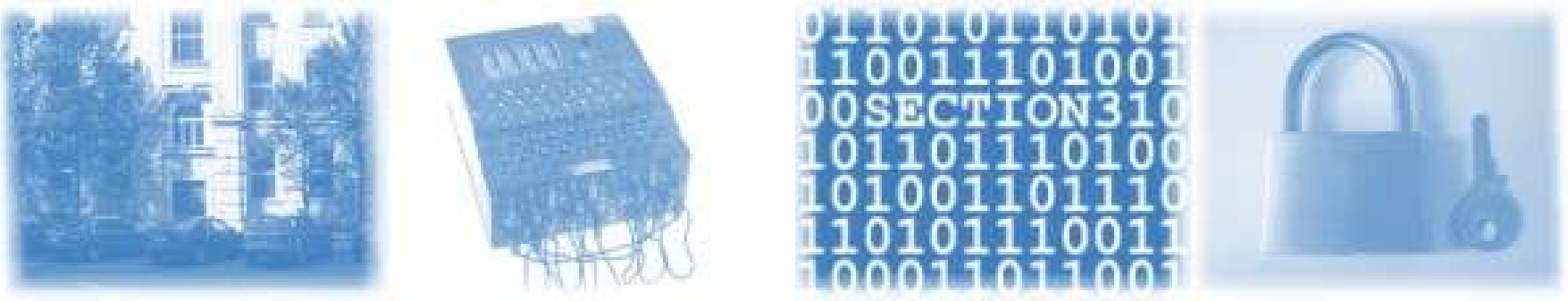

How To IRT ?

Why using the IRT Object is not complicated

Ulrich Kiermayr - Marco Thorbrügge - Jan Meijer

RIPE 47 – Amsterdam, NL

Jan 29, 2004

vienna university
computer center

What does the IRT-Object do?

- documents **I**ncident **R**esponse **T**eams in the RIPE Database
  - registers contact information: PGP-Keys, ...
- supports a more fine grained and scalable approach than individual 'abuse-c, security-c, spam-c, ...'
- links to resource objects (inetnum, inet6num)
- only one object needs maintenance

What does it look like?

```
irt:            IRT-JANET-CERT
address:        Atlas Centre
address:        Chilton
address:        DIDCOT, Oxon
address:        OX11 0QS  UK
phone:          +44 1235 822 340
fax-no:         +44 1235 822 398
e-mail:         cert@cert.ja.net
signature:      PGPKEY-836D7141
encryption:     PGPKEY-836D7141
admin-c:        AB2554-RIPE
tech-c:         RT644-RIPE
auth:           PGPKEY-3EA2BD2B
remarks:        JANET-CERT coordinates security in JANET.
remarks:        http://www.ja.net/cert/
remarks:        JANET is the UK education and research network.
irt-nfy:        ripe-admin@cert.ja.net
notify:         ripe-admin@cert.ja.net
mnt-by:         JANET-CERT
changed:        cert@cert.ja.net 20020808
source:         RIPE
```

Team's PGP-key used for signing

Team's PGP-key used for encryption

Team's PGP-key used to authenticate references

eMail Address to notify about references

vienna university computer center

What to do with it?

Attach the mnt-irt attribute to the resources:

- requires authorization from both parties:
  - maintainer of the address resource
  - signature of the IRT with the **`auth:`** PGP-Key

Search for the most specific inet(6)num referencing a mnt-irt:

```
whois -c <IP-Addr>
```


Search without -c

```
[uk@worf AcoNet]$ whois -r -Tinetnum 193.171.255.0

inetnum:        193.171.255.0 - 193.171.255.95
netname:        ACONET-VIX-SERVICES
descr:          ACOnet Services Network
country:        AT
admin-c:        GW13-RIPE
admin-c:        AP135-RIPE
tech-c:         CP8-RIPE
status:         ASSIGNED PA
notify:         domain-admin@univie.ac.at
mnt-by:         AT-DOM-MNT
changed:        andreas.papst@univie.ac.at 19970324
changed:        Woeber@CC.UniVie.ac.at 19970328
source:         RIPE
```


Search with -c included

```
[uk@worf AcoNet]$ whois -r -c -Tinetnum 193.171.255.0

inetnum:        193.170.0.0 - 193.171.255.255
netname:        AT-ACONET-193-170-193-171
descr:          ALLOCATED BLOCK
descr:          Provider Local Registry
descr:          ACOnet
country:        AT
admin-c:        WW144
tech-c:         WW144
tech-c:         WK42
tech-c:         CP8-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      ACONET-LIR-MNT
mnt-irt:        IRT-ACOnet-CERT
changed:        roderik@ripe.net 19950315
[ ... ]
changed:        hostmaster@ripe.net 20011018
source:         RIPE
```


How to get one?

- By the RIPE-NCC (see: ripe-254)
  - creation request submitted by the admin-c contact of the irt object.
  - request is authenticated by an existing mntner, referenced by the object. The need to create an irt object cannot be the (only) reason for mntner creation.
  - keys referenced by the irt object are in the database already, the key owner shows affinity to the irt.
  - reason(s) for creation is presented along with the time line for deployment (i.e. referencing the object from where and when). **Will not be audited, just recorded!**

HowTo - Creation

- Put your PGP Keys in the Database
  - They should be there for your mntner anyway :-)
- Have your maintainer ready
- Create an IRT Object by filling out the template
  - all PGP-Keys can be the same!
- Send this with a short 'what for' to **<ripe-dbm@ripe.net>**

HowTo – Creation - Example

```
irt:            IRT-UK
address:        Lacknergasse 71/23
address:        A-1180 Wien
address:        AT
phone:          +43 1 5248266
phone:          +43 664 8174818
e-mail:         Ulrich.Kiermayr@UniVie.ac.at
signature:      PGPKEY-A8D764D8
encryption:     PGPKEY-A8D764D8
admin-c:        UK3
tech-c:         UK3
irt-nfy:        Ulrich.Kiermayr@UniVie.ac.at
auth:           PGPKEY-A8D764D8
notify:         Ulrich.Kiermayr@UniVie.ac.at
mnt-by:         UK-MNT
changed:        Ulrich.Kiermayr@UniVie.ac.at 20020820
changed:        Ulrich.Kiermayr@UniVie.ac.at 20030115
source:         RIPE
```


HowTo - Linking

- Add the `mnt-irt: [.....]` to your Inetnums
- The update must be authorized by the mntner **and** the irt.

More Precisely: The update must pass an authorization check against the mntner as well as the auth: from the irt

  - Note: If the PGP Key in the mntner and the irt is the same, you only have to sign once!
  - You do not have to sign every object by itself (as in normal DB Procedure)
  - You do not need to update all your more-specifics due to the **-c** Hierarchy

Howto – Linking 2

- Possible Pitfalls here
  - Updates of objects assigned from RIPE to the LIR must be done by the Hostmasters. (Which is necessary for all Updates to these objects that can not be done through the LIR-Portal)
  - If you do not use PGP-Authentication (*not recomended*™), there is possibly a problem with password disclosure (which holds for the Routing-Registry as well!)

HowTo – Linking - Example

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

inetnum:      131.130.7.32 - 131.130.7.47
netname:      UK-V4
mnt-irt:      IRT-UK
descr:        LAN Ulrich Kiermayr TEST
country:      AT
admin-c:      UK6107-RIPE
tech-c:       UK3
mnt-by:       AS760-MNT
mnt-by:       UK-MNT
status:       ASSIGNED PA
changed:      ulrich.kiermayr@univie.ac.at 20031020
source:       RIPE
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.3 (GNU/Linux)

iD8DBQFAF4FuEF9JHajXZNgRAlcYAJwM1CTqWy6x9L4Jm7NmVanYRvyoiwCfSyHI
lJkbsynH+qaXWykYYBY4pPo=
=lbFX
-----END PGP SIGNATURE-----
```


Mass Linking Strategies

- You can update more than one object at once
- Use scripts :-)
  - The shortest one I could come up with:

```
whois -T inetnum,inet6num -i mnt-by -r
  UK-MNT | egrep -v '^(%|mnt-irt)' | sed
  -e 's#^inetnum:.*$#&\nmnt-irt: IRT-UK#'
  -e 's#^source:#changed:
  uk@uk.atat.at\n&#' | gpg -a --clearsign
  | mail -s 'Add IRT Object' auto-
  dbm@ripe.net
```


Tool using IRT

- RIPE Whois Client
- CERT-POLSKA abuse contact tool
  - http://www.cert.pl/cgi-bin/ipdig.pl
- ?
- ?
- ?
- ?
- ....

Open Issues - Discussion

- Default behavior of the Database
  - Return IRT by default?
  - Flag to return only an appropriate IRT? (For easy processing)
- Other Objects to add mnt-irt to
  - autnum
  - as-set
  - (org)
- Creation Policy
- Which attributes should be mandatory/optional?

More HowTo Documentation

- TF-CSIRT IRT Documentation
  - http://www.dfn-cert.de/team/matho/irt-object/
- ripe-254 document
  - http://www.ripe.net/ripe/docs/irt-object.html
- Ripe Database Manual
- Trusted Introducer
  - http://www.ti.terena.nl

Q&A

Questions

Contact Information

Ulrich Kiermayr

Vienna University Computer Center / ACOnet
Universitätsstrasse 7
1010 Vienna, AT

Phone: +43 1 4277 14104
Fax: +43 1 4277 9140
eMail: ulrich.kiermayr@univie.ac.at

vienna university computer center