Proposal of RSS Extension for Security Information Exchange

18th Annual FIRST Conference
2006/06/30

Masato Terada
m-terada@ipa.go.jp
http://jvn.jp/
Prologue

My contribution to JVN

2004 - current
Visitor Researcher
IPA

2002 - current
HIRT Staff
Hitachi

2004 - current
Visitor Researcher
Chuo University

2003 - current
Associate staff
JPCERT/CC

April 2002 - March 2006
Graduate student
Keio University

http://jvn.jp/
We propose JVNRSS (JP Vendor Status Notes RSS) as a security information sharing and exchanging specification. 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 and CIAC Bulletin.

In this presentation, firstly we'll explain the specification and applications of JVNRSS. Secondly, we'll introduce the result of our feasibility study on JVNRSS and lastly we'll propose the RSS Extension for security information sharing.
Contents

1. Vulnerability Information Handling Framework in Japan
2. JVN: JP Vendor Status Notes

I skip section 1 and 2.
Please refer to conference CD-ROM.
Proposal of RSS Extension for Security Information Exchange

http://jvn.jp/
How we can provide a more efficient PUBLIC security information distribution service for the security administrators that helps them reduce their workload related to collecting and grouping various PUBLIC information and take care of security incidents.

Distribution designed to encourage reusing of PUBLIC security information
More efficient aggregation of PUBLIC security information from product vendors
3. JVN RSS (JP Vendor Status Notes RSS)

- Keywords for the solution
  - Semantic Web
  - RSS (RDF Site Summary)

Format for the overview

**JVN RSS**

- Title
- Overview
- Affected System
- Impact
- Solution
- Exploit
- Reference

Format for the details

**VULDEF and others**

Using JVN RSS, an XML format to describe the overview, is an essential point in the security information exchange.
JVNRSS Specification

- **JVNRSS**

Please refer to JVNRSS spec [http://jvnrss.ise.chuo-u.ac.jp/jtg/jvnrss/](http://jvnrss.ise.chuo-u.ac.jp/jtg/jvnrss/)

```xml
<item rdf:about="URL of security information">
  <title>Title</title>
  <link>URL of security information</link>
  <description>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:date>Date last updated</dc:date>
  <dcterms:issued>Date first published</dcterms:issued>
  <dcterms:modified>Date last updated</dcterms:modified>
</item>
```
ID: JVNVU#834865

Title: Sendmail contains a race condition

- Reference: http://www.us-cert.gov/cas/techalerts/TA06-081A.html
- Reference: http://www.kb.cert.org/vuls/id/834865
- Reference: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-0058
3. JVN RSS: Proposal grouping (correlation) mechanism

- The grouping mechanism using Relational ID without mapping DB.

(1) Gathering of the security information

(2) Grouping of the security information.

(3) Convert XML to HTML

Vendor A Site

<item rdf:about="http://A.JP/alert-sql.html">Microsoft SQL Slammer Worm</item>

News X Site

<item rdf:about="http://X.JP/news-sql.html">SQL Slammer worm information</item>

Grouping Completed

match

CA-2003-04
3. JVN RSS: Proposal grouping (correlation) mechanism

- The grouping mechanism using Relational ID with mapping DB.

(3) Convert XML to HTML

<table>
<thead>
<tr>
<th>JVN Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-2003-04</td>
</tr>
<tr>
<td>- Vendor A</td>
</tr>
<tr>
<td>- Vendor B</td>
</tr>
<tr>
<td>- News X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Convert module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping module</td>
</tr>
<tr>
<td>Gathering module</td>
</tr>
</tbody>
</table>

(2) Grouping of the security information.

| Mapping DB |
| CERT-CA |
| CVE etc |

| Archive DB |

(1) Gathering of the security information.

<table>
<thead>
<tr>
<th>News X Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;a href=&quot;http://X.JP/news-sql.html&quot;&gt;SQL Slammer worm information&lt;/a&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vendor A Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;a href=&quot;http://A.JP/alert-sql.html&quot;&gt;Microsoft SQL Slammer Worm&lt;/a&gt;</td>
</tr>
</tbody>
</table>

‡ The grouping mechanism using Relational ID with mapping DB.
The grouping mechanism using Relational ID with mapping DB.

(1) Gather module
(2) Grouping module
(3) Convert module

Mapping DB entry

- CVE-2004-0230
- TA04-111A
- XF15886
- VU#415294
- BID10183

- CA-2003-20
- CIAC Bulletin N-133
- JPCERT-AT-2003-0005
- JPCERT-AT-2003-0006
3. JVN RSS: Proposal grouping (correlation) mechanism

- The grouping mechanism using Relational ID with mapping DB

(1) Gathering of the security information

(2) Grouping of the security information.

(3) Converting module

Vendor A Site

- Microsoft SQL Slammer Worm

News X Site

- SQL Slammer worm information

Grouping Completed
3. JVNRSST practical activity

- **CVE+**
  
  http://jvnrss.isc.chuo-u.ac.jp/jtg/cve+
  
  CVE+ is to make a relationship map between CVE and Japanese security information.

- **TRnotes**
  
  http://jvnrss.isc.chuo-u.ac.jp/jtg/trn/
  
  TRnotes provides HTML based information, JVNRSST format and Visualized TRnotes.

- **XSL_swf**
  
  http://jvnrss.isc.chuo-u.ac.jp/jtg/xswf/
  
  XSL_swf is FLASH tool for visualized JVNRSST and uses a part of XSL as a mechanism to describe how the document should be displayed.

- **RSS_dir**
  
  http://jvnrss.isc.chuo-u.ac.jp/jtg/rssd/
  
  RSS_dir is concept of RSS directory for RSS channel. RSS directory describes a RSS channel tree with RSS format.

- **SIG_rdf**
  
  http://jvnrss.isc.chuo-u.ac.jp/jtg/xsig/
Prototype system

- **Modules:** gathering, grouping and convert
**Viewer:** TouchGraph Link Browser (Java Applet)

- **Data Format:** TouchGraph XML format

```xml
<EDGESET>
  <EDGE fromID="CVE_2004-0230" toID="CERT_TA04-111A" />
</EDGESET>

<NodeSet>
  <NODE nodeID="CVE_2004-0230">
    <NODE_LABEL label="CVE CVE-2004-0230" />
  </NODE>
  <NODE nodeID="CERT_TA04-111A">
    <NODE_LABEL label="US-CERT TA04-111A" />
  </NODE>
</NodeSet>
```
3. **JVNRSS practical activity**

- **Viewer:** LIST Viewer (SWF)
  - **Data Format:** JVNRS + <sec:item> format

```xml
/item rdf:about="http://www.us-cert.gov/cas/..."/
<title>TA04-111A</title>
<sec:item>
  /item rdf:about="http://jvn.jp/cert/JVNTA04-111A"
  /title>Potential Reliability Issue in TCP</title>
</item>
/item rdf:about="http://www.hitachi.co.jp/..."
<title>GR2000/GR4000/GS4000/GS3000 ...</title>
</item>
</sec:item>
</item>
```
3. JVN RSS practical activity

- Archive DB data source
  - in Japanese (lang=ja)
    - http://jvn.doi.ics.keio.ac.jp/rss/jvnCIACRSS.rdf
    - http://www.turbolinux.co.jp/security/index.rdf
  - in English (lang=en)

I want to more data sources.
&
Let's make a mechanism for PUBLIC security information exchange.

Please refer to CVE+
http://jvnrsse.is.ise.chuo-u.ac.jp/jtg/cve+/
“Status Tracking Notes (TRnotes)” includes a list of event/time information on incidents concerning vulnerabilities.

- Each web page consists of the overview, timeline concerning a vulnerability and related information.
- The purpose of TRnotes is in sharing the timeline of the incident, which includes worm activities, the date exploit codes were released and the countermeasure against security incidents. The information is based on public information.

<table>
<thead>
<tr>
<th>TRxxxxxx</th>
<th>Event Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td></td>
</tr>
</tbody>
</table>

Event Information includes followings.

- Date the vulnerability was discovered
- Date any advisories are released
- Date exploit codes are published
- Date worms are produced
- Published alerts from governments.
- Additional resources, such as a government agency etc.
example of vendor status notes (TRnotes)

Microsoft sent the Japanese Security information of Sep. 2004 by Email.

ISSKK announces an alert “Microsoft GDI+ JPEG Processing Exploitation”.

<table>
<thead>
<tr>
<th>Time (JST)</th>
<th>Event Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#Post-Date: Tue, 14 Sep 2004 13:22:15 -0700</td>
</tr>
<tr>
<td>2004-09-17 04:58</td>
<td>US-CERT TA04-260A</td>
</tr>
<tr>
<td></td>
<td>#Post-Date: Thu, 16 Sep 2004 15:56:16 -0400</td>
</tr>
<tr>
<td>2004-09-23 03:38</td>
<td>Full-Disclosure <em>Microsoft Windows MS04-028 JPEG Overflow Shellcoded Exploit</em></td>
</tr>
<tr>
<td></td>
<td>#Cid: ms04-28-cmd.c</td>
</tr>
<tr>
<td></td>
<td>#Tested: Windows XP + SP1</td>
</tr>
<tr>
<td></td>
<td>#Post-Date: Wed, 22 Sep 2004 11:38:18 -0700 (PDT)</td>
</tr>
<tr>
<td>2004-09-23 15:22</td>
<td>Bugtraq <em>NEW GDI+ JPEG Remote Exploit</em></td>
</tr>
<tr>
<td></td>
<td>#Cid: JpegOfDeath.c</td>
</tr>
<tr>
<td></td>
<td>#Tested: Windows XP + SP1</td>
</tr>
<tr>
<td></td>
<td>#Post-Date: 23 Sep 2004 06:22:54 -0000</td>
</tr>
<tr>
<td>2004-09-23 23:55</td>
<td>ISS AlertCon 1 =&gt; 2</td>
</tr>
<tr>
<td></td>
<td>#Last-Modified: Fri, 24 Sep 2004 04:49:46 GMT</td>
</tr>
</tbody>
</table>
3. JVNRSST practical activity

- Visualized TRnotes: Arrange all events by time.

Currently, almost operations are manual based. I want to more automatic mechanism.

Please refer to TRnotes
http://jvnrss.isese.chuo-u.ac.jp/jtg/trn/
RSS_dir is a concept of the RSS directory for the RSS channel. RSS directory describes a RSS channel tree using the RSS format.

- Check the feed for changes and react to the changes in an appropriate way
3. **JVNRRSS practical activity**

- Use **RSS_dir** to selectively display the information collected/updated in the last 7 days.

**Step 1: Read top layer RDF**

- **jp_root.rdf**
  - JP root
  - JP vendor A
  - JP vendor B

**Step 2: Read 2nd layer RDFs**

- vendorA.rdf
- vendorB.rdf

*Updated in the last 7 days*
3. JVN RSS practical activity

Use RSS_dir to selectively display the information collected/updated in the last 7 days.

Let's make more machine readable environment for PUBLIC security information exchange to reduce workloads.

Please refer to RSS_dir
http://jvnrss.isc.chuo-u.ac.jp/jtg/rsssd/
JVNRSS is based RSS 1.0 and a proprietary format in Japan.

- Exchange security information in worldwide.

- The ability to use RSS holds the key to successfully implement a scheme for distributing security related information.

  - Qualified Security Advisory Reference (mod_sec)
  - RSS Extension definition of the tags for RSS 1.0, RSS 2.0 and Atom

Let's make a mechanism for PUBLIC security information exchange in worldwide.
sec:references is an element for a best reference (CVE, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert etc.) to related security information.

Syntax

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

- **%name**
  An attribute is abbreviation name, which provides the best reference, such as CVE, JPCERT, CERT, CIAC, BID, CERT-VN, MS, OSVDB, XF etc.

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

- **%ResourceReference**
  An entity value is a URI reference to a resource.
sec:identifier is an element for the unique identifier assigned by vendor.

Syntax

«sec:identifier>%id</sec:identifier>»

%id

An attribute is the unique identifier assigned by vendor, such as "Cisco Security Advisory ID#50960", HPSBMA01234 etc.
MOD_SEC: Example
Atom + <sec:identifier> and <sec:references>

- **ID:** JVNTA06-109A
- **Title:** Oracle Products Contain Multiple Vulnerabilities
  - **Reference:** http://www.us-cert.gov/cas/techalerts/TA06-109A.html

      <entry>
      <title>Oracle Products Contain Multiple Vulnerabilities</title>
      <link rel="alternate" type="text/html" href="http://jvn.jp/cert/JVNTA06-109A/"/>
      <id>http://jvn.jp/cert/JVNTA06-109A/</id>
      <summary type="text">Oracle products and components are affected by multiple vulnerabilities. </summary>
      <published>2006-04-20T11:30+09:00</published>
      <updated>2006-04-21T15:00+09:00</updated>
      <author>
      <name>JVN</name>
      <email>jvn@jvn.jp</email>
      <uri>http://jvn.jp/</uri>
      </author>
      <sec:identifier>JVNTA06-109A</sec:identifier>
      <sec:references sec:source="CERT" sec:id="TA06-109A">
        http://www.us-cert.gov/cas/techalerts/TA06-109A.html
      </sec:references>
    </entry>
Please access my feasibility study site and send your comments (typo, discussions and questions etc.) to me.

http://jvnrss.isc.chuo-u.ac.jp/
E-mail: jvn@jvn.jp or terada@sdn.hitachi.co.jp
Reference

- IPA (Information-technology Promotion Agency, Japan)

- JPCERT/CC
  - http://www.jpcert.or.jp/english/

- JVN (JP Vendor Status Notes)
  - http://jvn.jp/ (Japanese)

- JVN RSS (JP Vendor Status Notes RSS) Feasibility Study Site
  - http://jvnrss.ise.chuo-u.ac.jp/jtg/
We propose "JVNRSSE" to solve the problems and improve the security information exchange for security administrators. JVNRSSE is based on RSS 1.0 and use the field <dc:relation> of Dubline Core as index of grouping security information. This presentation has discussed the specification of JVNRSSE and the application, especially the gathering and grouping approach for the security information exchange. Furthermore, we introduce RSS extension of security information exchange.
Epilogue

My project summary

Project Name: Talking with all participants.
Period: Jun 25, 2006 - Jun 30, 2006 (6 days)

Name: Sticker

Threat Metrics

Wild: Low
Damage: Low
Distribution: High
Distribution Speed of Sticker: 40 persons/day

17th FIRST
328 persons (46.3%)

18th FIRST
343 persons (70.6%)

18.1% 25.7% 32.7% 47.5% 65.3%
Thank you

Proposal of RSS Extension for Security Information Exchange

2006/06/30

Masato Terada
office@jpcert.or.jp
http://jvn.jp/

IPA (Information-technology Promotion Agency, Japan)
JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)