

IRT Object in RIPE DB

TF-CSIRT Seminar, Zagreb, Jan. 22, 2003

Vienna University, ZID, ACOnet-IRT

Ulrich Kiermayr

`kiermayr@CC.UniVie.ac.at`

Wilfried Wöber

`woeber@CC.UniVie.ac.at`

A brief intro to the RIPE DataBase

- What is the goal?
 - Document holdership of Internet Resources
 - Answer queries for those resource (over the net)
- What type of information is stored?
 - IPv4 and IPv6 address allocations and assignments
 - Routing Identifiers (Autonomous System Numbers)
 - Contacts (person data, role data)
 - Support info (reverse DNS domains, IRTs, ...)
 - Routing policy

Logical structure of data in the DB

- The "piece of data" that can be handled (created, modified, queried) is an "object"
- An object has a well-defined set of properties
 - An object **type** (eg. person:, inetnum:, role:, mntner:, aut-num:, route6:[RPSLng])
 - A set of **attribute / value pairs** (eg. source: RIPE), some are "mandatory", others are "optional"
 - Can **link to** other objects (references, relations)

How is the data maintained?

- Creating objects, and keeping them up-to-date, is a distributed (shared) responsibility
- The holder of a resource "owns" the set of related objects
- For some resources there is a hierarchy,
 - IP address space
- others are "flat"
 - AS numbers, persons, ...

What do these objects look like?

```
% This is the RIPE Whois server.  
% The objects are in RPSL format.  
%  
% Rights restricted by copyright.  
% See http://www.ripe.net/ripenncc/pub-services/db/copyright.html
```

```
inet6num:    2001:0628:14fa::/48  
netname:     UK-V6  
mnt-irt:     IRT-UK  
descr:       IPv6 LAN Ulrich Kiermayr  
country:    AT  
admin-c:     UK3  
tech-c:      UK3  
mnt-by:     ACONET-LIR-MNT  
status:     ASSIGNED  
notify:      ulrich.kiermayr@univie.ac.at  
changed:     Woeber@CC.UniVie.ac.at 20020725  
changed:     UK@univie.ac.at 20020822  
source:     RIPE
```

```
person:      Ulrich Kiermayr  
address:     Dampierrestrasse 4/5  
address:     A-1140 Wien  
address:     AT  
phone:       +43 1 9671909  
phone:       +43 699 19671909  
e-mail:      Ulrich.Kiermayr@UniVie.ac.at  
nic-hdl:     UK3  
remarks:     GPG-Key: PGPKEY-A8D764D8  
mnt-by:     UK-MNT  
notify:      Ulrich.Kiermayr@UniVie.ac.at  
changed:     UK@UniVie.ac.at 20020723  
source:     RIPE
```

Hierarchy and Collaboration

- To preserve integrity in this environment, we need mechanisms
 - to **protect** sets of objects,
 - but also to support shared responsibility, i.e. to **authorise modification...**
 - IANA => RIRs => LIRs => IP-Address-Blocks
 - IANA => RIRs => LIRs => ISP => AS# => routes
 - The same person: can be the contact for different resources
 - Mapping of/to CERTs/IRTs is independent

Maintainer concept: "authorisation"

- The mechanisms available to define the authorisation for performing a DataBase transaction (create, update/delete):
 - **NONE** not recommended for a public DB ☺
 - **MAIL-FROM** weak, easy to fake, not recommended
 - **CRYPT-PW** the old Unix service – of limited value
 - **MD5-PW** better, still contains password in update
 - **PGPKEY** PGP, GnuPG support, asymm. crypt.
- Notification: success and failure logging

How are transactions submitted?

- Most transactions are (still) sent by eMail
 - Asynchronous mechanism
 - Easy to log and process on both sides
 - Confirmation/Failure notice is sent back as reply
 - Notification and logging is triggered
- Synchronous update
 - To support web-based user interfaces
 - For bulk updates (internally, protected)
 - API for other interfaces

Object creation paths

- "automatic" or "public" ("help yourself"!)
 - E.g. for person: and role: objects
 - Submitted to **<auto-dbm@ripe.net>**
 - Processed automatically, as soon as possible
- "manually" or "moderated"
 - E.g. for mntner: and irt: objects
 - Submitted to **<ripe-dbm@ripe.net>** directly or forwarded from **<auto-dbm@ripe.net>**
 - For human review and processing

The consumer view

- The bulk of the queries are (still) done with **whois** (on well-known port 43)
- A web-based interface has also become available a while ago [\[see web form\]](#)
 - Lookup types:
 - Simple lookup by supplying a (primary) key
 - More complex lookup via other (indexed) attributes
 - "inverse": `$ whois -i admin-c,tech-c,zone-c WW144`
 - Lookup in resource trees (more / less specific)

The irt: object for CERTs/IRTs

- What was (or rather is) the problem?
- The DataBase did already support different types of contact information (references):
 - admin-c: e.g. the "owner" of a domain
 - tech-c: on-site contact for operational issues
 - zone-c: contact for DNS zone maintainer
- Why don't we simply add
 - abuse-c: for all sorts of complaints?
 - and then spam-c:, IDS-c:, routing-problem-c: :-O

There's a better approach!

- The "add more" approach doesn't scale well
- But - haven't we solved a similar problem already? Yes, so, let's try to copy the maintainer (mntner: object) model!
- The irt: object is similar, but not the same
 - Different set of attribute / value pairs (schema)
 - SHOULD be maintained linking to a mntner:
 - Does not allow weak auth: mechanisms

What does it look like?

```
irt: IRT-UK
address: Dampierrestrasse 4/5
address: A-1140 Wien
address: AT
phone: +43 1 9671909
phone: +43 699 19671909
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: UK@Univie.ac.at 20020820
changed: UK@Univie.ac.at 20030115
source: RIPE
```

```
person: Ulrich Kiermayr
address: Dampierrestrasse 4/5
address: A-1140 Wien
address: AT
phone: +43 1 9671909
phone: +43 699 19671909
e-mail: Ulrich.Kiermayr@Univie.ac.at
nic-hdl: UK3
remarks: GPG-Key: PGPKEY-A8D764D8
mnt-by: UK-MNT
notify: Ulrich.Kiermayr@Univie.ac.at
changed: UK@Univie.ac.at 20020723
source: RIPE
```

How to create an irt: object?

- For the man in the streets:
 - Submit to & ask for manual creation by **ripe-dbm**
 - The RIPE NCC decides: yes/no
- For teams existing within a well-defined "structure", or going through a certification:
 - The structure provides the approval (the yes/no) as input to the RIPE NCC
 - Manual creation of object by **ripe-dbm**
 - Agreement between **ripe-dbm** and the source of the "yes/no" decision is required

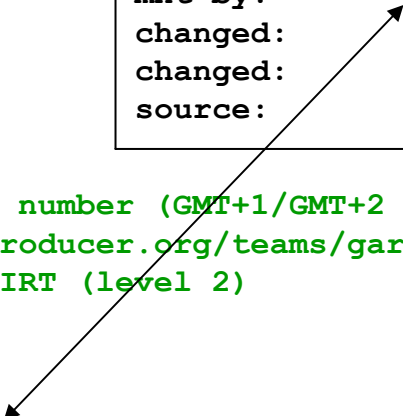
The role of the Trusted Introducer

- TI is one, if the first, well-defined structure!
- Agreement TI \Leftrightarrow RIPE-NCC is in place
- A well-defined interaction between teams and TI (the accreditation process) is in place
- TI usually has all the data on file to build an irt: object and submit it to **ripe-dbm**
- Referencing (linking to) it's own maintainer object

The little difference...

```
irt:          IRT-GARR-CERT
address:     GARR-CERT
address:     c/o INFN, Sez. di Firenze
address:     L.go E. Fermi 2
address:     I 50125 Firenze
address:     ITALY
phone:       +39 055 2307696
phone:       +39 055 2307764
phone:       +39 055 4572113
fax-no:      +39 055 229330
fax-no:      +39 055 4572364
e-mail:      cert@garr.it
signature:   PGPKEY-6291A891
encryption:  PGPKEY-6291A891
admin-c:     TI123-RIPE
tech-c:      TI123-RIPE
auth:        PGPKEY-6291A891
remarks:     No emergency telephone number (GMT+1/GMT+2 with DST)
remarks:     http://www.trusted-introducer.org/teams/garr-cert.html
remarks:     This is an accredited IRT (level 2)
irt-nfy:     cert@garr.it
notify:      tiirt@stelvio.nl
notify:      cert@garr.it
mnt-by:      TRUSTED-INTRODUCER-MNT
changed:     gert-henk.bakker@stelvio.nl 20021112
source:      RIPE
```

```
irt:          IRT-UK
address:     Dampierrestrasse 4/5
address:     A-1140 Wien
address:     AT
phone:       +43 1 9671909
phone:       +43 699 19671909
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:     UK@Univie.ac.at 20020820
changed:     UK@Univie.ac.at 20030115
source:      RIPE
```



What to do with those tools?

- Tag the resource objects,
 - initially inet[6]num: only, (routing may be next?)
 - belonging to a team's constituency,
- with a reference to the IRT/CERT,
 - i.e. link to the team's irt: object
- Note: both parties' credentials (auth:) in referenced irt: and mntner: are required!
 - Do not use password based protection!
 - Use digital signatures!

Again, what does it look like?

```
inet6num: 2001:0628:14fa::/48
netname: UK-V6
mnt-irt: IRT-UK
descr: IPv6 LAN Ulrich Kiermayr
country: AT
admin-c: UK3
tech-c: UK3
mnt-by: ACONET-LIR-MNT
status: ASSIGNED
notify: ulrich.kiermayr@univie.ac.at
changed: WW@Univie.ac.at 20020725
changed: UK@univie.ac.at 20020822
source: RIPE
```

```
mntner: ACONET-LIR-MNT
descr: AConet Local-IR
admin-c: WW144
tech-c: WW144
auth: MD5-PW $1$aHlRO/$9qhLS1f/CbmLFUMfs8Xf/0
auth: PGPKEY-DBC579D4 # AConet Local-IR
auth: PGPKEY-A8D764D8 # UK6107-RIPE
auth: PGPKEY-087772F4 # HM3550-RIPE
mnt-by: ACONET-LIR-MNT
source: RIPE
```

```
irt: IRT-UK
address: Dampierrestrasse 4/5
address: A-1140 Wien
address: AT
phone: +43 1 9671909
phone: +43 699 19671909
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: UK@Univie.ac.at 20020820
changed: UK@Univie.ac.at 20030115
source: RIPE
```

irt: & mntner: references
auth: credentials

How do I query for an IRT?

- Let's assume that you identify an intrusion coming from *ipv4-address-crack* ...
 - Do a
 - `$ whois -h whois.ripe.net -Tinetnum ipv4-address-crack`
 - and then do a
 - `$ whois -h whois.ripe.net -c ipv4-address-crack`
- Which tries a direct lookup for an irt: object,
 - and if found returns the result, or
- does a tree-walk \implies root, looking for an irt:

More information and outlook...

- The DataBase reference documentation
 - <http://www.ripe.net/ripe/docs/databaseref-manual.html>
- A helping hand provided by the Trusted Introducer?
- Training material to be put together?
- A hands-on workshop?
- The challenge:
 - get the DB populated?!
 - educate the "consumers"?!

Thank you!

any questions?

`mousevirus.jpg`

