Information Security
Exchange Formats and Standards
Till Dörges
Table of Contents / Outline

- About the Author
- Preliminaries
  - Definitions
  - Standards of Choice
  - Areas for Standards
- Standards
- Conclusion
About the Author

- 2002 started working for PRESECURE
  - Consulting
  - Research (eCSIRT.net, POSITIF, CarmentiS, …)
  - …

- 2008/12 PRESENSE Technologies GmbH founded with 3 colleagues
  - Founder
  - Managing Director

- PRE-CERT Team-Representative
  - FIRST
  - Trusted Introducer (TI)
Motivation

- Standards can help
  - Collaboration ↔ Information exchange
  - Clear semantics
  - Process automation

- Overview
  - Many standards exist
  - Important areas unstandardized?
Definitions

- **Standard / Specification**
  - Norm, requirement
  - Formal document, that establishes uniform methods, processes
  - Explicit set of requirements

- **Language**
  - Description of actual information

- **Enumeration**
  - Vocabulary, ontology
Definitions (cont'd)

- Data model
  - What information
- Data format
  - Bit sequence
- Protocol
  - How to exchange with others
- Other
  - Metric
  - Collection of standards
Standards of choice

- IT security only
- Very many standards exist
- Excluded
  - ISO 27001, ...
  - Emergency standards (EXDL, CAP, ...)
  - Military interoperability Standards (ICD, ...)
  - RFC 2350, Expectations for Computer Security Incident Response
Areas for Standards

- Advisory exchange
- Asset
  - Management
  - Security assessment
- Early Warning
- Incident handling (Phishing, Spam)
- Intrusion detection
- Malware (Naming, ...)
- Patch management
- Threat management
- Vulnerability management
Area Dependencies

- Areas include others
Investigation of Standards

- **Purpose:** Description (what)
- **Area:** Domain
- **Author:** Organization, Person (who)
- **Year:** Last update of standard
- **URL:** Homepage
- **Type:** Enumeration, Language, Other?
- **Used:** Is it used? If so, where?
- **Comment(s)**
Standards: Asset

- CAPEC, Common Attack Pattern Enumeration and Classification
  - standard schema for representing attack patterns
  - Cigital Inc. (sponsored by US DHS), 2008
  - http://capec.mitre.org/

- CCE, Common Configuration Enumeration
  - purpose: provides unique identifiers to system configuration issues
  - MITRE Corporation, 2009
  - http://cce.mitre.org/
Standards: Asset (cont'd)

- **CIM, Common Information Model**
  - provide a common definition of management information for systems, networks, applications and services, and allows for vendor extensions
  - Distributed Management Task Force, Inc., 2009
  - [http://www.dmtf.org/standards/cim/](http://www.dmtf.org/standards/cim/)

- **CMSI, Common Model of System Information**
  - machine readable descriptions of systems (products, platforms, not hardware)
  - CERT-Verbund, 2005
  - [http://www.cert-verbund.de/cmsi/](http://www.cert-verbund.de/cmsi/)
Standards: Asset (cont'd)

- **CPE, Common Platform Enumeration**
  - structured naming scheme for information technology systems, platforms, and packages (URI style)
  - (?) MITRE, 2009
  - http://cpe.mitre.org/

- **CRF, Common Result Format**
  - standardized IT asset assessment result format that facilitates the exchange of assessment
  - http://makingsecuritymeasurable.mitre.org/crf/
  - MITRE Corporation, 2007
Standards: Asset (cont'd)

- DPE, Default Password Enumeration
  - enumeration of default logons and passwords of network devices, applications, ...
  - Security-Database, 2008

- OVAL, Open Vulnerability & Assessment Lang.
  - standardize the transfer of this information across security tools and services
  - MITRE, OVAL Board, sponsored by the US-CERT at the U.S. DHS, 2008
  - http://oval.mitre.org/
Standards: Asset (cont'd)

- XCCDF, Extensible Configuration Checklist Description Format
  - structured collection of security configuration rules for some set of target systems
  - NIST, 2008
Standards: Vulnerability

- **CVE, Common Vulnerabilities and Exposures**
  - dictionary of publicly known information security vulnerabilities and exposures
  - CVE Editorial Board, MITRE, 2009
  - [http://cve.mitre.org/](http://cve.mitre.org/)

- **CVSS, Common Vulnerability Scoring System**
  - vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response
  - FIRST, CVSS-SIG, 2007
  - [http://www.first.org/cvss/](http://www.first.org/cvss/)
Standards: Vulnerability (cont'd)

- VEDEF, Vulnerability and Exploit Description and Exchange Format
  - free exchange of information on new Vulnerability and Exploit
  - (?) 2005
  - http://www.vedef.org/ (offline)

- VuXML, Vulnerability and Exposure Markup Language
  - vulnerability database for FreeBSD
  - Jacques A. Vidrine, 2005
  - http://www.vuxml.org/
Standards: Vulnerability (cont'd)

- OASIS Application Vulnerability Description Language TC (AVDL)
  - create a uniform way of describing application security vulnerabilities
  - OASIS AVDL TC, 2004
Standards: Advisory

- CAIF, Common Announc't Interchange Format
  - RUS-CERT, 2005
  - http://www.caif.info/

- DAF, Deutsches Advisory Format
  - profile for EISPP
  - CERT-Verbund, 2004
  - http://www.cert-verbund.de/daf/index.html

- European Information Security Promotion Programme (EISPP) advisory format
  - EISPP consortium, 2004
  - http://www.eispp.org/
Standards: Threat analysis

- CWE, Common Weakness Enumeration
  - (not sure about area classification)
  - unified, measurable set of software weaknesses
  - MITRE Corporation, 2009
  - http://cwe.mitre.org/
Standards: Malware

- CME, Common Malware Enumeration
  - provide single, common identifiers to new virus threats (...) neutral indexing
  - CME Editorial Board, 2005
  - http://cme.mitre.org/

- “DHS/DoD Software Assurance Forum Malware Working Group”
  - Develop Malware Attribute Enumeration and Characterization (MAEC)
  - https://buildsecurityin.us-cert.gov/swa/malact.html
Standards: Intrusion Detection

- **IDMEF, Intrusion Detection Msg. Exchange Format**
  - Data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems
  - IETF, IDWG, 2007

- **IDXP, Intrusion Detection Exchange Protocol**
  - Exchange of IDMEF messages, BEEP profile
  - IETF, IDWG, 2007
Standards: Incident Handling

- IODEF, Incident Object Desc. Exchange Format
  - sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents
  - APWG extensions
  - IETF, INCH WG, 2007

- ARF, Abuse Reporting Format
  - communicating feedback about email abuse
  - MIPA, 2009
Standards: Other

- CEE, Common Event Expression
  - creation of a Common Event Taxonomy that allows event producers to consistently and unambiguously define each heterogeneous event;
  - creation of a Common Log Syntax combined with a public data dictionary to provide consistency for specifying and gathering event-specific details.
- docs announced for Feb 2008 (behind schedule)
- http://cee.mitre.org/
- Indirectly: Intrusion Detection, Incident Handling
Standards: Other (cont'd)

- **SCAP, Security Content Automation Protocol**
  - combines a number of open standards that are used to enumerate software flaws and configuration issues related to security
- **CVE, CCE, CPE, CVSS, XCCDF, OVAL**
- **Superset: Asset & Vulnerability**
- **NIST**
- [http://nvd.nist.gov/scap.cfm](http://nvd.nist.gov/scap.cfm)
Standards: Missing?

- **Patch Management**
  - included in Asset management
- **Early Warning**
  - IODEF perhaps enough
- **Malware**
  - no active standard
  - enumeration difficult, but important
- **Threat**
  - CWE used elsewhere
Summary

- Investigated > 30 standards
  - 13 languages
  - 8 enumerations
  - 5 other
- 9 unused (dead or never alive)
- 6 unclear
- 17 actively used or developed
<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advisory</td>
<td>3</td>
</tr>
<tr>
<td>Asset</td>
<td>9</td>
</tr>
<tr>
<td>Early warning</td>
<td>-</td>
</tr>
<tr>
<td>Incident handling</td>
<td>2</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>2</td>
</tr>
<tr>
<td>Malware</td>
<td>2</td>
</tr>
<tr>
<td>Patch</td>
<td>-</td>
</tr>
<tr>
<td>Threat</td>
<td>1</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>5</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
</tr>
</tbody>
</table>
Thank you

Thanks for your attention!

Questions?
Contact Information

Till Dörges
PRESENSE Technologies GmbH

doerges@pre-sense.de
http://www.pre-sense.de/

PGP
- 0x37FC5954
- F95B 5EBE 9DFC 3B30 1800 9492 2901 BAED 37FC 5954