Semantic Potential of existing Security Advisory Standards

Secure Business Austria
Challenges

• Well maintained and audited IT infrastructure is critical for ensuring business continuity
  – Ever-growing complexity of IT environments
  – Legal regulations and rating systems (e.g., Basel II)
  – Numerous security alerts
    • majority is not structured for automatic processing

→ Management of networks and IT infrastructure elements is time-consuming and expensive
Challenges

• CERT Coordination Center
  - Cataloged vulnerabilities doubled in the past three years (3780 in 2004; 7236 in 2007).

• Channels
  - 93% of the CSIRT constituents receive their incident information via email, 79% also via phone
  - RSS Feeds, Websites, faxes, SMS, …
  → Unstructured and therefore not machine-processable
CSIRT

• CSIRT (Computer Security Incident Response Team)
  – Reactive Services (Incident Handling, Alerts and Warnings, …)
  – Proactive Services (Configuration, Technology Watch, Announcements, …)
  – Security Quality Management Services (Risk Analysis, Training, …)

• Advisory Messages
  – Describe computer security problems and/or solutions
Contribution

- Introduction of a collection of existing security advisory standards
- Review and evaluation of those standards
Evaluation

• Goal
  – Identification of semantic usable standards

• Criteria
  – Semantic Usability
    • Does the standard use a standardized language such as XML to ensure machine-readability?
    • Does the standard provide clear and unambiguous semantics to ensure machine-recognition?
  – Information Complexity
    • Does the standard provide the necessary elements for describing IT incidents? A comprehensive and well defined set of elements is required to describe IT incidents in the most granular form.
    • Does the standard offer the possibility for a complete workaround for an IT incident or does it simply provide links to external resources?
Evaluation

• Distribution
  – Is this standard used by any major CSIRTs?
  – Is it still supported? When was the last update?
  – The usage and support by major CSIRTs is crucial for the acceptance of the semantic security advisory standard within the community.
ANML

- Advisory and Notification Markup Language
- XML-based specification for advisories and other types of notifications
- Open Security Project (OpenSec)
- Aims to solve inconsistent use of terminology
  - Benefit for the community and vendors
- Notifications: bug-fixes, feature enhancements, upgrade availability,…
- Description, Status, Affected, Assessments, Update, Verify, and Revision History
ANML Example

```xml
<?xml version="1.0" encoding="utf-8" ?>
...
<subject>Unchecked Buffer In Windows...</subject>
<dateCreated>2003-03-17</dateCreated>

<status>
  <vendor>Confirmed</vendor>
  <severity>Critical</severity>
  <class>Buffer overflow</class>
...
</status>
<summary>...</summary>
<affected>
  <system id="WinNT">
    <os>
      <name>Windows NT 4.0</name>
      <productType>Server</productType>
      <productType>Workstation</productType>
    </os>
  </system>
...
```
ANML

- Semantic usability ~
  - Introduction of “RDF” element
  - Allows the usage of free text fields
    - OS name, productType, .. “xs:string” (“Windows” / “Win”)
    - SDML, SIML

- Information complexity ~
  - Missing information (e.g., vendor, software on operating systems, and CVE ref.)

- Distribution –
  - No major CSIRTs are currently using ANML, last update 2003
EISPP

• European Information Security Promotion Programme
  – Advisory Format - precise and timely information about new vulnerabilities
• EU-funded (5th framework programme)
• June 2002 until January 2004
• Cert-IST, esCERT-UPC, SIEMENS-CERT, Callineb Consulting, I-NET, CLUSIT and InetSecur
• Basic: Complete Identification (CVE, Bugtrag ID,…), Vulnerability Classification, System Information, Problem Description and Solution
EISPP

• Semantic usability ~
  – Due to this flexibility, cooperating organizations sometimes need a further explanation of their usage conventions (free text fields)
  – e.g., <FormattedText>Foo v1.3 on BAR OS</FormattedText>
  – Common Model of System Information (CMSI)

• Information complexity ~
  – Missing attributes such as required reboot, software and hardware vendor

• Distribution +
  – German CERT-Verbund uses the EISPP extension DAF
CAIF

• Common Announcement Interchange Format
• Exchange and store security advisories
  – multi-lingual textual descriptions
  – different renderings (Markup)
• RUS-CERT
• Identification (target-group)
• Affected System (OVAL linking possible)
• identification, target-groups?, revisions, category, subject, summary, affected?, workaround?, solution?, ...

www.securityresearch.at

© 2004-2008 Secure Business Austria
CAIF

• Semantic usability ~

• MTEXT, UTEXT (e.g., affected systems)
  ```xml
  <!ENTITY % MTEXT "(
      %UTEXT; | p | b | vb | em | pre | vendor | program | file | aff | update | ...)
  ```

• Information complexity ~
  – e.g., affected system and its operating system, patch level, and vendor are not described by distinct elements

• Distribution ~
  – Some middle-sized and company-owned CSIRTs use the CAIF advisory standard
IODEF

- Incident Object Description Exchange Format
- Common data format for describing and exchanging incident information between CSIRTs
- IETF Extended Incident Handling (INCH) Working Group
- IDMEF compatibility
- Covers the entire attack (including e.g., log files)
IODEF

• Semantic usability ~
  – Overlapping elements such as Incident and EventData

• Information complexity -
  – No information on affected files, patch location (URL), or potential workaround

• Distribution +
  – Some vulnerability management tools are able to handle IODEF messages; Oct-10-2007: accepted for RFC publication
OVAL

- Open Vulnerability and Assessment Language
- Transfer & expression of public available security content
- Assessment Process
  - System Characteristics
  - Analysis (vulnerability, configuration, patch state, …)
  - Results schema
OVAL

• Semantic usability +
  – Well-defined and semantically usable

• Information complexity ~
  – Highly granular but missing patch information and predefined product lists (CPE in new versions “<reference source="CPE" ref_id="cpe:/o:microsoft:windows_2003::gold:itanium"/>”)

• Distribution +
  – OVAL is supported and used by several governmental and commercial organizations, Various existing tools
Conclusion

• Evaluation of existing security advisory standards
• OVAL standard is the most suitable standard for the automatic or semi-automatic interpretation of security advisories

→ Faster reaction times and avoidance of interpretation errors for newly-discovered vulnerabilities
Contact

Andreas Ekelhart
aekelhart@securityresearch.at