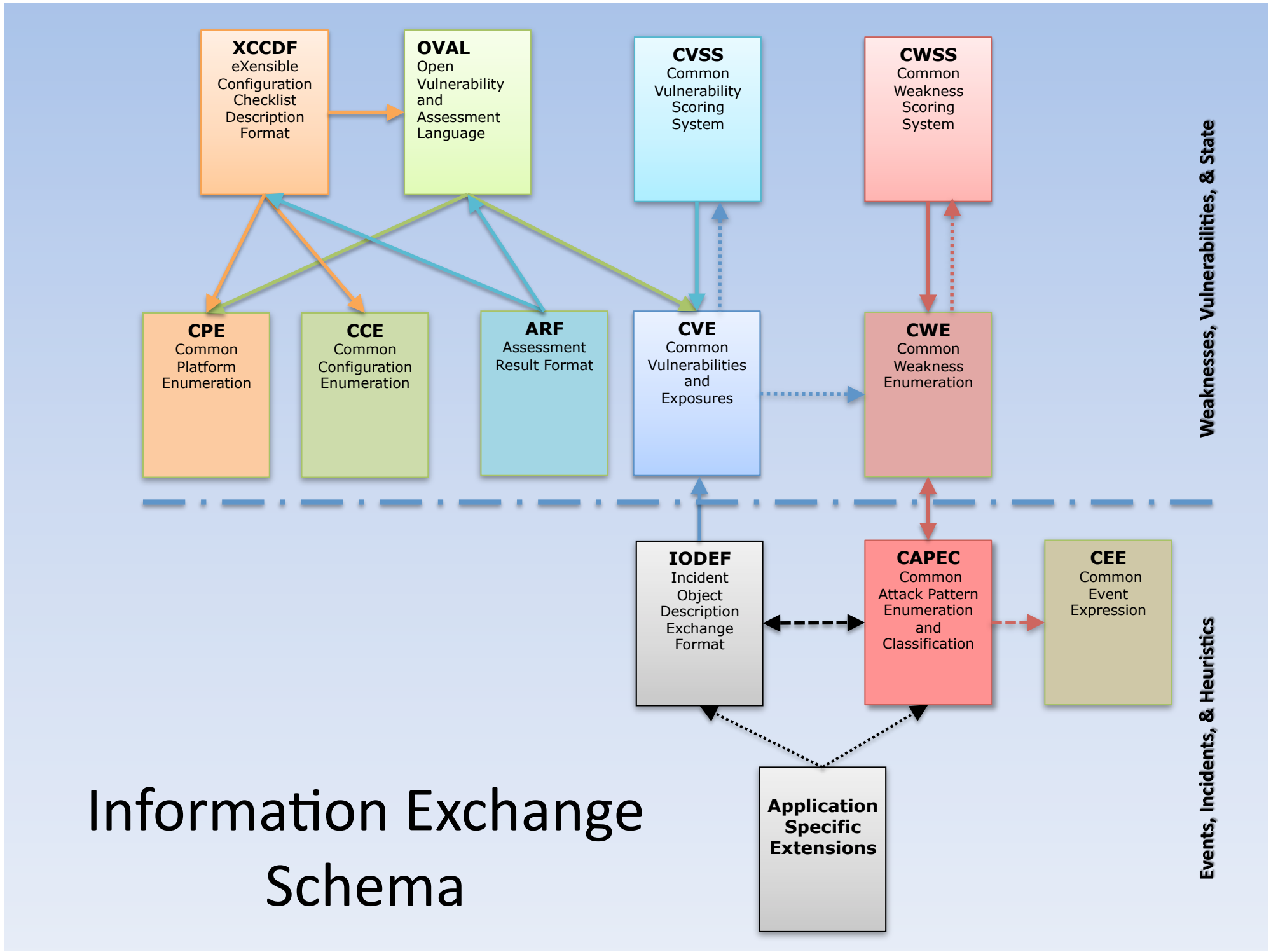
Information Exchange Structuring

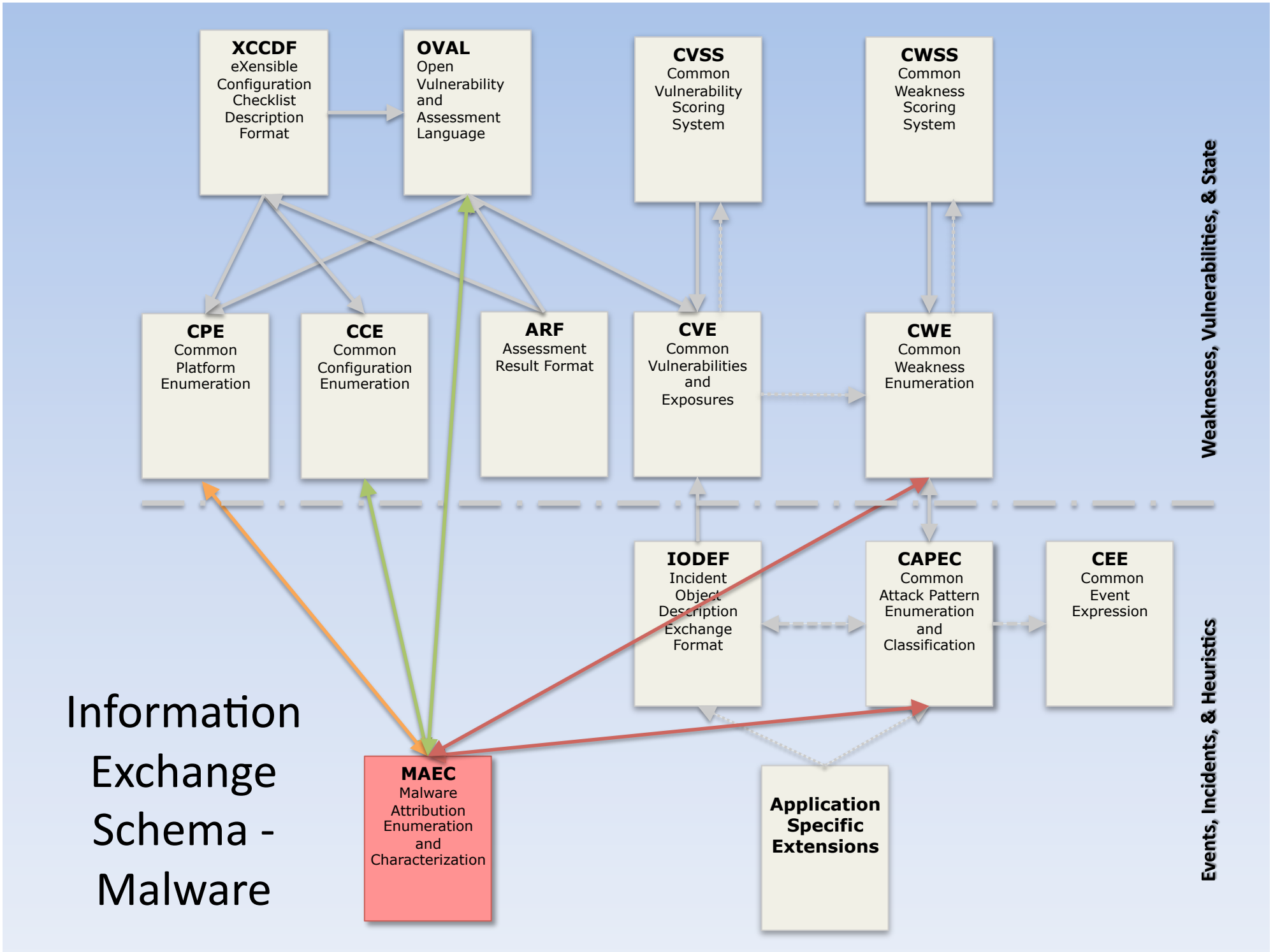


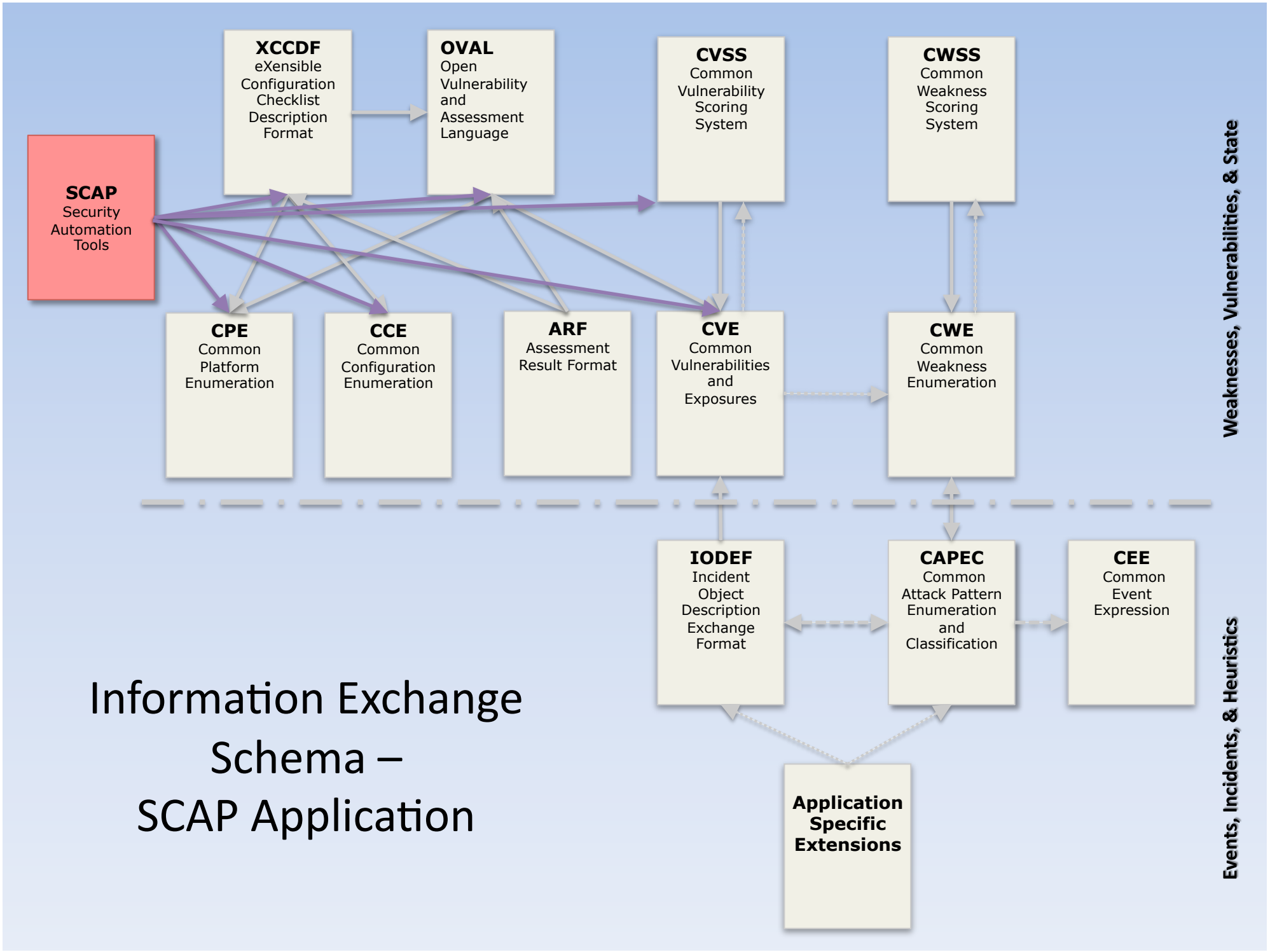







XCCDF
eXensible Configuration Checklist Description Format
OVAL
Open Vulnerability and Assessment Language
CVSS
Common Vulnerability Scoring System
CWSS
Common Weakness Scoring System
CPE
Common Platform Enumeration
CCE
Common Configuration Enumeration
ARF
Assessment Result Format
CVE
Common Vulnerabilities and Exposures
CWE
Common Weakness Enumeration
Weaknesses, Vulnerabilities, & State
IODEF
Incident Object Description Exchange Format
CAPEC
Common Attack Pattern Enumeration and Classification
CEE
Common Event Expression
Application Specific Extensions
Events, Incidents, & Heuristics
Information Exchange Schema


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
IODEF
Incident Object Description Exchange Format
CAPEC
Common Attack Pattern Enumeration and Classification
CEE
Common Event Expression
MAEC
Malware Attribution Enumeration and Characterization
Application Specific Extensions
Weaknesses, Vulnerabilities, & State
Events, Incidents, & Heuristics
Information Exchange Schema - Malware


XCCDF
eXensible Configuration Checklist Description Format
OVAL
Open Vulnerability and Assessment Language
CVSS
Common Vulnerability Scoring System
CWSS
Common Weakness Scoring System
SCAP
Security Automation Tools
CPE
Common Platform Enumeration
CCE
Common Configuration Enumeration
ARF
Assessment Result Format
CVE
Common Vulnerabilities and Exposures
CWE
Common Weakness Enumeration
Weaknesses, Vulnerabilities, & State
IODEF
Incident Object Description Exchange Format
CAPEC
Common Attack Pattern Enumeration and Classification
CEE
Common Event Expression
Application Specific Extensions
Events, Incidents, & Heuristics
Information Exchange Schema – SCAP Application

Information Exchange Trust capabilities

Discovery of parties, standards, schema, enumerations, instances and other objects

- Common Namespace
- Discovery enabling mechanisms
- Request and distribution mechanisms

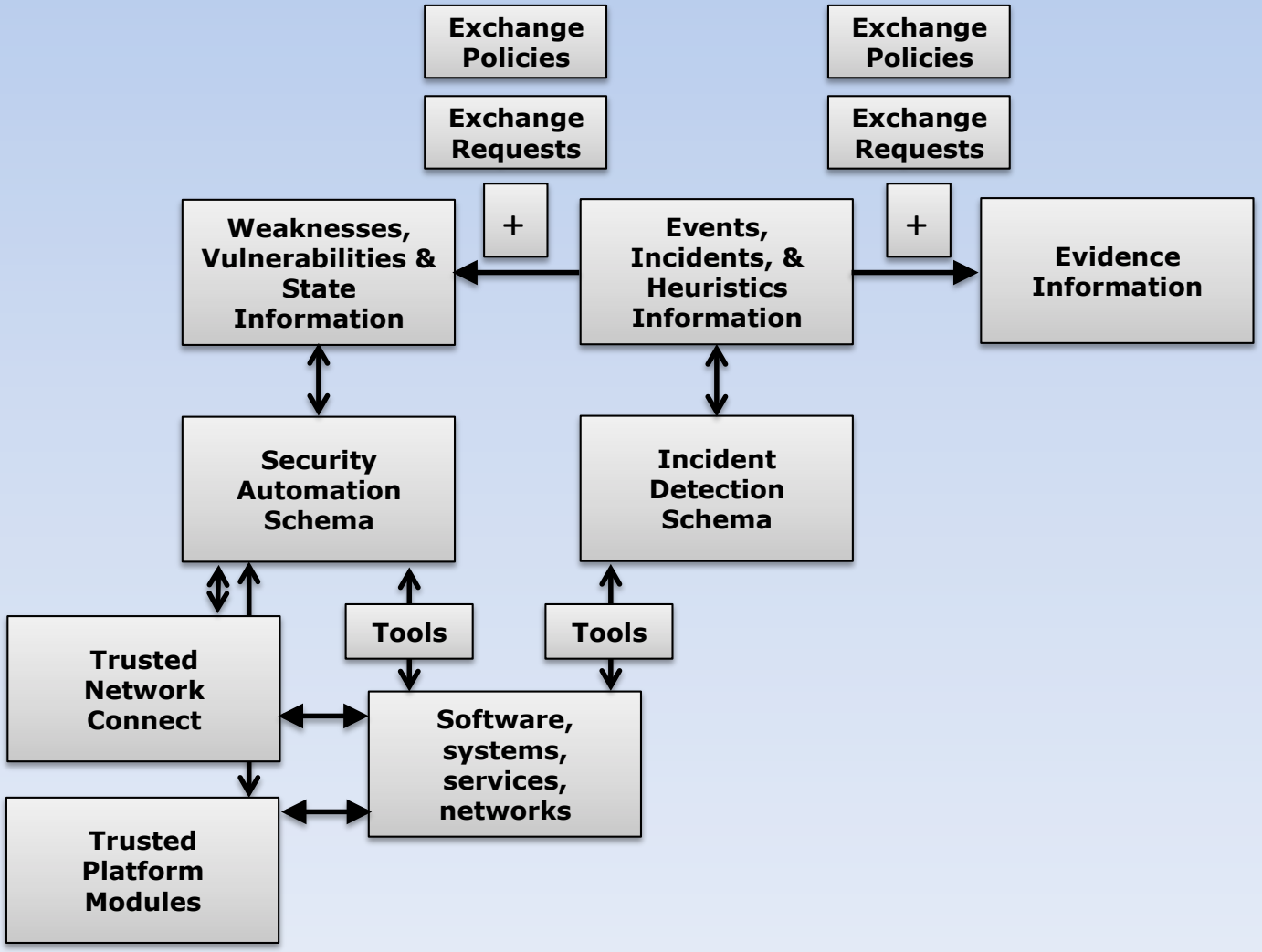
Identity Assurance Cluster

- Trusted Platforms
- Authentication Assurance Methods
- Authentication Assurance Levels

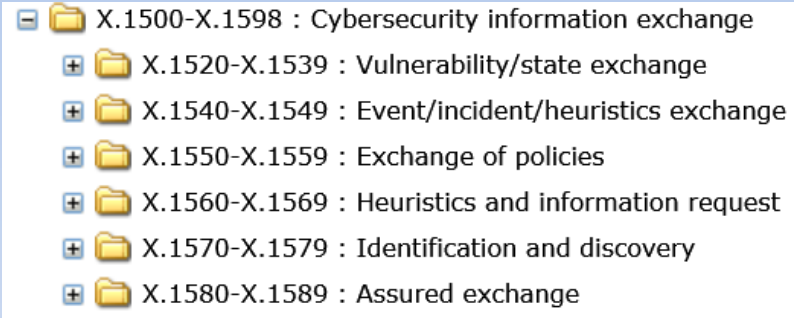
Exchange Cluster

- Trusted Network Connect
- Interaction Security
- Transport Security

CYBEX Implementation



So where do we go from here: the challenges



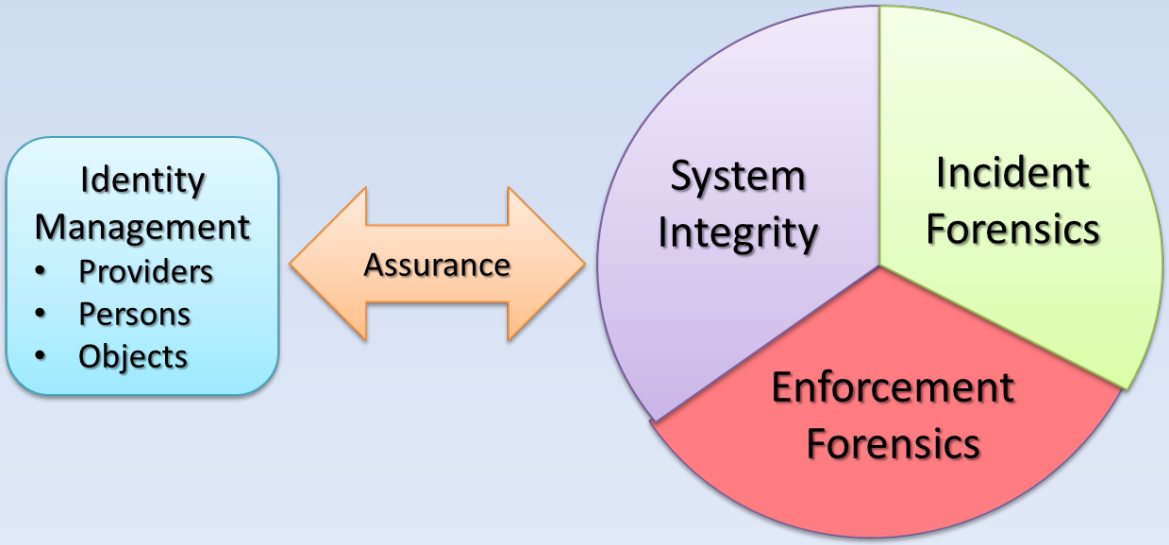
- An entire ITU-T Recommendation X-series has been allocated
- Recs. X.cybex, X.cve, X.cvss should be approved in December
- Future of IODEF remains a question mark
- Many additional CYBEX pieces are in various stages of preparation for adoption during 2011-2013 and subsequent maintenance
- A global structured website of cybersecurity organizations has been created on ITU-T website
- Substantial challenges remain…

Challenge:
Extent and evolution of CYBEX Recommendation

- Is the framework currently complete?
- What standards should be included in the framework? What are the criteria for inclusion?
- Which standards get published as ITU-T Recommendations and which do not?
- How do ITU-T published versions maintain "sync" with authoritative community versions?
- How do regional and national variants/schemas become included?
- How should Security Content Automation Protocol (SCAP) schema be treated?
  - Presently included in an appendix as examples
- How does CYBEX deal with "soft" standards, e.g., other ITU-T, ITU-D, ISO SC27
  - Presently referenced in an appendix

Challenge:
Discovery and trust capabilities

- Cybersecurity object discovery, trust, and related exchange policy mechanisms are compartmentalized, incoherent, and frequently primitive
- Identity Management for cybersecurity has complex assurance relationships



Ongoing relevant cybersecurity IdM developments

- eDiscovery
  - Trusted discovery of identifier meta information is essential in distributed systems
  - Bob Kahn has been leading effort in ITU-T to develop a X.discovery specification
- Resolvers
  - New joint ISO ITU-T specification ITU-T X.673 | ISO/IEC 29168-2 provides for DNS based ability to resolve OIDs to information addresses
  - Handles system proceeding in ITU-T
- Trust interoperability
  - Joint ITU-T and ISO X.eaa specification currently being discussed
  - ENISA trust interoperability protocol may be underway in OASIS
- Cloud/Smartgrid Identity
  - Multiple global initiatives underway to develop specifications for cloud and Smartgrid Identity (ITU-T, OASIS, 3GPP, CEN, ISO, NIST, etc)
- Platform trust
  - Trusted Platform Module and Trusted Network Connect now included in CYBEX standard
    - Should Virtual TPMs be included?
  - Distribution channel trust
    - OID based NID standards emerging as a major object ID platform for distribution chain trust
    - Handles based DOIs a second order choice
    - What others exist?
- No apparent consensus on use of cyber security object identifiers
- NICT contributions have been seminal in exploring naming and discovery options
- CNIS (Cyber-security Naming and Information Structures Group) is emerging as a significant new forum for treating CYBEX information identifiers

Challenge:
Achieving implementation and widespread use

- Much public and industry dialogue is primitive, fractious, and politically contentious at best – especially in the West
  - See, e.g., FCC Cybersecurity Roadmap proceeding in Docket 10-146
- Meaningful platforms (e.g., CYBEX), like the systems involved, are complex
- Best initial implementation avenues are within coherent bounded communities
  - ISOG-J
  - National government networks
  - Common Criteria Control Board
  - NATO
- SCAP implementations should proliferate
  - How to enumerate and discover?
- Analytical "bridging" platforms are emerging
  - Deep Packet Inspection
  - Application/platform behavior signature enumerations
- Ultimately carefully designed mandates by national regulatory authorities seem likely to emerge

Exemplar:

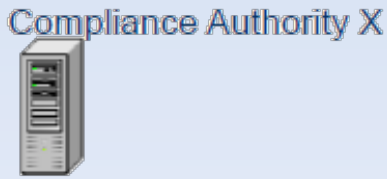
6th IT Security Automation Conference, Baltimore, 27-29 Sep 2010*

Emerging NIST view of CYBEX as SCAP

A familiar ensemble

	SCAP 1.0	SCAP 1.1	SCAP 1.2
Scheduled Release Date	Currently Final	Q4, 2010 – Final Version	Q1, 2011 – Initial Draft
Included Specifications	• CVE • CCE 5.0 • CPE 2.2 • XCCDF 1.1.4 • OVAL 5.3, 5.4 • CVSS 2.0	• CVE • CCE 5.0 • CPE 2.2 • XCCDF 1.1.4 • OVAL 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 • CVSS 2.0 • OCIL 2.0	• CVE • CCE 5.0 • CPE 2.3 • XCCDF 1.2 • OVAL 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 • CVSS 2.0 • OCIL 2.0 • ARF 1.0 • AI 1.0

A significant dependency



Credit: Overview by Paul Cichonski, BAH-NIST

*See: http://scap.nist.gov/events/2010/itsac/presentations/index.html

Exemplar:
Japan Vulnerability Notes

JVN Japan Vulnerability Notes

Date Last Updated:October 05, 2010

JVN English Site Open

Past Announcements

Recent Vulnerability Notes

RSS

JVN#69191943:		AD-EDIT2 vulnerable to cross-site scripting [October 05, 2010 11:00]
JVN#35605523:		Cross-site scripting vulnerability in Access Analyzer CGI by futomi's CGI Cafe [September 10, 2010 12:00]
JVN#75101998:		moobbs2 vulnerable to cross-site scripting [August 31, 2010 11:00]
JVN#24423311:		moobbs vulnerable to cross-site scripting [August 31, 2010 11:00]
JVN#12683004:		SEIL/X Series and SEIL/B1 IPv6 Unicast RPF vulnerability [August 25, 2010 12:00]
JVN#91740962:	Critical	Winny vulnerable to buffer overflow [August 20, 2010 12:00]
JVN#21471805:	Critical	Winny vulnerable to buffer overflow [August 20, 2010 12:00]
JVN#25393522:	Critical	Winny node information processing vulnerability [August 20, 2010 12:00]
JVN#54336184:	Critical	Winny BBS information processing vulnerability [August 20, 2010 12:00]
JVN#86832361:		Microsoft Windows denial of service (DoS) vulnerability [August 13, 2010 15:00]
JVN#34729123:		Explzh buffer overflow vulnerability [June 22, 2010 14:00]
JVN#67120749:		Multiple vulnerabilities in ActiveGeckoBrowser [June 17, 2010 19:15]
JVN#36925871:		e-Pares vulnerable to session fixation [June 02, 2010 15:00]
JVN#82465391:		e-Pares vulnerable to cross-site request forgery [June 02, 2010 15:00]
JVN#58439007:		e-Pares vulnerable to cross-site scripting [June 02, 2010 15:00]

JVN

- HOME
- What is JVN ?
- Instructions
- List of Vulnerability Report
- VN_JP
- TRnotes
- JVN iPedia
- JVNJS/RSS
- Vendor List
- Contact

JVN provided by

- JPCERT/CC
- IPA

Related Associations

- JEITA
- JISA
- CSAJ
- JNSA

Partners

- CERT/CC
- CPNI

CVE COMPATIBLE