Designing and Developing an Application for Incident Response Teams

Kees Leune and Sebastiaan Tesink

Tilburg University, The Netherlands

FIRST 2006, Baltimore, MD, USA
Overview

• The Problem
• Objectives
• The solution: AIRT
• Related work
• Recent improvements
• Summary
Context

• Tilburg University CSIRT established in March, 2004
  – 2,000 managed nodes on-campus
  – 3,000 nodes in student houses using cable-modems
  – 2,000 nodes in student houses using direct glass-fiber connections
  – Campus-wide wireless access for all faculty, staff and students.

• Cable modems were causing 95% of incidents; exposed directly to the Internet in our main IP range (not a good plan)
Problem analysis

• Seven incident responders, all part-time.

• Consequence:
  – Tracking problem
    *Which incidents are being handled, and how?*
  
  – Coordination problem
    *Who does what?*
Starting development

- Need for a tool to support day-to-day operations.

- Regular email ticketing systems (Top Desk and Request Tracker) did not provide much improvement.

- Specialized incident response tool: RTIR was too much RT and not enough IR.

- Need to tap in many existing databases to find information (MAC address registrations, LDAP, other internal databases).
Development Objectives

- Ability to record incidents and take initial actions in less than 30 seconds (average) after an incident handler becomes aware of the report.

- Email that is generated and sent automatically should be received and processed automatically as much as possible.

- Application should be web-based and available under an Open license.

- Application must be able to interact with existing data sources, tools and programs.
Importance of incoming email

PREPARE

Detect → Triage → Respond

Estimated 95% or more comes in the form of Email

PROTECT

Carnegie Mellon's Incident Management Process
Email vs. Information

Automated reporting originating from known sources, containing data in known formats

85%-95%

Unknown sources and/or unknown formats

The actual message is **NOT** all that important-- it is the information contained in the message in which we are interested
AIRT Features

- Comprehensive incident management console,
- Outgoing mail using mail templates, including support for PGP signed mail and automatic actions,
- Import queue to automatically process data from known (and trusted) sources. AIRT ships with support for MyNetwatchman, Spamcop, IDMEF, etc.
- Export queue to (securely) run commands on the host operating system,
- Maintains original incident identifiers,
- Extensive search abilities (by IP address, hostname, incident number, network range),
- Detects “repeat offenders”,
- Open and extensible.
AIRT Basics

Incident data:

- Basic incident data: *incident type, and incident status, and incident state, and logging.*

- A number of *IP addresses*, which belong to a *network*, which is managed by a *constituency*, which has *constituency contacts*. Each IP address plays a certain *role in the incident*.

- A number of *users*. 
Incident Overview

- The incident overview provides a comprehensive overview of the current state of the constituency.
- Features:
  - Display of incident ID, Constituency, host name, Status, State, Type, Date (including ordering)
  - Filtering by status/state/type
  - Mass creation of incidents
  - Mass update of incidents
  - Mass processing of outgoing email (template-based)
## Screenshot incident overview

### Incident overview

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Constituency</th>
<th>Hostname</th>
<th>Status</th>
<th>State</th>
<th>Type</th>
<th>Last updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>SURFnet-CERT#013460</td>
<td>cons-1</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>05 May 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013559</td>
<td>airt.nl</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspected</td>
<td>infected</td>
<td>16 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013600</td>
<td>cons-1</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>spam</td>
<td>15 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013610</td>
<td>airt.nl</td>
<td>10.0.x.y</td>
<td>open</td>
<td>acknowledged</td>
<td>spam</td>
<td>12 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013619</td>
<td>cons-2</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>16 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013620</td>
<td>cons-1</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>16 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013633</td>
<td>cust-1</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>probe</td>
<td>13 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013643</td>
<td>external</td>
<td>10.0.x.y</td>
<td>open</td>
<td>blockrequest on</td>
<td>spam</td>
<td>14 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013647</td>
<td>airt.nl</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>probe</td>
<td>13 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013650</td>
<td>external</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>16 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013673</td>
<td>cust-2</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>16 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013677</td>
<td>cons-1</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>16 Jun 2006</td>
</tr>
<tr>
<td>SURFnet-CERT#013678</td>
<td>cust-2</td>
<td>10.0.x.y</td>
<td>open</td>
<td>inspection requested</td>
<td>infected</td>
<td>17 Jun 2006</td>
</tr>
</tbody>
</table>

**New State:** Leave Unchanged
**New Status:** Leave Unchanged
**New Type:** Leave Unchanged

---

**High-quality Internet for higher education and research**
Import queue

- The AIRT import queue allows data from different sources to be automatically processed and relevant information to be extracted from the incoming mail.
Search facilities

- AIRT provides a number of search facilities to quickly find all data required to adequately respond to complaints:
  - Search by IP address
  - Search by email address
  - Search by network range
  - Search by incident ID (internal and external)
### Detailed information for host fuga.uvt.nl

Search results for the following host:

<table>
<thead>
<tr>
<th>ID</th>
<th>IP Address</th>
<th>Hostname</th>
<th>Network</th>
<th>Constituency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>137.56.127.214</td>
<td>fuga.uvt.nl</td>
<td>Infolab GDW (137.56.127.192/26)</td>
<td>Infolab</td>
</tr>
</tbody>
</table>

### Constituency Contacts

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leune. kees</td>
<td><a href="mailto:kees@uvt.nl">kees@uvt.nl</a></td>
<td>2688</td>
</tr>
<tr>
<td>Infolab abuse contact.</td>
<td><a href="mailto:liroot@uvt.nl">liroot@uvt.nl</a></td>
<td>2688/2857/2779</td>
</tr>
</tbody>
</table>

### Previous incidents

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Created</th>
<th>Type</th>
<th>State</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIRT-dev#000003</td>
<td>24 Feb 2006</td>
<td>Spam</td>
<td>Inspectionrequest</td>
<td>open</td>
</tr>
</tbody>
</table>

### Whois information

<table>
<thead>
<tr>
<th>AS</th>
<th>IP</th>
<th>AS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1103</td>
<td>137.56.127.214</td>
<td>SURFNET-NL SURFnet, The Nether</td>
</tr>
</tbody>
</table>

Rights restricted by copyright. See http://www.domain-registry.nl/whois.php

Domain name:
  uvt.nl (next domain)

Status: active

Registrant:
  Katholieke Universiteit Brabant
  Warandelaan 2
  5037 AB TILBURG
  Netherlands
Related work

Standards

– IODEF
  • Overly complex and elaborate. Subset of IODEF can be implemented as import filter.

– CAIF
  • Still in development, used for storing security announcements. CAIF import filter is viable.

– IDMEF
  • Under development at IETF; simple XML-based standard for incident response alert representation. Possible candidate to replace XIRL.
Related Work

Products

- Request Tracker for Incident Response. E-mail ticketing system with web-based front-end. Most well-known competitor to AIRT. Operates on top of general RT product, enhanced with several security-related functions.

- SIRIOS: Modular application framework designed for (CSIRTs) with main focus on incident management and vulnerability handling. SIRIOS is based on OTRS and is sponsored by CERT-Bund, the German governmental CERT.
Improvements since paper was authored

- IDMEF import filter,
- Ability to associate actions with sending mail templates,
- Ability to associate external incident identifiers with AIRT incidents,
- Mass sending of email,
- Export queue,
- Numerous bug fixes,
- Various interface enhancements.
Summary and conclusions

• AIRT provides an incident management system that is based on the notion of an 'incident'.

• Provides easy integration with existing products.

• Adopts Open standards where possible.

• Currently in use with a number of CSIRTs in The Netherlands (SURFnet-CERT, UvA-CERT, UvT-CERT, CERT-UT). Being evaluated by several others worldwide.
Thanks

• AIRT has been developed with the support of SURFnet, the Dutch National Research and Education Network. http://www.surfnet.nl
Contact Information

Kees Leune
kees@uvt.nl

Tilburg University, Infolab
P.O. Box 90153
5000 LE Tilburg
The Netherlands

http://www.airt.nl