Semantic Potential of existing Security Advisory Standards

Stefan Fenz, Andreas Ekelhart, and Edgar Weippl

Abstract— **New discoveries made on a nearly daily basis and the constantly growing amount of vulnerabilities in software products have led to the distribution of great numbers of vendor dependent vulnerability information over various channels such as mailing lists and RSS (Really Simple Syndication) feeds. However, the format of these messages presents a major problem as it lacks standardized, semantic information, resulting in very time-intensive, expensive, and error-prone processing due to the necessary human involvement. Recent developments in the field of IT security have increased the need for a sound semantic security advisory standard that allows for automatic processing of relevant security advisories in a more precise and timely manner. This would reduce pressure on organizations trying to keep their complex infrastructures secure and up-to-date by complying with standards, such as Basel II and local legislations. This paper conducts an evaluation of existing security advisory standards to identify usable semantic standards, which enable the automated processing of security advisories to ensure faster reaction times and precise response to new threats and vulnerabilities. In this way IT management can concentrate on solutions rather than on filtering messages.**

I. Introduction

Over the years, the complexity of IT environments has grown at an extremely rapid pace. The range of functions provided by information technology reaches into almost every area of daily life. Therefore, a well maintained and audited IT infrastructure is critical for the maintenance of every organization. Legal regulations and rating systems, such as Basel II [1], in particular, require a certified and secure IT environment for allowing organizations to remain in the competitive market. The fact that IT environments grow in their complexity (e.g., heterogeneous environments, introduction of new technologies), makes the management of the networks and IT infrastructure elements very time-consuming and expensive [2] [3]. Those responsible, such as security administrators, have to deal with numerous security alerts related to different types of systems and platforms on a daily basis, thus they are not always able to filter relevant information for their organization [4] and to patch their systems appropriately [5]. According to the CERT (Computer Emergency Response Team) Coordination Center [6] their number of cataloged incident reports doubled in the past years (3780 reported incidents in the year 2004; 7236 reported incidents in the year 2007). An organization that practices due care has to check each reported security incident to determine whether that incident affects corporate assets. When a relevant incident has been identified, incident management must be initiated to avoid further damage within the organization's IT environment. According to the CSIRT (Computer Security Incident Response Team) Organizational Survey [7], 93% of the CSIRT constituents receive their incident information via email and 79% also via phone. The majority of these reports are not structured for automatic processing and human beings have to interpret and process the reports manually to filter information which is relevant to their IT infrastructure.

In conjunction with the nature of an emergency, which can vary from a natural disaster to a software vulnerability, different CSIRT (Computer Security Incident Response Team) types [8] are required and each type specifies its own security advisory format for exchanging information. As we will see in this paper, there are currently many security advisory standards available. Although they are all designed for describing advisories, they vary in terms of use, potential for machine-readability, and application area. Specifying vulnerabilities is a non-trivial task considering the immense variety of existing software and exploits. Due to the daily emergence of new exploits, software vendors must constantly fix security holes, leading to new releases of the vulnerable software, often resulting in new exploit families and new kinds of threats. Security advisory formats have been developed to release information about vulnerabilities and offer solutions.

In this paper a collection of existing security advisory standards is reviewed and compared in terms of semantic usability, information complexity and distribution.

II. Incident Management

In formulating our definition of the incident management concept we refer to the Information Technology Infrastructure Library (ITIL) [9]. The ITIL framework was founded by the Office of Governance Commerce (OGC) on behalf of the British government. Nowadays ITIL is the de-facto standard for service management and contains technical documentation for planning and supporting IT services. Service management is the framework for planning and coordinating all IT relevant activities and resources to meet the functional and strategic goals of an organization. The ITIL glossary [10] defines an incident as:

'An Incident is an unplanned interruption to an IT Service or reduction in the quality of an IT service. Any event which

Stefan Fenz and Andreas Ekelhart are with Secure Business Austria, Vienna, Austria (e-mail: {sfenz, aekelhart}@securityresearch.at).

Edgar Weippl is with the Institute of Software Technology & Interactive Systems, Vienna University of Technology, Vienna, Austria (e-mail: weippl@ifs.tuwien.ac.at).

This work was performed at Secure Business Austria, a competence center that is funded by the Austrian Federal Ministry of Economics and Labor (BMWA) as well as by the City of Vienna.

could affect an IT service in the future is also an incident.'

Incident management itself is defined in the ITIL glossary [10] as:

'Incident management is the process responsible for managing the life cycle of all incidents. The primary objective of incident management is to return the IT service to customers as quickly as possible.'

The process of incident management includes many activities to minimize the disruption caused by an incident and should bring the affected services or resources back into working order as quickly as possible. Initially, incidents are reported to CSIRTs via various channels such as phone calls, faxes, or emails. Obviously all of these incident reports have to be classified by type, status, urgency, impact, and priority in order to process the request efficiently. Afterwards, the reported incident is matched to an incident database and if the incident is not already known, a detailed description of the incident will be stored in the database to continue in the incident analysis phase. Appropriate response and recovery information is passed at a minimum to the incident reporter. Furthermore, information on the incident (security advisory) is distributed to other affected sites via channels such as mailings lists, RSS feeds, or websites.

III. Computer Security Incident Response Team

A CSIRT (Computer Security Incident Response Team) is an organization that attempts to limit the damage caused by exploits of vulnerable software and services. The CSIRT acts by responding, receiving, and reviewing incident reports that are used to exchange the information concerning new or known vulnerabilities and threats. The response and recovery information for the incident is propagated via various channels, such as mailing lists and RSS feeds, to the CSIRT's subscribers (e.g., governmental institutions, companies, and Internet service providers).

Due to the steady increase in amounts of security advisories, CSIRT subscribers are overwhelmed by processing warnings and are not able to react in a timely manner and take the necessary steps (e.g., patching). One of the main reasons is that among the numerous security advisories only a fraction is relevant to a specific organization.

Our research addresses the vulnerabilities of existing CSIRT approaches and works on the development of a semantic CSIRT, the Austrian Computer Security Incident Response Team (ATCSIRT)[1], in an effort to increase the degree of automation on the subscribers' side, to ensure faster reaction times and to avoid interpretation errors for newly-discovered vulnerabilities. Warnings are formatted in a semantic way to enable a filter mechanism to process only those messages that are relevant to a certain environment. A semantic security advisory standard is required for the automatic or semi-automatic interpretation of security advisories, which is addressed in this paper.

[1]ATCSIRT: http://research.securityresearch.at/research/projects/atcsirt/, last access: 15 April 2008

A. Channels

1) Mailing Lists: Nearly every CSIRT offers a mailing list to ensure that interested parties receive up-to-date information about the latest security issues per mail. Interested parties have to subscribe to this mailing list (the predecessor of the RSS feed) to receive information. RSS feeds enable the presentation of advisories, whereas mailing lists additionally support interaction between subscribers. Currently, most of the interaction between CSIRTs is handled by mailing lists. A major CSIRT, such as US-CERT[2] offers a great deal of information regarding new vulnerabilities via mailing lists, comprising information about security bulletins, tips for solving problems concerning vulnerabilities, and alerts caused by new threats.

2) RSS Feeds: Nearly every software vendor allocates its own RSS feed with the latest security information pertaining to its own products. The messages often contain in-depth information about vulnerabilities, including impact, remediation, updates, patches, and CVE (Common Vulnerabilities and Exposures)[3] references. Contrary to mailing lists, RSS feeds are XML-based, thus giving clients the opportunity to adapt the presentation style of the message.

3) Other Channels: Along with mailing lists and RSS feeds, other channels such as websites, faxes, phone calls, SMS messages, posted letters, and personal visits are additional options for the security advisory distribution. Compared to these channels, mailing lists and RSS feeds have the highest potential as a distribution channel for security advisories because they implement a push-model to ensure timely distribution and are able to reach a significant amount of subscribers at a low cost.

IV. Evaluation of existing standards

The goal of this security advisory standard evaluation is the identification of semantic usable standards since we aim to automatically or semi-automatically interpret security advisories. The following listing describes the individual criteria of the evaluation:

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.
  Required elements: subject, description, author, creation date, affected operating system, patch level of operating system, vendor of operating system, affected software, patch level of software, and vendor of software.

[2]US-CERT: http://www.us-cert.gov/, last access: 15 April 2008
[3]CVE: http://cve.mitre.org/, last access: 15 April 2008

Name	The name of the standard.
URL	A link to a location where further information about the standard can be found.
Issuer	The proposing organization.
Last Update	Represents the last update of the standard. This section shows if this standard is still in progress.
Version	Current version of the standard.
Classification	Type of the advisory standard: • IT incident management • Intrusion detection • General incident management
Summary	A short description of the standard.
Description	This section explains the standard in more detail.
Application	Current applications using the standard.
Strengths	Strengths of the standard identified on the basis of our evaluation criteria.
Weaknesses	Weaknesses of the standard identified on the basis of our evaluation criteria.

TABLE I
METHODOLOGY

Optional elements: CVE reference, general references, update date, change information for updated messages, patch location (URL), file size, file hash value, workaround description, severity rating, impact type, and if a reboot is required after patch implementation.

- Does the standard offer the possibility for a complete workaround for an IT incident or does it simply provide links to external resources?

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.

For each advisory format a description, identified strengths and weaknesses (see Table I), and a concluding rating, which uses the following rating schema is given:

+
The standard fulfills all or almost all criteria.
~
The standard accomplishes most of the criteria but there are shortcomings concerning the evaluation criteria.
-
The standard does not accomplish the criteria.

A. ANML

Name: Advisory and Notification Markup Language
URL: http://www.opensec.org/anml/
Issuer: OpenSec
Last Update: 8 October 2003
Version: 0.5
Classification: IT incident management

Summary: The Advisory and Notification Markup Language (ANML) is an XML-based specification for security advisories. The standard intends to solve the problem of software vendors using inconsistent terminology in their advisories and aims at machine-readability. Tools for automatic update services are a possible application. Although ANML is primarily designed for security advisories, it can be used for any type of notification. Some examples include bug-fixes, feature enhancement, and upgrade availability. [11]

Description: Besides the general description of the vulnerability (*subject*, *release date*, *revision history*, *summary*) the ANML structure provides an optional reference field for a more detailed external description (*vendor advisory*, *non-vendor advisory*, *alternative language*). The affected products and technical details about the vulnerability, as well as the availability of solutions (patch location or workaround description) have to be provided in the ANML message. Vendor status (*confirmed*, *unconfirmed*, etc.), severity rating (*low*, *medium*, *high*, *critical*), impact (e.g., system instability, read unauthorized files) and classification (e.g., buffer overflow, cross-site scripting) of the vulnerability are required for a valid ANML message.

Application: While the standard provides a solid framework in theory, we could not identify any CSIRTs providing ANML-formatted advisories.

Strengths: An advantage of ANML is the precise and clear description of a vulnerability. Although other standards provide more classification options, the straight-forward structure of ANML enables a fast transformation from non-semantic content, such as RSS feeds, websites, or mailing lists into XML-based ANML advisories.

Weaknesses: The ANML standard lacks some attributes that are required for automatic processing and furthermore, ANML does not support linking vulnerable software to its specific operating system. An inquiry shows that the standard has not progressed since its last update in 2003.

Rating:

semantic usability **~**
ANML is XML-based and provides to a great extent, a clear and unambiguous structure but unfortunately the standard allows the usage of undefined RDF (Resource Description Framework) elements, which narrows the semantic usability of the standard.

information complexity **~**
The ANML standard covers most of the elements defined in our evaluation criteria except for the required author and vendor element, the optional CVE reference, which is mixed with the general references, and information about required reboots. The standard offers the possibility for both workaround descriptions and patch location information as a vulnerability solution. Describing vulnerabilities for software products on specific operating systems is not specified in ANML.

distribution **-**

No major CSIRTs are currently using the ANML standard. Since the last update was on 8 October 2003, we assume that the standard is not being developed or supported.

B. EISPP

Name: European Information Security Promotion Programme

URL: http://www.eispp.org/

Issuer: Co-funded by the European Union under the Fifth Framework Programme, run by a consortium of private sector organizations, comprising CERTs, ISP/ASPs, and Security professional organizations (members are CERT-IST, esCERT-UPC, SIEMENS-CERT, Callineb Consulting, I-NET, CLUSIT, and InetSecur).

Last Update: 20 September 2004

Version: 2.0

Classification: IT incident management

Summary: The EISPP project [12] aims to develop a European framework to share security knowledge but also to define the content and ways of disseminating security information to small and medium sized enterprises and between CSIRTs. EISPP is an XML-based advisory standard.

Description: The EISPP format comprises a comprehensive set of elements and provides great flexibility by defining a minimum set of required elements, including complete identification data (*issuer*, *reference number*, *date*, *language*, *title*, and *abstract*), basic vulnerability classification information, system information, a problem description, and a solution. The vulnerability classification defines the nature and danger of the described vulnerability. The vulnerability identifier and the issuer, taken from a predefined list, including CVE, Security Focus Bugtraq, Sun Bug ID, etc., have to be provided. Classification values to define the confidence level, vulnerability category, and attack requirements are also taken from predefined lists. The vulnerability status, propagation method, immediacy, vulnerability effect, impact, and the current impact identification are supported by well-elaborated decision tables. Information on affected systems and platforms is modeled in the system information section. Workarounds and code fixes can be defined as advisory solutions. Furthermore, external references can be found in the references section.

DAF [4] (Deutsches Advisory Format), an extension to EISPP, developed and maintained by CERT-Bund, DFN-CERT, PRESECURE, and Siemens-CERT, is specially tailored for the needs of German CSIRTs. DAF modifies the EISPP standard in the following way: (1) Adding a model of system information to EISPP by introducing CMSI (Common Model of System Information) and (2) constraining the use of EISPP (e.g., EISPP allows to specify the current impact and risk rating of a vulnerability on the top-level of an advisory. DAF does not use these top-level elements but instead the corresponding fields directly within the *vulnerability* element).

Application: The SIRIOS (System for Incident Response in Operational Security) application, used by all members of the German "CERT-Verbund"[5], is an Open Ticket Request System (OTRS) framework made for incident management of CSIRTs. An additional module is able to generate advisories in EISPP format.

Strengths: The EISPP format offers a large degree of freedom and a rich set of predefined elements. A scheme for uniform evaluation of the vulnerability status, propagation method, immediacy, vulnerability effect and impact is part of the standard. EISPP has strong support of the German CSIRT network with regard to the distribution of this standard.

Weaknesses: Flexibility is often not an advantage with regard to semantic usability, thus EISPP needs further refinement for automatic processing. Some necessary connections and elements, such as connections between affected systems and specific solutions or detailed patch level information, are not integrated into this standard.

Rating:

semantic usability ~

EISPP is a comprehensive and flexible, XML-based standard. Due to this flexibility, cooperating organizations sometimes need a further explanation of their usage conventions (e.g., free text fields in an EISPP message could exist, which contain patch solution information and a link to the patch file).

information complexity ~

The EISPP standard covers most of the elements defined in our evaluation criteria except for the required hardware and software vendor, and information about required reboots is missing. The standard offers the possibility for both workaround descriptions and patch location information as vulnerability solutions but connections between solutions and affected systems are not provided. Furthermore, fields for the patch file size and hash value are not available.

distribution +

The "CERT-Verbund" manages the DAF, an EISPP extension and offers SIRIOS, a framework for Incident Handling and Vulnerability Management in Computer Emergency Response Teams.

C. CAIF

Name: Common Announcement Interchange Format

URL: http://www.caif.info/

Issuer: RUS-CERT (CSIRT of the University of Stuttgart)

Last Update: 10 November 2005

Version: 1.2

[4]DAF: http://www.cert-verbund.de/daf/daf_description.html, last access: 15 April 2008

[5]CERT-Verbund: http://www.cert-verbund.de/, last access: 15 April 2008

Classification: IT incident management

Summary: CAIF [13] is an XML-based message format that is used to exchange and store security advisories. It is possible to address more than one security issue in one document and it allows defining each issue for different technical abilities and in different languages.

Description: This section will only describe mandatory and important elements of the standard. CAIF offers a number of markup elements used for presentation, which will not be included here. The element *identification* provides information to uniquely identify the document by author and issuer. The element *target-groups* intends to define users based on different languages and technical abilities. The element *category* describes the affected product and the platform relevant for the vulnerability. The elements *subject* and *summary* define the subject and provide a short description of the vulnerability in a human-readable form. The *problems* element represents the problems in natural language and it is possible to describe one or more vulnerabilities in this section. Some of them refer to a CVE number, CAN number, or Microsoft Security Bulletin. This section allows a very detailed description, including the status, impact, risk level, release, and the affected files or registry entries of the problem. The element *solution* contains the solution or links to patches that mitigate the vulnerability.

Application: Several CSIRTs, such as RUS-CERT (Stuttgart University), CERT-VW (Volkswagen AG), dCERT (Deutsche Telekom AG), and ComCERT (Commerzbank AG) currently use the CAIF advisory standard.

Strengths: The strength of the CAIF advisory standard is its semantics, which enable a very detailed and multi-lingual description of a vulnerability and possible solutions.

Weaknesses: Although CAIF offers a wide range of distinct elements to describe a vulnerability it neglects some important information such as required reboots and a machine-readable description of the affected systems and possible patch locations. The affected operating system or software, including its patch level and vendor, is described in one element, which makes it complicated for a machine to interpret the information in an unambiguous way. Solutions (human-readable descriptions and patch locations) are also defined in one element, which makes the automatic processing of that information (e.g., automatic patch download) more complicated.

Rating:

semantic usability ~
The XML-based CAIF advisory standard provides mostly clear semantics but the affected systems and solutions are not defined as distinct information objects.

information complexity ~
CAIF covers most of the elements defined in our evaluation criteria except for the element that defines a required reboot of the affected system. Furthermore, the affected system and its operating system, patch level, and vendor as well as the patch location are not described by distinct elements, which makes it hard to process this information automatically.

distribution ~
Several middle-sized and company-owned CSIRTs use the CAIF advisory standard. The distribution of the standard is mainly confined to the German area.

D. IODEF

Name: Incident Object Description Exchange Format
URL: http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-11.txt
Issuer: IETF Extended Incident Handling Working Group (INCH WG)
Last Update: 14 March 2007
Version: Internet draft expiring on 15 September 2007
Classification: IT incident classification

Summary: The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by CSIRTs about computer security incidents.

Description: An IODEF message consists of one or more *incident* elements. Each of these elements can be referred to by the globally unique attribute *incidentID*, assigned by the CSIRT that generates the IODEF document. The element *contact* describes contacts for organizations that are involved in the incident. The element *method* describes the methodology used by the intruder to exploit the vulnerability. It allows linking this description to external resources such as a CVE number. The element *assessment* describes the consequences of the incident, including the technical description of the impact and resulting activities, taking time and financial loss into account. Each sub element of *assessment* holds the attribute severity. This attribute accepts the values “high”, “medium” and “low” and denotes the estimate of the relative severity of the activity. The element *EventData* describes a particular event of the incident in detail, specifying the impact of the incident on a target and the techniques that are used by the intruder to exploit the vulnerability. The sub element *flow* explicitly describes the affected target and offers the elements *node*, *service*, and *operatingsystem*. The element *node* denotes the fully qualified domain name and the network or hardware address of the node. The element *service* enables specifying the service and vulnerable application.

Application: The Japanese organization IPA provides Java packages[6] that allow for generating IODEF documents.

[6]IPA: http://www.ipa.go.jp/security/fy16/development/IODEF/api/overview-summary.html, last access: 15 April 2008

An additional module for the application SIRIOS is able to generate security incident reports in IODEF format. The *Automated Incident Reporting*[7] project (initiated by CERT/CC) is a scalable distributed system for sharing security event data among administrative domains, such as CSIRTs. This system provides several formats for exchanging incident reports, such as IODEF and IDMEF.

Strengths: IODEF is meant to provide a picture of the entire attack in an incident that exploits a specific vulnerability. Therefore, unlike the other advisory standards it allows specifying the source and the target of an incident. Furthermore, it enables describing data (e.g., log files) caused by the incident.

Weaknesses: There are overlapping elements, such as *incident* and *EventData*. Both consist of nearly the same elements but differ in their meaning. While the element *incident* offers a summary of the entire incident, the element *EventData* describes specific events relating to the incident. This potentially ambiguous semantic description may lead to confusion in reading and analyzing.

Rating:

semantic usability ~
IODEF is XML-based and most of the elements are clear and unambiguously defined. Nevertheless, the overlapping of the elements *incident* and *EventData* lowers the rating.

information complexity -
IODEF allows for detailed descriptions of software products and operating systems, but it does not offer a way to specify optional elements, such as the affected files, patch location (URL), and the entire workaround. In addition, information on required reboots is missing. IODEF is capable of reporting incidents in detail but does not offer many elements necessary to pose as an advisory standard.

distribution +
Some vulnerability management tools developed by major CSIRTs can handle IODEF messages and unlike other standards IODEF is still under development and supported.

E. CAP

Name: Common Alerting Protocol
URL: http://www.oasis-open.org/committees/emergency/
Issuer: Organization for the Advancement of Structured Information Standards (OASIS)
Last Update: 1 November 2005
Version: 1.1
Classification: General incident management

Summary: The Common Alerting Protocol (CAP) [14] is an XML-based incident standard, for describing all kinds of incidents such as natural disasters and terrorist attacks.

Description: The Common Altering Protocol standard is designed in a very general way and uses the segments *alert*, *info*, *resource*, and *area* to describe warnings, such as natural or man-made disasters. The segment *alert* is used to define the alert in a general way and the segment *info* complements the alert information with a detailed description. The segment *resource* and its sub elements can be used to refer to additional references with supplemental information, such as image or audio files. Geographical location information about the incident is stored in the segment *area*.

Application: OASIS provides a Java API called "caplib" for generating and converting CAP messages, which can be exchanged by RSS or Atom (XML language used for web feeds). There are many organizations, for example the US weather service or the LA fire department, that use CAP for natural and manmade disasters. Another application area of CAP is the nationally and internationally exchange of information about convicts and terrorists.

Strengths: CAP is focused on disasters, therefore we could not identify any strengths relating to IT security advisories.

Weaknesses: This standard was not designed for IT security advisories. It is not possible to specify an affected system or to link software to an operating system. The available segments (*alert* and *info*), which should describe the incident, are too universal for IT security advisory purposes.

Rating:

semantic usability -
Although CAP is XML-based and it provides a well-defined and clear structure, it can not be used for describing vulnerabilities in a way that ensures enough semantics for our purposes. Because the elements are defined very broadly and in a non-IT related way they can be ambiguously interpreted.

information complexity -
The CAP standard covers some general elements defined in our evaluation criteria (author, creation date, severity, patch location (URL) + file size + file hash value). Because CAP was not designed as an IT security advisory standard, very important elements such as affected systems and workaround descriptions are missing.

distribution +
CAP is used by many organizations[8] for exchanging information regarding natural and manmade disasters.

F. OVAL

Name: Open Vulnerability and Assessment Language

[7] AirCERT: http://aircert.sourceforge.net/, last access: 15 April 2008

[8] CAP Distribution: http://www.incident.com/cookbook/index.php, last access: 15 April 2008

URL: http://oval.mitre.org/index.html
Issuer: National Cyber Security Division (NCSD) at the U.S. Department of Homeland Security
Last Update: 10 April 2008
Version: 5.4
Classification: IT incident management

Summary: The Open Vulnerability and Assessment Language (OVAL) is a common standard for expressing public available security content and standardizing the transfer of this content.

Description: OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process, namely, representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language, such as the MITRE OVAL repository[9]. [15]

Application: Besides governmental institutions such as the U.S. Department of Homeland Security and the National Institute of Standards and Technology, several commercial organizations utilize OVAL for security advisory distribution, vulnerability assessment, and patch management. Vulnerability descriptions in the OVAL format exist for various platforms of vendors such as Microsoft, HP, IBM, Novell, Red Hat, Sun, SUSE. For the efficient usage of the OVAL definitions MITRE developed the OVAL Interpreter as a reference implementation. Several third-party vendors provide OVAL compatible products in the area of patch management and vulnerability assessment.

Strengths: OVAL, the international information security community baseline standard supports the detection of vulnerabilities and configuration issues on computer systems. One of OVAL's strengths is its rich and well-defined schema definition. The provided information is sufficient for detailed vulnerability testing on a broad range of platforms and applications. Another major strength of OVAL is the strong support by governmental and commercial organizations. In addition, publicly available repositories of OVAL definitions, created by the OVAL community, are available.

Weaknesses: While the OVAL standard supports the three phases of vulnerability assessment, solution possibilities are not integrated into this standard. Moreover, system descriptions (*AffectedType*) are not standardized and thus render different representations possible. According to the OVAL standard this information can be used by tools to filter messages and thus is critical. Note that Common Platform Enumeration (CPE) [16] integration is planned for future versions.

[9]OVAL repository: http://oval.mitre.org/repository/, last access: 15 April 2008

STANDARD	SEMANTIC USABILITY	INFORMATION COMPLEXITY	DISTRIBUTION
ANML	~	~	-
EISPP	~	~	+
CAIF	~	~	~
IODEF	~	-	+
CAP	-	-	+
OVAL	+	~	+

TABLE II
EVALUATION RESULTS

Rating:

semantic usability **+**
Well-defined and semantically usable element, type, and attribute definitions exist for the OVAL standard.

information complexity **~**
OVAL offers the possibility to describe vulnerabilities on a highly granular level but does not provide information on patch issues such as download locations or required reboots. Furthermore, no predefined product lists have been enforced to guarantee a consistent representation.

distribution **+**
OVAL is supported and used by several governmental and commercial organizations. The wide range of commercial tools shows the wide-spread usage of this standard.

V. CONCLUSION

In the current paper we evaluated several security advisory standards to identify a standard that is, due to its semantic structure, most appropriate for automated message processing. The evaluation has shown that the OVAL standard is the most suitable standard for the automatic or semi-automatic interpretation of security advisories (see Table II). Although the standard lacks some required elements, such as required reboot or patch information, it contains most elements for the purpose of automatic security advisory interpretation. Another major strength of OVAL is the strong support by governmental and commercial organizations and the wide range of available tools.

REFERENCES

[1] BASEL2, "Basel committee on banking supervision (bcbs), basel 2 - international convergence of capital measurement and capital standards - a revised framework," 2001.
[2] R. Bhaskar, "State and local law enforcement is not ready for a cyber katrina," *Commun. ACM*, vol. 49, no. 2, pp. 81–83, 2006.
[3] M. Franz, "Containing the ultimate trojan horse," *IEEE Security and Privacy*, vol. 5, no. 4, pp. 52–56, 2007.
[4] D. Lekkas and D. Spinellis, "Handling and reporting security advisories: A scorecard approach," *IEEE Security and Privacy*, vol. 3, no. 4, pp. 32–41, July/August 2005. [Online]. Available: http://www.spinellis.gr/pubs/jrnl/2005-CS-SecAdvisory/html/LS05.htm

[5] M. Carvalho, T. Cowin, N. Suri, M. Breedy, and K. Ford, "Using mobile agents as roaming security guards to test and improve security of hosts and networks," in *SAC '04: Proceedings of the 2004 ACM symposium on Applied computing*. New York, NY, USA: ACM Press, 2004, pp. 87–93.
[6] CERT/CC, "Cert/cc statistics 1988-2006," http://www.cert.org/stats/, January 2007.
[7] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, "State of the practice of computer security incident response teams (csirts)," Carnegie Mellon Software Engineering Institute, Tech. Rep. CMU/SEI-2003-TR-001, October 2003.
[8] European Network and Information Security Agency (ENISA), "A step-by-step approach on how to set up a csirt," European Network and Information Security Agency (ENISA), Tech. Rep. Deliverable WP2006/5.1(CERT-D1/D2), 2006.
[9] Office of Government Commerce (OGC), *The Official Introduction to the ITIL Service Lifecycle*. Stationery Office, 2007.
[10] ——, "Itil - glossary of terms, definitions and acronyms," May 2006.
[11] N. Elkarra, "Advisory and notification markup language (anml)," http://www.opensec.org/anml/, April 2003.
[12] EISPP Consortium, "Eispp common advisory format description," http://www.eispp.org/commonformat_2_0.pdf, May 2004.
[13] O. Goebel, "Common announcement interchange format (caif) version 1.2," http://www.caif.info/draft-goebel-caif-format.html, November 2005.
[14] Organization for the Advancement of Structured Information Standards (OASIS), "Common alerting protocol, v. 1.1," October 2005.
[15] MITRE, "An introduction to the oval language," http://oval.mitre.org/oval/documents/docs-06/an_introduction_to_the_oval_language.pdf, 2006.
[16] A. Buttner and N. Ziring, "Common platform enumeration (cpe) - specification," The MITRE Corporation and National Security Agency, Tech. Rep., 2007. [Online]. Available: http://cpe.mitre.org/files/cpe-specification_2.0.pdf