18th Annual FIRST Conference
June 25-30, 2006 - Baltimore, Maryland, United States

Proposal of RSS Extension for Security Information Exchange

Masato Terada†, Shingo Takada
Graduate School of Science and Technology, Keio University.
3-14-1 Hiyoshi, Kohoku, Yokohama, Kanagawa 223-8522, Japan

Junji Fukuzawa
Security Center, Information-technology Promotion Agency (IPA), Japan
Bunkyo Green Court, 2-28-8, Hon-Komagome, Bunkyo-ku, Tokyo 113-6591, Japan

and

Norihisa Doi ‡
Graduate School of Science and Engineering, Chuo University.
1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

Abstract

Unauthorized access intended to distribute malware has been widely spread across the Internet and causing a lot of damage worldwide. In order to eliminate vulnerabilities that can be exploited by those malware and prevent unauthorized access, it is necessary to improve the way to distribute security information about computer software and hardware. In this paper, we examines how we can provide a more efficient security information distribution service for the security administrators that helps them reduce their workload related in gathering and grouping information from various sources and take care of vulnerabilities and incidents.

We propose JVNRSS (JP Vendor Status Notes RSS) as a security information sharing and exchanging specification. Currently, JPCERT/CC and IPA (Information-technology Promotion Agency) are promoting a framework to handle vulnerability information in Japan. They offer JVN (JP Vendor Status Notes), a portal site to provide security information about the domestic computer software and hardware manufactured by the vendors participating in the framework. JVNRSS is one of the methods JVN has been using to distribute security information.

JVNRSS is based on RSS 1.0 and uses the "<dc:relation>" field defined in the Dublin Core as a Relational ID to correlate security information issued by various sources. JVNRSS uses the reference URL specified in a security alert, for example, an URL of the Common Vulnerability Exposure, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert and CIAC Bulletin. In this paper, firstly we will explain the specification and applications of JVNRSS. Secondly, we will introduce the result of our feasibility study on JVNRSS and lastly we will propose the RSS Extension for security information sharing through the Internet.

Keywords: Network Security, Vulnerability, Information Sharing, Exchange Specification and RSS

1. Introduction

Recently, malware (Viruses, Worms, Trojan Horses etc.) propagation is widely seen and causing a lot of damage broadly in various ways. Especially since the havoc brought by SQL Slammer in January 2003 and MS-Blaster in August 2003, we should promote the countermeasures that protect not only the server systems but also the client systems. In order to prevent unauthorized access and eliminate the vulnerabilities in the information systems, it is necessary to improve the security information sharing to enable users to take appropriate actions.

In Japan we hadn't had a function like the CERT/CC Vulnerability Notes Database that collected security information. To improve this situation, the JVN (at this point called JPCERT/CC Vender Status Notes Database) [1] was created in February 2003 with the support of the JPCERT/CC. We designed the JVN as a portal site to provide information on vulnerabilities in software products used in Japan. The purpose of the database is to provide the latest information about the vulnerabilities in the domestic software products and help users deal with those vulnerabilities. Although information about vulnerabilities

†) Security Center, IPA (Information-technology Promotion Agency, Japan)
JVN WG member, JPCERT/CC
Hitachi Incident Response Team, Hitachi Ltd.
‡) Graduate School of Science and Technology, Keio University

per se has been already disseminated in the form of the security hole reports put out by many organizations and vendors, the database greatly enhances the usefulness of the information by also including the updates and the status reports on the latest efforts by the product venders to deal with vulnerabilities. The primary purpose of the JVN Database is to collect and disseminate these information.

In July 2004, the Ministry of Economy, Trade and Industry (METI) adopted the "Standard for Handling Software Vulnerability Information" as an official rule, and began promoting the "Information Security Early Warning Partnership" as an implementation framework [2]. The JVN has become the portal site to provide the security information about the domestic computer software and hardware manufactured by the vendors registered in the framework [3]. Launched with the support of the JPCERT/CC on the basis of its successful feasibility study, the JVN has become a joint venture by IPA and JPCERT/CC within the official framework. Subsequently, the name of the organization was changed to "JP Vendor Status Notes," but the original acronym JVN was retained, and the portal site for publishing the status of the vendor's effort dealing with the domestic software vulnerabilities has also been kept as it was.

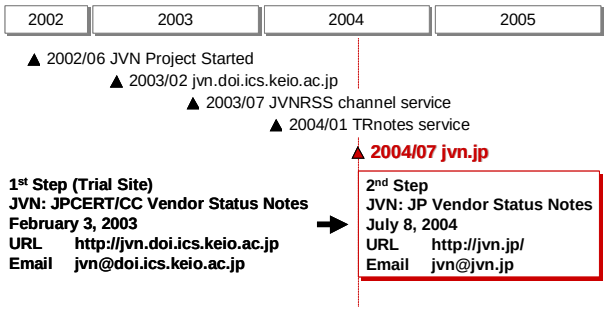


Figure 1: JVN History

JVN provides the "Vendor Status Notes (VN)" and the "Status Tracking Notes (TRnotes)". VN is a service providing information on how to fix vulnerabilities. It is similar to the "CERT Vulnerability Notes" and follows up the IPA/JPCERT Vulnerability reports, US-CERT Alerts, US-CERT Vulnerability Notes and NISCC Advisories. TRnotes is a service providing a list of incident information related to vulnerabilities such as the followings:

- When was the exploit code released to the public?
- What kind of incidents were they?
- What kind of countermeasure was applied to the incidents?

Currently, VN, TRnotes and other security information are distributed in the form of a HTML-based web page. This means that fragmented information from various websites are collected and reassembled, and considerable time and efforts are required to reestablish the connections and relationships among the various bits and pieces of information. In short, it is necessary to improve the method of the security information exchange. From the information provider's point of view, if information could be published in a form more easily processed by a machine, then information could be reused much more flexibly and extensively. We propose "JVNRSS", an RSS based format, as an approach to solve this problem. JVNRSS is based on RSS 1.0 [4] and uses the field <dc:relation> of the Dublin Core as a primary key to group security information. This paper discusses the specification of JVNRSS and its applications. At the end, we will introduce RSS extension for security information exchange.

2. Related Work

2.1 Security Information Sharing

The related researches on the security information sharing are the followings:

CVE [5]
Common Vulnerabilities and Exposures (CVE) is a list of standardized names for vulnerabilities and other information security exposures (ex. CVE-1999-1011). CVE supports relationship among all publicly known vulnerabilities and security exposures. Many tools, Web sites, databases, or services use the CVE name in a way that allows them to cross-link with other repositories that also use the CVE name.

NIST NVD [6]
National Vulnerability Database (NVD) is a comprehensive cyber security vulnerability database and refers to CVE. It provides the search capability and directs users to vulnerability and patch information.

OSVDB [7]
Open Source Vulnerability Database (OSVDB) is a vendor-neutral vulnerability database for the information security community. The goals of the project are to promote a greater and more open collaboration between companies and individuals, eliminate redundant works and reduce expense inherent in the system and product development.

Our approach supports to distribute security information and build a relationship among these vulnerability information.

2.2 Security information exchange specification

The related researches on the security information exchange specification are the followings.

EISPP [8]
European Information Security Promotion Programme (EISPP) is a project co-funded by the European Community. EISPP Common Advisory Format Description enables an easy exchange of advisory data among four CERTs participating in EISPP. EISPP merges best-practice information regarding security advisories issued by those CERTs.

CAIF [9]
Common Announcement Interchange Format (CAIF) is an XML-based format to store and exchange security announcements in a normalized way. It provides a basic but comprehensive set of elements that are designed to describe the main aspects of a security-related issue.

VULDEF [10]
The purpose of the "Vulnerability Data Publication Format (VULDEF)/Security Advisory Publication Format" is to define the data formats for the information related to security advisories typically published by the product vendors and CSIRTs. VULDEF has some elements to describe the vulnerability, affected items and solutions etc.

EISPP, CAIF and VULDEF are the XML formats to describe the details of security information and JVNRSS is an XML format based on RSS to describe the overview of those formatted security information (Figure 2).

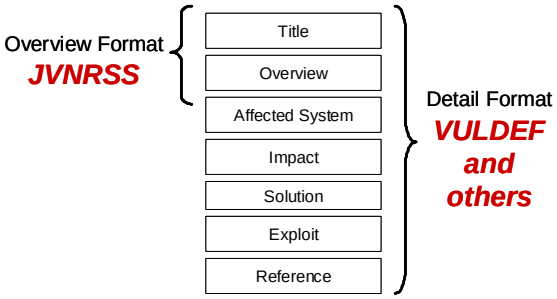


Figure 2: The classification of JVNRSS and Others.

Making use of JVNRSS is an essential point in the security information exchange, for this handily resolves the following two basic issues:

- ***Distribution designed to encourage reuse of information***
  Our primary objective is to aggregate security information from the product vendors and provide it through the JVN website. But in order to reuse published information, it must be offered in a machine-readable format. This is where RSS comes in. By using RSS, JVN data can be distributed in the same way just as the news feeds provided by the news websites. And because the content is described by RSS, it can be easily verified if information has been added to an item or an item has been updated.

- ***More efficient aggregation of information from product vendors***
  JVN aggregates security information from the product vendors received via e-mail notifications. But in order to enlist the participation of as many product vendors as possible, an efficient means of collecting information other than e-mail must be also set up. Use of RSS will enable information to be collected from the product vendor's website and be automatically combined with other security information at the JVN website.

3. Specification of JVNRSS

RSS is an XML-based format that allows the consolidation of the lists of hyperlinks. The original RSS, version 0.90, was developed by Netscape as a format for building the portals of headlines for the major news sites. RSS 1.0 was based on RDF (Resource Description Framework) and designed by the original guiding principles of RSS 0.90.

JVNRSS is based on RSS 1.0 and uses the field <dc:relation> of the Dublin Core as a primary key to group security information (See Table 1) [11]. JVNRSS with the Relational ID in <dc:relation> is shown in Figure 3. RSS contains a list of items, each of which is identified by a link. Each item can have any amount of metadata associated with it. The most basic metadata supported by RSS includes a title for the link and a description of it. Our proposed Relational ID allows the security information from the different websites to correlate with each other.

```
<item rdf:about="URL of security information">
 <title>Title</title>
 <link>URL of security information</link>
 <dscription>Outline of security information</description>
  <dc:publisher>Product vendor name</dc:publisher>
  <dc:creator>Contact point information</dc:creator>
  <dc:identifier>Security information ID</dc:identifier>
  <dc:relation>Relational ID (1) {CVE|CERT-CA|CERT-VU|etc.}</dc:relation>
  <dc:relation>Relational ID (2) {CVE|CERT-CA|CERT-VU|etc.}</dc:relation>
  <dc:relation>        :        :                              </dc:relation>
  <dc:date>Date last updated</dc:date>
  <dcterms:issued>Date first published</cterms:issued>
  <dcterms:modified>Date last updated</dcterms:modified>
</item>
```

Figure 3: The format of the item part of JVNRSS.

JVNRSS uses the reference URL specified in a security alert as Relational ID, for example, an URL of the Common Vulnerability Exposure, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert and CIAC Bulletin. These are the best reference for the Internet security information.

Table 1: The definition of the item part of JVNRSS.

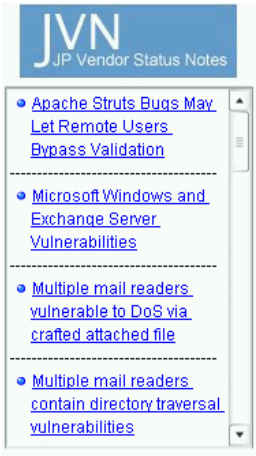
Element	Description
item	***Syntax:*** <item rdf:about="{item_uri}"> ***Requirement:*** >= 1 ***Required Attribute(s):*** rdf:about ***Model:*** (title, link, description?, dc:publisher, dc:identifier?, dc:relation, dc:date, dcterms:issued?, dcterms:modified?) ***Definition:*** A security information headline. {item_uri} must be unique with respect to any other rdf:about attributes in the JVNRSS document and is a URI which identifies the item.
title	***Syntax:*** <title>{item_title}</title> ***Requirement:*** Required ***Model:*** (#PCDATA) ***Definition:*** The item's title for security information.
link	***Syntax:*** <link>{item_link}</link> ***Requirement:*** Required ***Model:*** (#PCDATA) ***Definition:*** The item's URL for security information.
description	***Syntax:*** <description>{item_description}</description> ***Requirement:*** Optional ***Model:*** (#PCDATA) ***Definition:*** A brief description/abstract of the item for security information.
dc:publisher	***Syntax:*** <dc:publisher>{Product vendor name}</dc:publisher> ***Requirement:*** Required ***Model:*** (#PCDATA) ***Definition:*** A product vendor name, an organization name, or a site name for the item for security information.
dc:creator	***Syntax:*** <dc:creator>{Contact point information}</dc:creator> ***Requirement:*** Optional ***Model:*** (#PCDATA) ***Definition:*** An entity primarily responsible for making the content of the resource. Typically, the name of a Creator should be email address for contact.
dc:identifier	***Syntax:*** <dc:identifier>{Security information ID}</dc:identifier> ***Requirement:*** Optional ***Model:*** (#PCDATA) ***Definition:*** A unique identifier assigned by vendor.
dc:relation	***Syntax:*** <dc:relation>{Relational ID}</dc:relation> ***Requirement:*** Required ***Model:*** (#PCDATA) ***Definition:*** A best reference URI (CVE, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert etc.) to a related security information. ***Comment:*** NULL when there is no reference URI.
dc:date	***Syntax:*** <dc:date>{Date last updated}</dc:date> ***Requirement:*** Required ***Model:*** (#PCDATA) [W3CDTF] ***Definition:*** Its value is a date, indicating when the item was last updated. ***Recommendation:*** Complete date plus hours and minutes: YYYY-MM-DDThh:mmTZD (eg 1997-07-16T19:20+01:00)
dcterms:issued	***Syntax:*** <dcterms:issued>{Date first published}</dcterms:issued> ***Requirement:*** Optional ***Model:*** (#PCDATA) [W3CDTF] ***Definition:*** Its value is a date, indicating when the item was first published.
dcterms:modified	***Syntax:*** <dcterms:modified>{Date last updated}</dcterms:modified> ***Requirement:*** Required ***Model:*** (#PCDATA) [W3CDTF] ***Definition:*** Its value is a date, indicating when the item was last updated.

The RSS items with the same Relational ID belong to the same group. For example, two RSS items in Figure 4 refer to the same vulnerability and are related to the US-CERT Technical Alert TA04-111A, "Vulnerability in TCP". This relational concept is based on the "Semantic Web" that defines and links information in a way that can be automatically processed by computers using XML and RDF.

```
<item rdf:about="http://jvn.jp/cert/JVNTA04-111A">
  <title>Potential Reliability Issue in TCP</title>
  <link>http://jvn.jp/cert/JVNTA04-111A</link>
  <description />
  <dc:publisher>JVN</dc:publisher>
  <dc:identifier>JVNTA04-111A</dc:identifier>
  <dc:relation>http://www.us-cert.gov/cas/techalerts/TA04-111A.html</dc:relation>
  <dc:date>2005-04-01T18:00+09:00</dc:date>
  <dcterms:issued>2004-04-21T06:45+09:00</dcterms:issued>
  <dcterms:modified>2005-04-01T18:00+09:00</dcterms:modified>
</item>

<item rdf:about="http://www.hitachi.co.jp/Prod/comp/network/notice/TCP.html">
  <title>GR2000/GR4000/GS4000/GS3000 Vulnerability Issues in TCP</title>
  <link>http://www.hitachi.co.jp/Prod/comp/network/notice/TCP.html</link>
  <description />
  <dc:publisher>Hitachi Ltd.</dc:publisher>
  <dc:identifier />
  <dc:relation>http://www.us-cert.gov/cas/techalerts/TA04-111A.html</dc:relation>
  <dc:relation>http://jvn.jp/cert/JVNTA04-111A</dc:relation>
  <dc:date>2004-04-26</dc:date>
  <dcterms:issued>2004-04-26</dcterms:issued>
  <dcterms:modified>2004-04-26</dcterms:modified>
</item>
```

Figure 4: An example of item part of JVNRSS.



jvnbox

jvnticker

Figure 5: An example of a visualized JVNRSS for VN.

4. Applications of JVNRSS

This chapter describes the applications of JVNRSS.

4.1 Visualized JVNRSS

(1) Visualized JVNRSS
JVN provides not only an HTML-based information and JVNRSS feed of the "Vendor Status Notes (VN)", but also a visualized JVNRSS, which is an information box or ticker for JVNRSS using FLASH [12]. The visualized JVNRSS is shown in Figure 5. The purpose of the visualized JVNRSS feed is to supply the summary of the JVN articles through other websites.

(2) Visualized TRnotes
We should cooperate with other Internet websites to eliminate security incidents and event information sharing is important to accomplish it. The purpose of TRnotes is to share the timeline of the events, which include the discovered date of a vulnerability, a published date of any advisories, a released date of exploit codes and a confirmed date of any worms on the vulnerability. The each web page consists of the overview, impact, the timeline of the events and related information. An example of the HTML-based TRnotes is shown in Figure 6. The characteristics of TRnotes are the followings:

- ***The event time is marked hourly***
  The state is marked hourly, not daily, which is shown in Figure 6. In case of a mailing list, the sent or received time becomes the event time. And in case of a website, the Last-Modified in the header information defined by the HTTP protocol is used as the event time.
- ***The event information is based on public information***
  It is important that the security administrators for any organizations share the same event information to eliminate the incidents on the Internet. The public information has no restriction such as non-disclosure policy and is possible to share information among more security administrators.

TRnotes has the event list organized by the timeline and each event entry of TRnotes is equivalent to the item part of JVNRSS. We can make the formatted and visualized TRnotes by JVNRSS such as Figure 7. The purpose of the visualized TRnotes is to arrange all events by time, which is accomplished by the FLASH tool that sorts the items by <dcterms:issued>.

4.2 Security information gathering system

JVNRSS format is based on RSS 1.0, which is the same RSS format used by the major news sites. Then, once security information is in the JVNRSS format, an RSS-aware program can check the feed for changes and react to the changes in an appropriate way. When security information is machine-readable, many Internet sites can reduce the cost of information gathering and grouping. Our gathering and grouping approach using the JVNRSS format has three steps, which are shown in Figure 8.

(1) Gathering of the security information
The gathering module periodically checks changes in JVNRSS feeds on other Web sites and extracts the JVNRSS items upon change.
(2) Grouping of the security information
The grouping module extracts the Relational ID from the JVNRSS feed <item>. This module checks other JVNRSS feed items using Relational ID as the search key.

Figure 6: An example of HTML based TRnotes.

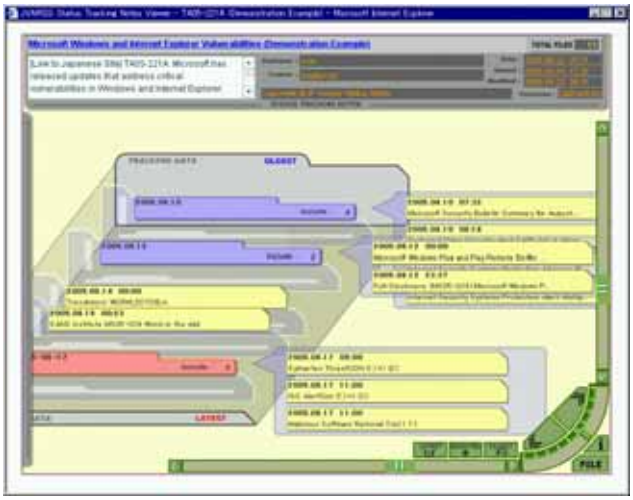


Figure 7: Visualized TRnotes with JVNRSS format.

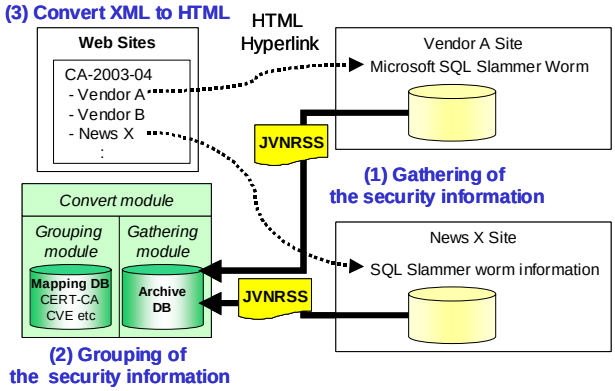


Figure 8: Overview of the gathering and grouping approach by JVNRSS.

When the module finds <item> with the same Relational ID, it makes these <items> into a group (Figure 12). When this module does not find any item with the same Relational ID, it will try to find a matching Relational ID using the Mapping DB (Figure 13). The Mapping DB of the Relational IDs is shown in Figure 9. The upper group in the mapping DB shows the vulnerability information related to the TCP stack and the lower group shows the incident information about the MS-Blaster worm. The items on the right, which refer to the same vulnerability or incident, belong to the same group. In case the feed <items> have a different Relational ID yet refer to the same vulnerability, the mapping DB traces the relationship between those Relational IDs.

(3) Convert XML to HTML

The Convert module transforms XML documents into a HTML form to present security information.

4.3 CVE mapping of the security information

CVE is a list of standardized names for vulnerabilities and other information security exposures. Currently CVE mostly doesn't include security information published by Japanese vendors, because Japanese vendors don't post security information in a CVE-compatible format. The purpose of grouping security information is to make a relationship map between CVE and Japanese security information. Our approach to CVE mapping is the same as the above section. The grouping module extracts the Relational ID of JVNRSS feed <item> and finds the CVE entry with the same Relational ID. In addition, the visualized CVE, which is a folder box using FLASH, is shown in Figure 10. The visualized CVE uses the extended JVNRSS format to describe the grouping of security information (Figure 11 and Table 2).

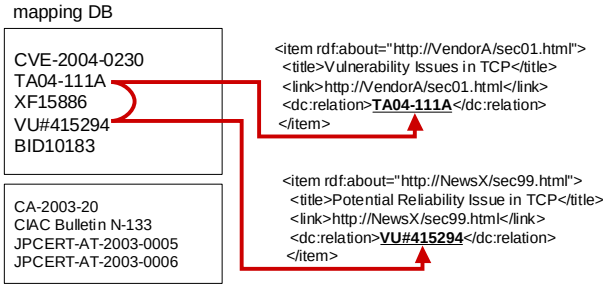


Figure 9: Relational ID and Mapping DB.

Figure 10: Visualized CVE with the security information of Japanese Vendors.

```
<item rdf:about="http://www.us-cert.gov/cas/techalerts/TA04-111A.html">
  <title>Vulnerabilities in TCP</title>
  <link>http://www.us-cert.gov/cas/techalerts/TA04-111A.html</link>
  <description>Most implementations of the BGP ...</description>
  <dc:publisher>US-CERT</dc:publisher>
  <dc:identifier>TA04-111A</dc:identifier>
  <dc:date>2005-09-09</dc:date>
  <sec:item>
   <item rdf:about="http://jvn.jp/cert/JVNTA04-111A">
    <title>Potential Reliability Issue in TCP</title>
    <link> http://jvn.jp/cert/JVNTA04-111A</link>
    <dc:publisher>JVN</dc:publisher>
    <dc:identifier>JVNTA04-111A</dc:identifier>
    <dc:relation>http://www.us-cert.gov/cas/techalerts/TA04-111A.html</dc:relation>
    <dc:date>2005-04-21T18:00+09:00</dc:date>
    <sec:item>
     <item rdf:about="http://www.hitachi.co.jp/Prod/comp/network/notice/TCP.html">
      <title>GR2000/GR4000/GS4000/GS3000 Vulnerability Issues in TCP</title>
      <link>http://www.hitachi.co.jp/Prod/comp/network/notice/TCP.html </link>
      <dc:publisher>Hitachi</dc:publisher>
      <dc:identifier />
      <dc:relation>http://jvn.jp/cert/JVNTA04-111A</dc:relation>
      <dc:date>2004-04-22</dc:date>
     </item>
    </sec:item>
   </item>
  </sec:item>
</item>
```

Figure 11: The format of item part of Extended JVNRSS for visualized CVE.

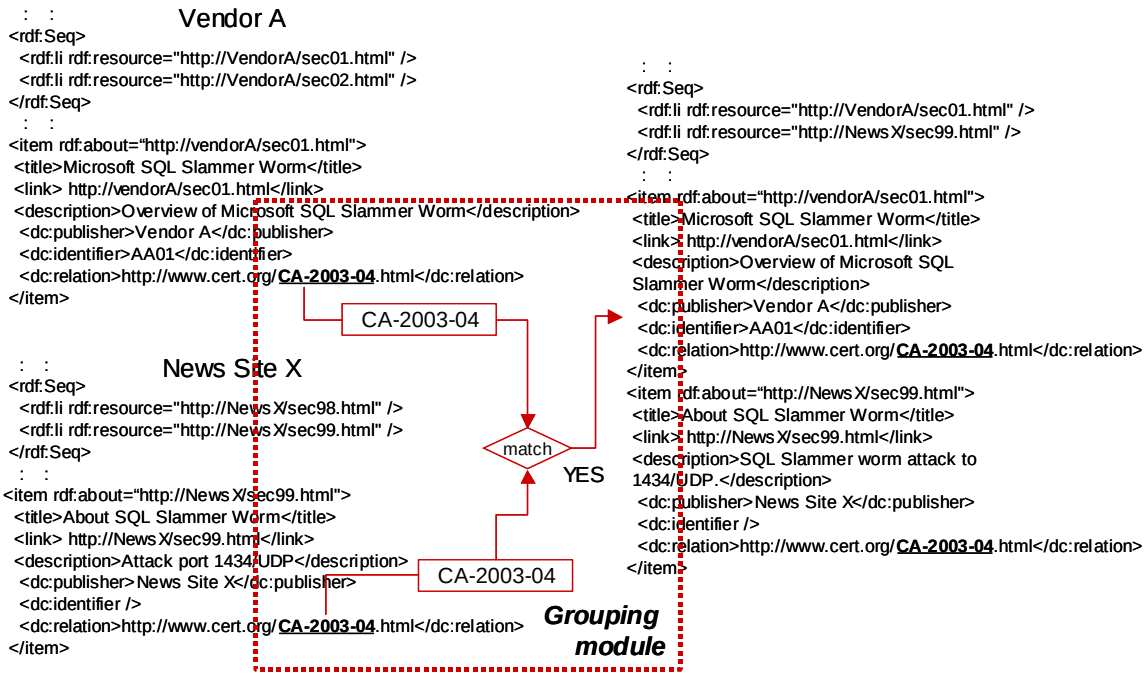


Figure 12: The grouping mechanism using Relational ID without mapping DB.

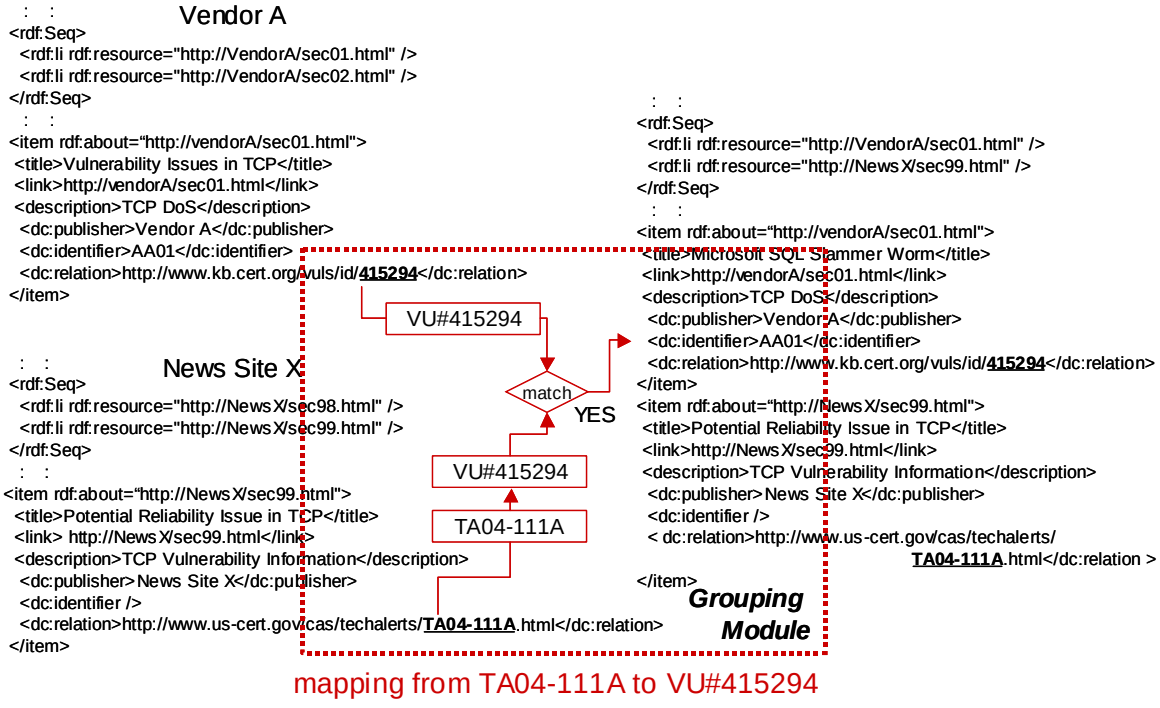


Figure 13: The grouping mechanism using Relational ID with mapping DB.

5. JVNRSS practical activity

In May 2006, a website for the feasibility study on JVNRSS's practical activities was launched [13]. This chapter introduces JVNRSS activities.

- CVE+
  http://jvnrss.ise.chuo-u.ac.jp/jtg/cve+/
  CVE+ is to make a relationship map between CVE and Japanese security information. Some modules in Figure 14 have been implemented as a Proof of Concept prototype. Also the convert module produces a TouchGraph XML format to describe the relationship map [14].
- TRnotes
  http://jvnrss.ise.chuo-u.ac.jp/jtg/trn/
  TRnotes will provide not only the HTML-based information but also the JVNRSS format and the Visualized TRnotes. Currently, some information is available at the above website.
- XSL_swf
  http://jvnrss.ise.chuo-u.ac.jp/jtg/xswf/
  XSL_swf is a FLASH tool for the visualized JVNRSS and uses part of XSL as a mechanism to describe how a document should be displayed. For example, if an item entry of RSS or JVNRSS doesn't have a severity level, XSL_swf displays a document with the severity level defined in the XSL file. Currently, our XSL_swf implementation refers to RSS including XSL, and parses an XSL file to display the severity level such as red (LEVEL1), yellow (LEVEL2) and blue (LEVEL3) when the XSL file includes the following entries (Figure 15).

```
<xsl:when test="rss:link='"http://xxx"'>LEVEL1</xsl:when>
<xsl:when test="rss:link='http://yyy"'>LEVEL2</xsl:when>
<xsl:when test="rss:link='http://zzz"'>LEVEL3</xsl:when>
```

- RSS_dir
  http://jvnrss.ise.chuo-u.ac.jp/jtg/rssd/
  RSS_dir is a concept of the RSS directory for the RSS channel. The RSS directory describes a RSS channel tree with the RSS format. Some visualized tools have been implemented as a Proof of Concept prototype such as one shown in Figure 16.

Table 2: The definition of item part of Extended JVNRSS for visualized CVE

Element	Description
sec:item	***Syntax:*** <sec:item> ***Requirement:*** Optional ***Model:*** (item*) ***Definition:*** Nest of item set in JVNRSS.

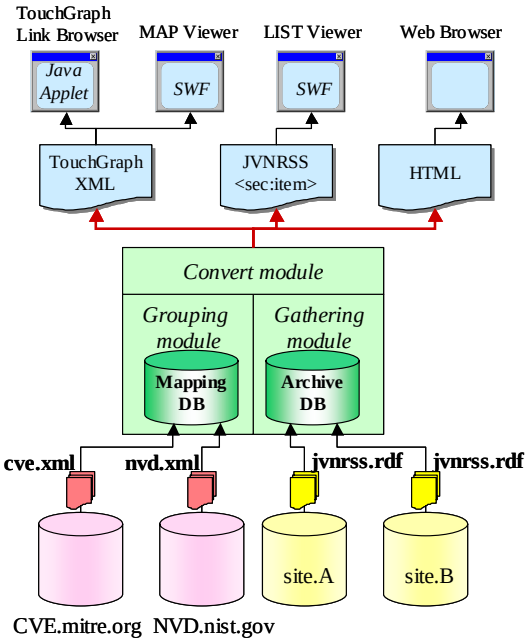


Figure 14: System overview of CVE+.

Figure 15: Example of XSL_swf

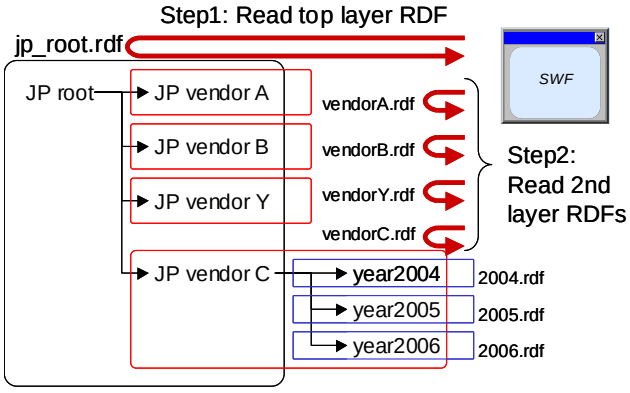


Figure 16: RSS directory for RSS channel.

6. Proposal RSS Extension

JVNRSS is based on RSS 1.0 and a proprietary format in Japan. Right now, in other words, the ability to use RSS holds the key to successfully implement a scheme for distributing security related information. This section describes the RSS Extension's definition of the tags for RSS 1.0, RSS 2.0 and Atom [15].

Here is the list of the proposed elements. Examples with the proposed elements are shown in Figure 18 and Figure 17.

```
<?xml version="1.0" encoding="utf-8"?>
<rss version="2.0"
   xmlns:sec="http://jvn.jp/rss/mod_sec/"
>

<channel>
   <title>JVNRSS Feed</title>
   <link>http://jvn.jp/jp/</link>
   <description>JP Vendor Status Notes - JP</description>
   <pubDate>Sun, 01 May 2005 08:00:00 +0900</pubDate>
<lastBuildDate>Sat, 18 Jun 2005 08:23:00 +0900</lastBuildDate>

 <item>
   <title>JVN Qualified Security Advisory #12345678</title>
   <link>http://jvn.jp/jp/JVN%2312345678</link>
   <description>This example is description about Qualified
              Security Advisory Reference #12345678</description>
   <author>JVN</author>
   <pubDate>Sat, 18 Jun 2005 08:23:00 +0900</pubDate>
   <sec:identifier>JVN#12345678</sec:identifier>
   <sec:references sec:source="JPCERT"
      sec:id="JPCERT-AT-2005-0522">
      http://www.jpcert.or.jp/at/2005/at050522.txt
   </sec:references>
 </item>

 <item>
   <title>JVN's Qualified Security Advisory #00ABCDEF</title>
   <link>http://jvn.jp/jp/JVN%2300ABCDEF</link>
   <description>This example is description about Qualified
            Security Advisory Reference #00ABCDEF</description>
   <author>JVN</author>
   <pubDate>Tue, 31 May 2005 22:22:00 +0900</pubDate>
   <sec:identifier>JVN#00ABCDEF</sec:identifier>
   <sec:references sec:source="JPCERT"
      sec:id="JPCERT-AT-2005-0501">
      http://www.jpcert.or.jp/at/2005/at050501.txt
   </sec:references>
 </item>

 </channel>
</rss>
```

Figure 17: An example of RSS 2.0 with Extension.

```
<?xml version="1.0" encoding="utf-8"?>
<rdf:RDF
   xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
   xmlns="http://purl.org/rss/1.0/"
   xmlns:dc="http://purl.org/dc/elements/1.1/"
   xmlns:dcterms="http://purl.org/dc/terms/"
   xmlns:sec="http://jvn.jp/rss/mod_sec/"
>

<channel rdf:about="http://jvn.jp/rss/jvnJPRSS.rdf">
   <title>JVNRSS Feed</title>
   <link>http://jvn.jp/jp/</link>
   <description>JP Vendor Status Notes - JP</description>
   <dc:publisher>JVN</dc:publisher>
   <dc:creator>jvn@jvn.jp</dc:creator>
   <dcterms:issued>2005-05-01T08:00+09:00</dcterms:issued>
<dcterms:modified>2005-06-18T08:23+09:00</dcterms:modified>
   <items>
     <rdf:Seq>
       <rdf:li rdf:resource="http://jvn.jp/jp/JVN%2312345678" />
       <rdf:li rdf:resource="http://jvn.jp/jp/JVN%2300ABCDEF" />
     </rdf:Seq>
   </items>
 </channel>

<item rdf:about="http://jvn.jp/jp/JVN%2312345678">
   <title>JVN Qualified Security Advisory #12345678</title>
   <link>http://jvn.jp/jp/JVN%2312345678</link>
   <description>This example is description about Qualified
              Security advisory Reference #12345678</description>
   <dc:publisher>JVN</dc:publisher>
   <dc:creator>jvn@jvn.jp</dc:creator>
   <dcterms:issued>2005-05-22T14:00+09:00</dcterms:issued>
<dcterms:modified>2005-06-18T08:23+09:00</dcterms:modified>
   <sec:identifier>JVN#12345678</sec:identifier>
   <sec:references sec:source="JPCERT"
      sec:id="JPCERT-AT-2005-0522">
      http://www.jpcert.or.jp/at/2005/at050522.txt
   </sec:references>
 </item>

<item rdf:about="http://jvn.jp/jp/JVN%2300ABCDEF">
   <title>JVN Qualified Security Advisory #00ABCDEF</title>
   <link>http://jvn.jp/jp/JVN%2300ABCDEF</link>
   <description>This example is description about Qualified
            Security Advisory Reference #00ABCDEF</description>
   <dc:publisher>JVN</dc:publisher>
   <dc:creator>jvn@jvn.jp</dc:creator>
   <dcterms:issued>2005-05-01T08:00+09:00</dcterms:issued>
<dcterms:modified>2005-05-31T22:22+09:00</dcterms:modified>
   <sec:identifier>JVN#00ABCDEF</sec:identifier>
   <sec:references sec:source="JPCERT"
      sec:id="JPCERT-AT-2005-0501">
      http://www.jpcert.or.jp/at/2005/at050501.txt
   </sec:references>
 </item>

</rdf:RDF>
```

Figure 18: An example of RSS 1.0 with Extension.

(1) sec:references

sec:references is an element for the best reference (CVE, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert etc.) to the related security information.

Syntax:

```
<sec:references
  sec:source="%name"
  sec:id="%id">
  %ResourceReference
</sec:references>
```

%name

This attribute specifies an abbreviated name, which provides the best reference, such as CVE, JPCERT, CERT, CIAC, BID, CERT-VN, MS, OSVDB, XF etc.

%id

This attribute specifies the unique identifier assigned by sec:source, such as VU#105259, MS01-044, CVE-2001-0525, CA-2001-14, TA05-111A etc.

%ResourceReference

This attribute specifies a URI of the reference to the resource.

(2) sec:identifier

sec:identifier is an element for the unique identifier assigned by the vendor.

Syntax:

```
</sec:identifier>%id</sec:identifier>
```

%id

This attribute specifies the unique identifier assigned by the vendor, such as "Cisco Security Advisory ID#50960", HPSBMA01234 etc.

7. Conclusion

We propose "JVNRSS" to improve the security information exchange for security administrators. JVNRSS is based on RSS 1.0 and uses the field <dc:relation> of the Dublin Core as a primary key to group security information. This paper has discussed the specification of JVNRSS and its applications, especially the gathering and grouping approach to the security information exchange. Furthermore, we introduced the RSS extension for security information exchange. The security administrators must engage in information gathering to eliminate the threats, and we believe our approach greatly supports this task.

Some visualization tools have been implemented as a Proof of Concept prototype. For the future work, we will implement the JVNRSS gathering, grouping and convert modules. In addition, we will clarify how we can establish a relationship between RSS extension and the existing information sharing mechanisms such as CVE, NIST NVD and OSVDB.

Acknowledgements

Part of this work was supported by "The Special Coordination Funds for Promoting Science and Technology" by the Ministry of Education, Culture, Sports, Science and Technology (MEXT), Japan. The authors are grateful to Hiroshi Takasaki and Hiroko Okashita for their assistance, and to their colleagues in the IPA and JPCERT/CC for their insightful comments.

References

[1] JPCERT/CC Vendor Status Notes,
http://jvn.doi.ics.keio.ac.jp/
[2] Information Security Early Warning Partnership,
http://www.ipa.go.jp/english/security/third.html
[3] JP Vendor Status Notes,
http://jvn.jp/
[4] RDF Site Summary (RSS),
http://web.resource.org/rss/1.0/
[5] Common Vulnerabilities and Exposures,
http://cve.mitre.org/
[6] National Vulnerability Database,
http://nvd.nist.gov/
[7] Open Source Vulnerability Database,
http://www.osvdb.org/
[8] European Information Security Promotion Programme,
http://www.eispp.org/
[9] Common Announcement Interchange Format,
http://cert.uni-stuttgart.de/projects/caif/
[10] VULDEF: Security Advisory Publication Format,
http://jvnrss.ise.chuo-u.ac.jp/jtg/vuldef/
[11] JVNRSS - JP Vendor Status Notes RDF Site Summary
http://jvnrss.ise.chuo-u.ac.jp/jtg/jvnrss/
[12] About JVNRSS,
http://jvn.jp/rss/jvnrss.html
[13] JVNRSS feasibility site,
http://jvnrss.ise.chuo-u.ac.jp/jtg/
[14] TouchGraph Link Browser
http://touchgraph.sourceforge.net/index.html#TGLB
[15] Qualified Security Advisory Reference (mod_sec)
http://jvnrss.ise.chuo-u.ac.jp/jtg/mod_sec/