IRT Object in the RIPE Database

Andrew Cormack
Don Stikvoort
Wilfried Woeber
Andrei Robachevsky

Document ID: ripe-254
Date: 19 July 2002

Abstract

This document describes the **irt** object and related functionality in the RIPE Database. The **irt** object is used to provide information about a Computer Security Incident Response Team (CSIRT). This document also describes the creation procedure for the **irt** object.

Table of Contents

1. Motivation

When a computer/network security incident happens, such as DOS (Denial of Service) or spam attack, or other abuse of services, it is important to know whom to contact. The RIPE Database provides the facility to get administrative and technical contacts for a network where the attack came from by a simple IP lookup. In many cases such incidents are handled by CSIRTs whose contacts are different from those listed in "admin-c:" and "tech-c:" attributes. Unfortunately there is no easy way to identify which CSIRT is serving any given IP address.

Also, presenting additional information, such as public certificates of a CSIRT, and query functionality that allows to search for the responsible team would facilitate prompt incident handling.

2. Object template

```
irt:         [mandatory] [single]   [primary/lookup key]
remarks:     [optional]  [multiple] [ ]
address:     [mandatory] [multiple] [ ]
phone:       [optional]  [multiple] [ ]
fax-no:      [optional]  [multiple] [ ]
e-mail:      [mandatory] [multiple] [lookup key]
signature:   [mandatory] [multiple] [ ]
encryption:  [mandatory] [multiple] [ ]
admin-c:     [mandatory] [multiple] [inverse key]
tech-c:      [mandatory] [multiple] [inverse key]
auth:        [mandatory] [multiple] [ ]
irt-nfy:     [optional]  [multiple] [inverse key]
notify:      [optional]  [multiple] [inverse key]
mnt-by:      [mandatory] [multiple] [inverse key]
changed:     [mandatory] [multiple] [ ]
source:      [mandatory] [single]   [ ]
```

3. New attributes

"irt:"

Specifies the name of the **irt** object. The name should start with the prefix "IRT-", reserved for this type of object. An irt name is made up of letters, digits, the character underscore "_", and the character hyphen "-"; it must start with "irt-", and the last character of a name must be a letter or a digit.

"signature:"

References a **key-cert** object representing a CSIRT public key used by the team to sign their correspondence. The value of this attribute has the format: PGPKEY-<id>, where <id> is the PGP key ID of the public key in 8-digit hexadecimal format without "0x" prefix.

"encryption:"

References a **key-cert** object representing a CSIRT public key used to encrypt correspondence sent to the CSIRT. The value of this attribute has the format: PGPKEY-<id>, where <id> is the PGP key ID of the public key in 8-digit hexadecimal format without "0x" prefix.

"irt-nfy:"

Specifies the e-mail address to be notified when a reference to the **irt** object is added or removed. An e-mail address as defined in RFC 2822.

"mnt-irt:"

May appear in an **inetnum** or **inet6num** object. It points to an existing **irt** object representing CSIRT that handles security incidents for the address space specified by the **inetnum** or **inet6num** object. The value of this attribute is the name of the **irt** object. Please see section "Referencing an irt object" for details.

Please refer to the RIPE Database Reference Manual [1] for the description of other attributes.

4. Referencing an irt object

An **irt** object can be referenced from an **inetnum** or **inet6num** object by using the optional "mnt-irt:" attribute, which can appear multiple times in the object. The value of this attribute is the name of an **irt** object. Please see section "Usage Examples" for details.

5. Authorisation checks

When modifying an **irt** object the update should pass authorisation checks specified by one of the mntners listed in "mnt-by:" attributes of the **irt** object.

When adding a reference to an **irt** object the update of an **inet**[**6**]**num** should pass the following authorisation checks:

- from the **irt** object itself as specified in one of the "auth:" attribute
- from any of the **mntner** objects that protect the **inet**[**6**]**num** object (i.e. referenced using "mnt-by:" attribute).

6. Notifications

Whenever a reference to an **irt** object is added to an **inet**[**6**]**num** object or removed from it, a notification about this event is sent to e-mail address specified in the "irt-nfy:" attribute of the referenced **irt** object. This facility may be useful for tracking purposes.

All other notification rules apply too. Please see [1] for the description of the RIPE Database Notifications.

7. New query functionality

As was already mentioned, in many cases administrative contacts for a network may differ from a CSIRT. Also a CSIRT may be responsible for several networks within a specific address range. For example, a large ISP may have a CSIRT that handles incidents in all clients' networks. It is desirable to put the reference to an **irt** object only from the **inetnum** (**inet6num**) encompassing the clients' networks.

The new query functionality allows searching for an **inetnum** object that contains the reference to an **irt** object representing CSIRT responsible for a given address or address range. It is implemented with a new '-c' flag that modifies the behaviour of a normal ip lookup, so that the Database will return the smallest less specific **inetnum** (**inet6num**) object containing the reference to an **irt** object.

The result of this lookup is an **inet**[**6**]**num** object and referenced contacts, if name recursion is not disabled (-r flag). It does not contain the referenced **irt** object, nor contact information about the team.

8. Creation procedure

An **irt** object is created manually by the RIPE Database Administration.

There are two main categories of CSIRTs:

1. A CSIRT that is a member of a recognised and trusted body within the CSIRT community.

2. An independent CSIRT. It may also be a CSIRT from category 1 willing to be registered as independent.

The creation procedure is different for these two cases. We will consider each of them below.

It is important to stress here that existence of an **irt** object in the Database does not prove authenticity and credibility of the team. A stand-alone **irt** object has little meaning, the actual meaning emerges when a reference to the object is made. The role of the above described creation process is to help maintain a high quality of information in the database in this area. However, it is up to a consumer to verify the team's authenticity and credibility.

8.1. Member teams

There are several consortiums that provide a framework for formation and coordination of incidence response teams. Trusted Introducer [2] and FIRST [3] are examples of such consortiums. It is expected that such forums maintain their own procedures regarding CSIRTs, like authentication of teams, maintaining contact information up to date, etc, and use the RIPE Database to publish this information as **irt** objects. Therefore such forums register themselves with the Database Administration to become a single point of contact for creation of the **irt** objects in the Database. General guidelines here are (but alterations are possible):

- The consortium is responsible for correctness of the information presented in **irt** object. Therefore such objects are protected by the **mntner** held by the consortium. The **mntner** should use the strongest authorisation scheme available in the RIPE Database. Please refer to [1] for more information.

- The **mntner** name may be recognised by incident tracing tools and used to present affiliation of an IRT to the consortium. Details of such functionality are outside the scope of this document.

- The creation request comes from the registered contact signed by a public PGP key of the consortium. The Database Administration verifies the signature and creates the object in the database.

- All other **irt** related database transactions, such as modifying or deleting an **irt**, referencing an **irt** from **inetnum** or **inet6num** objects do not require Database Administration intervention. They are controlled by security features of the database system. Please see section "Authorisation checks" above.

8.2. Independent teams

There may be cases when a CSIRT do not belong to any particular forum, or would like to register themselves independently. In such cases the following criteria must be satisfied:

- The creation request comes from the admin-c contact of the **irt** object.

- The request is authenticated by an existing **mntner**, referenced by the object. The need to create an **irt** object cannot be the reason for mntner creation.

- The keys referenced by the **irt** are in the database, the key owner shows affinity to the **irt**.

- The reason for creation is presented along with the timeline for deployment (i.e. referencing the object from where and when).

9. Some recommendations on using irt object

The keys in the "signature" attribute(s) are used to authenticate correspondence from a CSIRT. It is recommended that the Team key comes first.

It is important to maintain the security of the **irt** object itself. The security level is determined by the security level of the weakest **mntner** referenced by the **irt** in its "mnt-by:" attributes. It is wise to ensure that the **mntner**(s) are using the strongest possible authentication scheme (currently, PGPKEY). Please refer to [1] for further information. The **mntner**[s] should be under trusted control (e.g. TI) or full control of the CSIRT.

Addition of a reference to an **irt** object representing a CSIRT means taking responsibility of the team over the address range specified by the **inet**[**6**]**num** object. This responsibility may be taken over by an **irt** object referenced from a more specific **inet**[**6**]**num** object.

The "irt-nfy:" attribute may be used to specify an e-mail address that will be used for tracking additions or removals of references to the **irt** object.

10. Usage examples

Consider the following **irt** object:

```
irt:        IRT-TEST
remarks:    This one should not be trusted
address:    Same address, 1234
phone:      +31 20 0000000
fax-no:     +31 20 0000001
e-mail:     csirt@example.net
signature:  PGPKEY-FFFFFFFF
encryption: PGPKEY-FFFFFFFF
admin-c:    DPO1-RIPE
tech-c:     DPO1-RIPE
auth:       PGPKEY-00000000
irt-nfy:    csirt-log@example.net
notify:     csirt-log@example.net
mnt-by:     TEST-MNT
changed:    ripe-dbm@ripe.net 20020117
source:     TEST
```

Now consider the following address space hierarchy registered in the RIPE Database (only relevant fields are shown):

```
inetnum: 172.16.0.0 - 172.31.255.255
source:  TEST

inetnum: 172.18.0.0 - 172.25.255.255
mnt-irt: IRT-TEST
source:  TEST

inetnum: 172.18.10.0 - 172.18.10.255
source:  TEST
```

The second **inetnum** object references the **irt** object (IRT-TEST). This implies that the CSIRT team represented by that object handles security incidents related to the address space covered by that **inetnum** object.

*Please note that if a more specific **inetnum** object references another **irt** object, that team takes over responsibility.*

If one makes the following query:

```
whois -c 172.18.10.12
```

the following **inetnum** will be returned in response:

```
inetnum: 172.18.0.0 - 172.25.255.255
mnt-irt: IRT-TEST
source:  TEST
```

11. Future applications

A utility could be developed that will accept IP numbers and yield the corresponding CSIRT as deduced from the RIPE Database CSIRT object space, including maintainer info. The latter offers the opportunity to visualize value added information, like e.g. the fact that CSIRT has a Trusted Introducer accreditation.

12. References

[1] RIPE Database Reference Manual
[2] Trusted Introducer. www.ti.terena.nl
[3] FIRST www.first.org

13. Acknowledgment:

The initial version of this document was produced by Andrew Cormack (JANET-CERT), Don Stikvoort (M&I/Stelvio b.v.), Wilfried Woeber (UniVie/ACOnet), and Andrei Robachevsky (RIPE NCC).