



RT for Incident Response (RTIR)

Andy Bone

JANET-CERT Manager

What is RTIR



A tool for incident handling

Now in production with assorted teams
from US to Japan

RTIR Functionality



- IRT specific workflows
- 'clicky' metadata extraction and tracking
- whois integration >
- separate "threads" for each conversation
- high-level overviews
- convenient searching
- simple scriptable actions
- new reporting functionality tied into our new SLA requirement

RTIR Structure



Incident Reports

- Someone has a problem of some kind

RTIR Structure



Incident Reports

- Someone has a problem of some kind

Investigations

- IRT attempts to get to the root of the problem

RTIR Structure



Incident Reports

- Someone has a problem of some kind

Investigations

- IRT attempts to get to the root of the problem

Blocks

- Track network level intervention against threat

RTIR Structure



Incident Reports

- Someone has a problem of some kind

Investigations

- IRT attempts to get to the root of the problem

Blocks

- Track network level intervention against threat

Incidents

- **Ties it all together. May have many related incident reports, investigations and blocks**

RT for example.com

New Incident

New Incident Report

Search

RT

Investigation #18: Incident #15: DOS attack

Reply | Resolve | Open | Comment

RTIR Home

Incidents

Incident Reports

Investigations

Search

New Search

Investigation #18

Display

Edit

Split

Merge

Blocks

Tools

Preferences

The Basics

State: **open**

Incident: **15: DOS attack (open)** [Link] [New]

Priority: **0**

Time Worked: **0 min**

People

Owner: **root**

Correspondents: **root@localhost, root@starsong.org**

Cc:

AdminCc:

Dates

Created: **Tue Apr 29 16:35:43 2003**

Starts: **Not set**

Started: **Not set**

Due: **Not set**

Updated: **Tue Apr 29 16:35:45 2003 by root**

More about root

Comments about this user:

Autogenerated on ticket submission

This user's 10 highest priority tickets:

- **2: yyy** (new)
- **18: Incident #15: DOS attack** (new)

History

Display mode:[Brief headers] [Full headers]

Tue Apr 29 16:35:43 2003 **root - Ticket created**

[Reply] [Comment]

Subject: Incident #15: DOS attack

Download (untitled)

We're receiving reports of a **DOS** attack from **spamdomain.com**. Can you look into it?

123b

Thanks!

Best regards,
The **CERT** team

Tue Apr 29 16:35:45 2003 **root - Ticket fsck.com-rt://example.com/ticket/18 MemberOf ticket 15.**

The WG



- Created after the Madrid meeting.
- Many teams have shown interest and have
- attended meetings
- So far
 - Madrid Meeting
 - London Meeting
 - Video Conference
 - A short get together (1hr) this afternoon in this room (confirmation of actions)

Areas of Interest



GPG/PGP

Current situation:

ACOnet/CERT-PT/RED-IRIS working on requirements and some prototyping

Decisions made:

- Use GPG
- Cached pass phrase.
- Crypto server side.
- Configurable storage of messages.
- Searches to leave out encrypted messages but facility to include should be available.
- Key ring to remain outside RTIR

Areas of Interest



XML Formatting

(passing tickets between teams (different RT Domains))

Current situation:

JANET-CERT has submitted a paper and completed some prototyping, work continues

Decisions made:

Mapping issues made it difficult to introduce IODEF.

Work will be carried out by the team

Areas of Interest



Multiple constituencies

Current situation:

Switch-CERT has submitted a requirements paper and completed much of the prototype work

Decisions made:

Multiple queues

Automated delivery of messages

Areas of Interest



Information Store

Current situation:

JANET-CERT look into the integration of RTFM into RTIR.

Decisions made:

Action ongoing, awaiting discussions with Bestpractical.

Can then store many information sources within the Incident.

Areas of Interest



Templates

Current situation:

Switch-CERT completed much of the work testing at sites is underway

Decisions made:

PH has already created the SRTL system allowing the automatic generation of standard messages.

Areas of Interest



Improve look-up facility

Current situation:

JANET-CERT investigate improvements into the look-up facility. Action ongoing.

Decisions made:

The possibility of multiple contact and whois look-ups.

Areas of Interest



Access to RT Queues

Current situation:

ACOnet-CERT are currently undertaking work in this area.

Work ongoing

Decisions made:

To give access to RT queues from within RTIR.

May give more insight into the advisory queues mentioned earlier.

Areas of Interest



Reporting

Current situation:

JANET-CERT are currently undertaking work in this area.

Work ongoing

Decisions made:

Investigate a automated report generator.

Be able to track incident reports from sites.

Constituent reports to/from, investigation/reports.



Other Actions:

- Code of conduct (**ongoing**)
- Communication
- Documentation release (**Completed**)
- Contracts (**TBD**)
- Bestpractical assurances (RTIR will be compatible with new RT versions). Improve upgrade procedure for new RTIR releases (**Complete**)
- Decision for team or Bestpractical work.
- Creation of the statement of work.

Finding out more



rtir-request@lists.bestpractical.com

- Closed list for incident response team staff

<http://www.bestpractical.com>

<http://www.bestpractical.com/pub/rt/release/rtir.tgz>

sales@bestpractical.com

Questions

