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

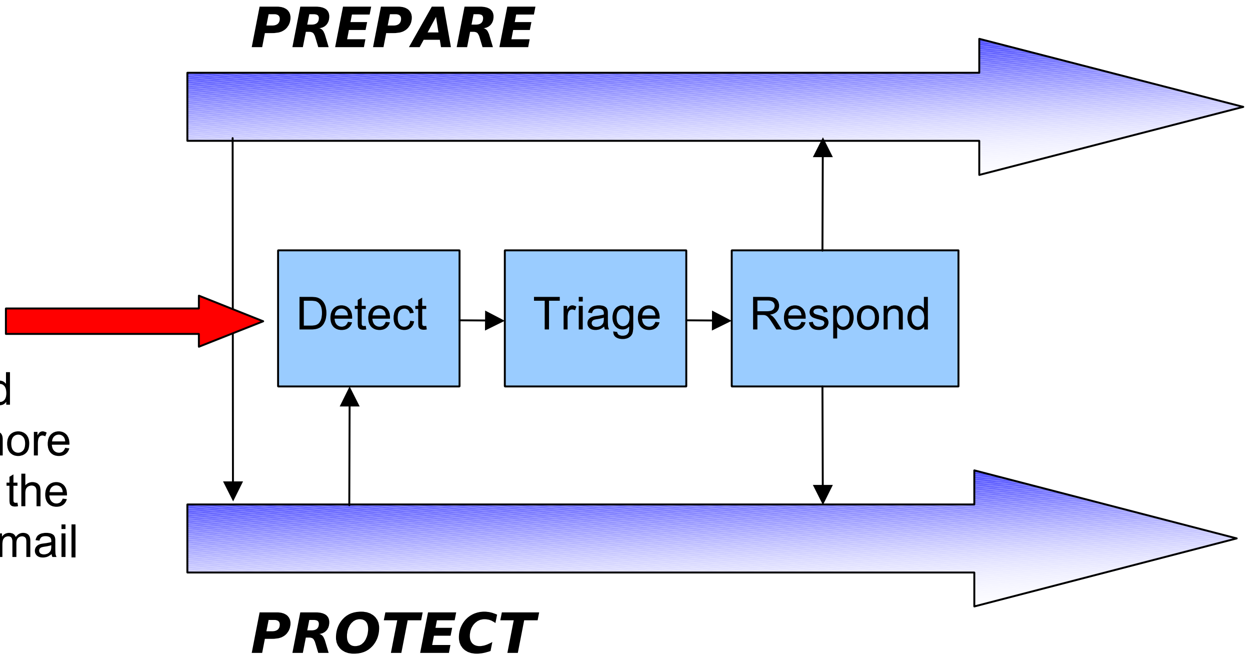
- Ability to record incidents and take initial actions in less than 30 seconds (average) after an incident handler becomes aware of the report.

- 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.

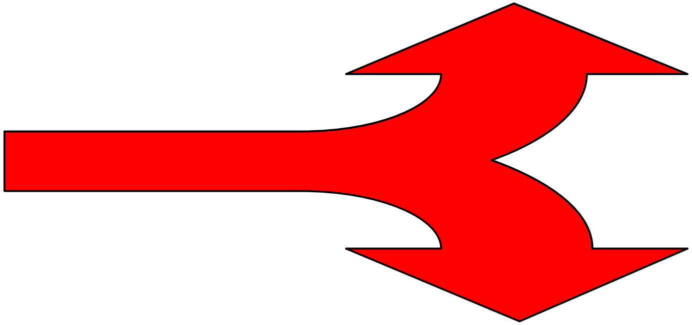
Importance of incoming email



Estimated 95% or more comes in the form of Email

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.*

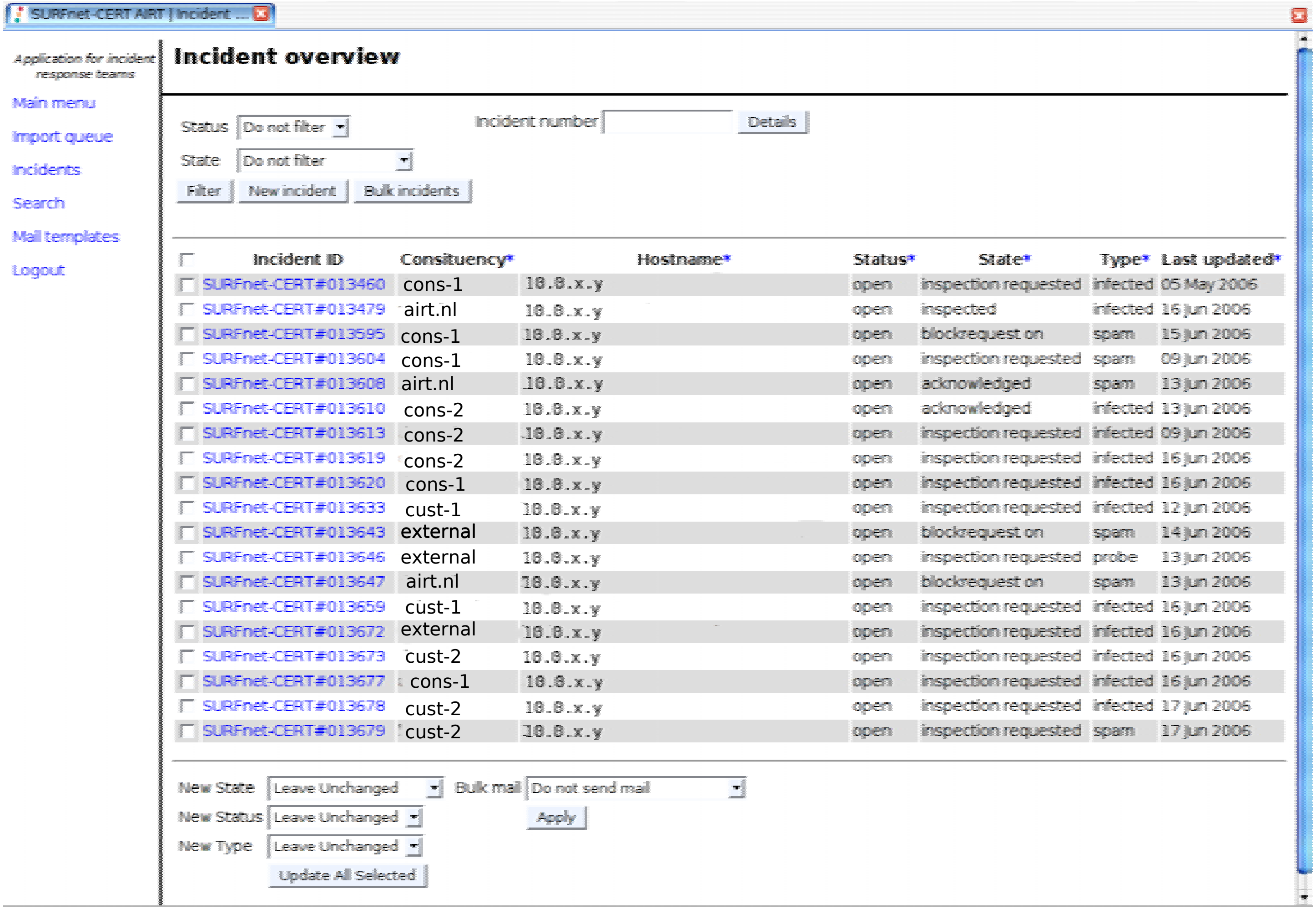
- A number of *IP addresses*, which belong to a *network*, which is managed by a *constituency*, which has *constituency contacts*. Each IP address plays a certain *role in the incident.*

- 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



SURFnet-CERT AIRT | Incident ...

Application for incident response teams

- Main menu
- Import queue
- Incidents
- Search
- Mail templates
- Logout

Incident overview

Status: Do not filter

State: Do not filter

Incident number: Details

Filter | New incident | Bulk incidents

☐	Incident ID	Consituency*	Hostname*	Status*	State*	Type*	Last updated*
☐	SURFnet-CERT#013460	cons-1	10.8.x.y	open	inspection requested	infected	05 May 2006
☐	SURFnet-CERT#013479	airt.nl	10.8.x.y	open	inspected	infected	16 Jun 2006
☐	SURFnet-CERT#013595	cons-1	10.8.x.y	open	blockrequest on	spam	15 Jun 2006
☐	SURFnet-CERT#013604	cons-1	10.8.x.y	open	inspection requested	spam	09 Jun 2006
☐	SURFnet-CERT#013608	airt.nl	10.8.x.y	open	acknowledged	spam	13 Jun 2006
☐	SURFnet-CERT#013610	cons-2	10.8.x.y	open	acknowledged	infected	13 Jun 2006
☐	SURFnet-CERT#013613	cons-2	10.8.x.y	open	inspection requested	infected	09 Jun 2006
☐	SURFnet-CERT#013619	cons-2	10.8.x.y	open	inspection requested	infected	16 Jun 2006
☐	SURFnet-CERT#013620	cons-1	10.8.x.y	open	inspection requested	infected	16 Jun 2006
☐	SURFnet-CERT#013633	cust-1	10.8.x.y	open	inspection requested	infected	12 Jun 2006
☐	SURFnet-CERT#013643	external	10.8.x.y	open	blockrequest on	spam	14 Jun 2006
☐	SURFnet-CERT#013646	external	10.8.x.y	open	inspection requested	probe	13 Jun 2006
☐	SURFnet-CERT#013647	airt.nl	10.8.x.y	open	blockrequest on	spam	13 Jun 2006
☐	SURFnet-CERT#013659	cust-1	10.8.x.y	open	inspection requested	infected	16 Jun 2006
☐	SURFnet-CERT#013672	external	10.8.x.y	open	inspection requested	infected	16 Jun 2006
☐	SURFnet-CERT#013673	cust-2	10.8.x.y	open	inspection requested	infected	16 Jun 2006
☐	SURFnet-CERT#013677	cons-1	10.8.x.y	open	inspection requested	infected	16 Jun 2006
☐	SURFnet-CERT#013678	cust-2	10.8.x.y	open	inspection requested	infected	17 Jun 2006
☐	SURFnet-CERT#013679	cust-2	10.8.x.y	open	inspection requested	spam	17 Jun 2006

New State: Leave Unchanged

Bulk mail: Do not send mail

Apply

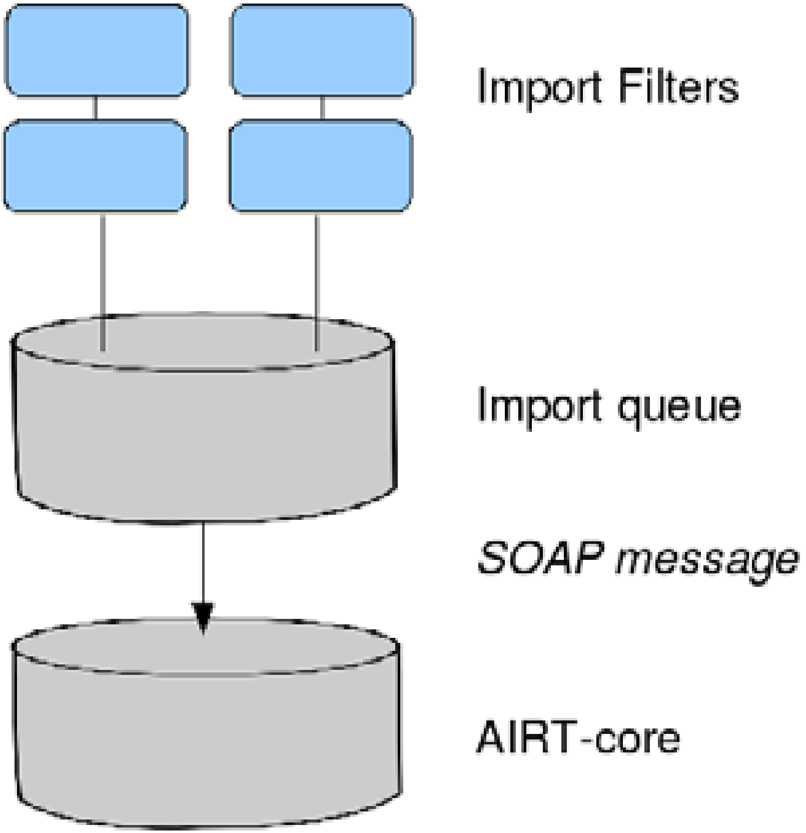
New Status: Leave Unchanged

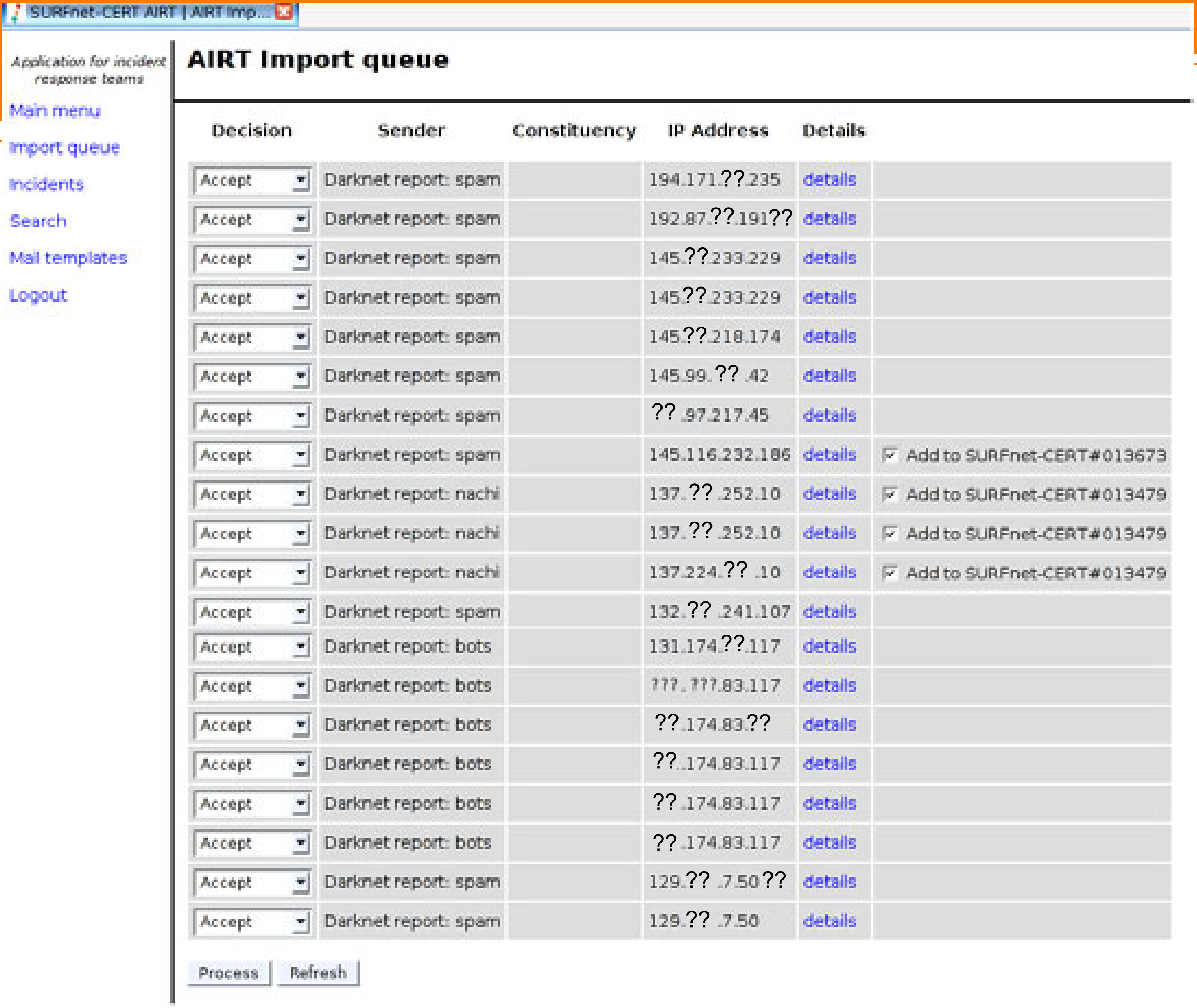
New Type: Leave Unchanged

Update All Selected

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.



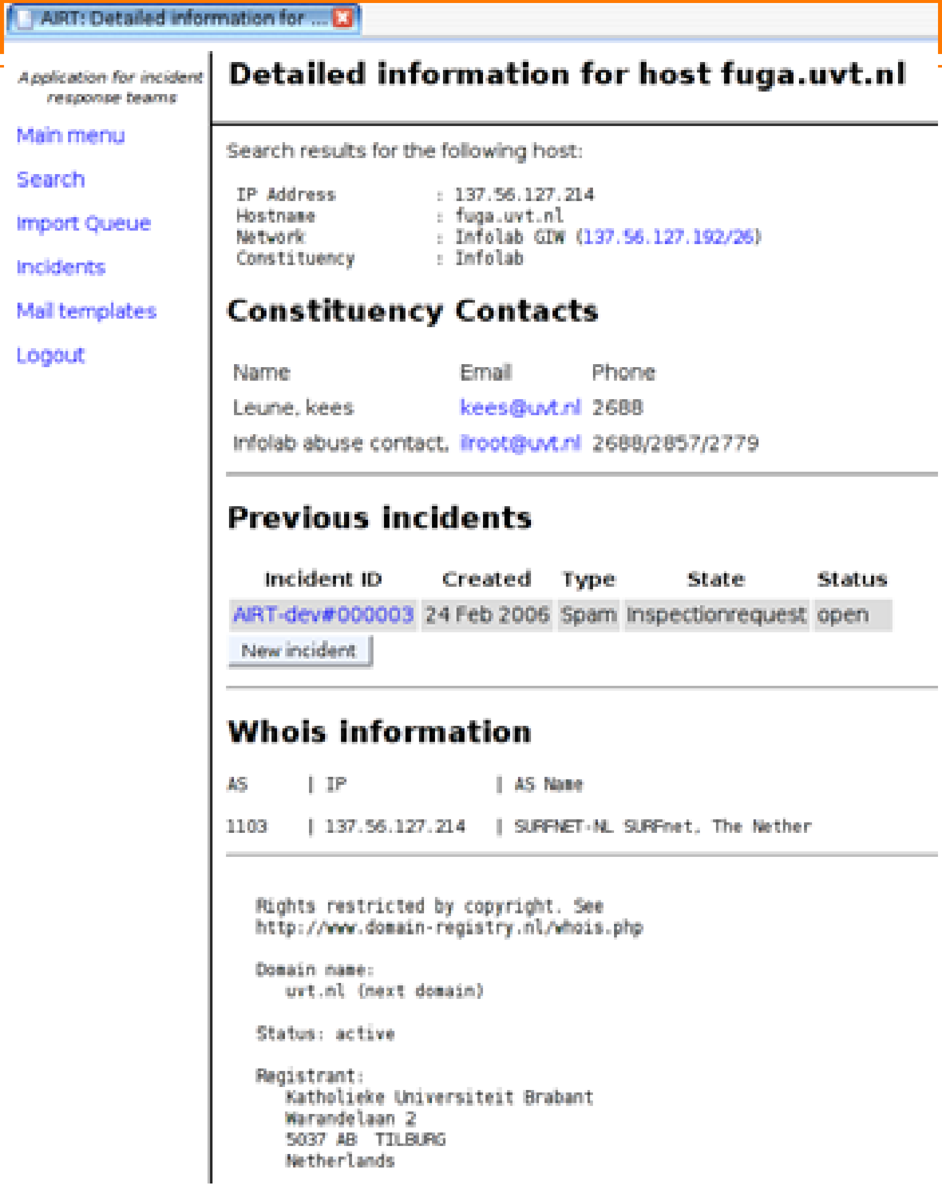

SURFnet-CERT AIRT | AIRT imp...
Application for incident response teams
Main menu
Import queue
Incidents
Search
Mail templates
Logout

AIRT Import queue

Decision	Sender	Constituency	IP Address	Details	
Accept	Darknet report: spam		194.171.??.235	details	
Accept	Darknet report: spam		192.87.??.191??	details	
Accept	Darknet report: spam		145.??.233.229	details	
Accept	Darknet report: spam		145.??.233.229	details	
Accept	Darknet report: spam		145.??.218.174	details	
Accept	Darknet report: spam		145.99.??.42	details	
Accept	Darknet report: spam		??.97.217.45	details	
Accept	Darknet report: spam		145.116.232.186	details	☑ Add to SURFnet-CERT#013673
Accept	Darknet report: nachi		137.??.252.10	details	☑ Add to SURFnet-CERT#013479
Accept	Darknet report: nachi		137.??.252.10	details	☑ Add to SURFnet-CERT#013479
Accept	Darknet report: nachi		137.224.??.10	details	☑ Add to SURFnet-CERT#013479
Accept	Darknet report: spam		132.??.241.107	details	
Accept	Darknet report: bots		131.174.??.117	details	
Accept	Darknet report: bots		???.???.83.117	details	
Accept	Darknet report: bots		??.174.83.??	details	
Accept	Darknet report: bots		??.174.83.117	details	
Accept	Darknet report: bots		??.174.83.117	details	
Accept	Darknet report: bots		??.174.83.117	details	
Accept	Darknet report: spam		129.??.7.50??	details	
Accept	Darknet report: spam		129.??.7.50	details	

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)


AIRT: Detailed information for ...
Application for incident response teams
Main menu
Search
Import Queue
Incidents
Mail templates
Logout
New incident

Detailed information for host fuga.uvt.nl

Search results for the following host:

```
IP Address          : 137.56.127.214
Hostname            : fuga.uvt.nl
Network             : Infolab GIW (137.56.127.192/26)
Constituency        : Infolab
```

Constituency Contacts

Name	Email	Phone
Leune, kees	kees@uvt.nl	2688
Infolab abuse contact,	lroot@uvt.nl	2688/2857/2779

Previous incidents

Incident ID	Created	Type	State	Status
AIRT-dev#000003	24 Feb 2006	Spam	Inspectionrequest	open

Whois information

```
AS      | IP                | AS Name

1103    | 137.56.127.214    | SURFNET-NL SURFnet, The Nether


   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 respose 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 world-wide.

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