



IRT object in the RIPE Database

Andrei Robachevsky

RIPE NCC

<andrei@ripe.net>



Outline

- Motivation
- Technical facility
- Current status
- Open issues



Motivation

- Need to get contact information to report an incident
- Network admin contacts differ from CSIRT's ones
- Need new query functionality



IRT Main Features

- Provides contact information of a CSIRT
 - admin-c, tech-c, fax-no, e-mail
- Provides security information (CSIRT public keys)
 - signature & encryption
- Can be referenced from inet[6]num objects
 - Addition of the reference requires double authorisation
- Searchable using new -c query



IRT Template

irt:	[mandatory]	[single]	[primary/look-up 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]	
inetnum:	[mandatory]	[single]	[primary/look-up key]
...			
mnt-irt:	[optional]	[multiple]	[inverse key]
...			



IRT Sample

```
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:            bitbucket@ripe.net
signature:         PGPKEY- 29A51C3D
encryption:        PGPKEY- 32D62B13
admin-c:           DP01-RIPE
tech-c:            DP01-RIPE
auth:              NONE # Never use this auth scheme !
irt-nfy:           cert-log@mynetwork.mydomain
notify:            cert@mynetwork.mydomain
mnt-by:            TEST-MNT
changed:           ripe-dbm@ripe.net 20020117
source:            TEST

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



-c query

```
i netnum:      172.16.0.0 - 172.31.255.255
```

```
i netnum: 172.18.0.0 - 172.25.255.255  
mnt-irt: IRT-TEST
```

```
i netnum:      172.18.10.0 - 172.18.10.255
```

```
whois -c 172.18.10.12
```



IRT BCP

- **“signature:”**
 - Team key comes first. Used to authenticate correspondence from a CSIRT.
- **“encryption:”**
 - Used to encrypt correspondence to an CSIRT
- **“mnt-by:” (auth), “auth:”**
 - The strongest possible scheme should be used
- **“irt-nfy:”**
 - Notifications about addition/removal of a reference to the CSIRT



Current Status

- DB functionality is in production since February
 - <http://www.ripe.net/ripe/docs/databaseref-manual.html>
- Creation procedure
 - Manual - requests are forwarded to ripe-dbm@ripe.net
 - Procedure with Trusted Introducer is developed
 - requests from level 2 teams come from the TI
- Number of **irt** objects has reached 2 and continues to grow
 - 2 level 2 TI teams (IRT-CERT-NL, IRT-RENATER)
- Draft document is almost ready
 - contains description, BCP and procedure
 - creation procedure is still unclear



Open Issues

- Creation procedure
 - Not to put unnecessary restrictions
 - Well defined and agreed entry points
 - Minimal RIPE NCC involvement
- How to proceed
 - depends on the discussions at the meeting
 - publish the RIPE document



A Few Questions

- What is the actual goal?
 - To provide extended abuse contact for a network.
 - To link CSIRT network with network objects in the RIPE Database.
- Who are the consumers?
 - An abused user.
 - A NOC handling an incident.
- Is it important for an IRT to be part of a consortium?
 - What is the downside of not being a member?
 - Which one? TF-CSIRT, FIRST, ...?
- What is the drawback of allowing any IRT to register themselves?
 - Better than nothing. If a network trusts an IRT.
 - It may obscure a member IRT that can handle an incident more efficiently.

