



universität
wien

irt: Object Workshop

Wednesday, Sept. 20, 2006 – Espoo, FI





Outline

1) The Background

2) "I/O" - Interactions with the Database

3) Technology

4) The TI-Approach - from an IRT-Team's point of view

5) Further Reading and Documentation

(to be added in an updated version of the slides)



The Background (1)

- **The Database: why and how?**

- initially, keeping track of Internet resources (IP #s, AS #s) was a pencil and paper task, sometime (really! the HP “accident”)
- done centrally at IANA (Jon Postel), then by SRI, InterNIC,...
- maintained like the „Hosts File“

- **Regional Activities started in the late 1900s**

- in Europe, Asia-Pacific (late 80s/early 90), then The Americas
- later LACNIC (late 90s) and eventually AfriNIC

- **Regional Registry Database Models**

- one per region (RIPE NCC)
- optionally with intermediate national (Asia-Pacific Region)
- optionally with „rwhois“ approach (ARIN Region)



The Background (2)

What do the Registries have to keep track of?

- **Authoritative data for unique identifiers**
 - IP Address Registry (IPv4 and IPv6)
 - Autonomous System numbers
- **Ancillary Data**
 - domain names (historic - last trace: „referral mechanism“)
- **Voluntary collaboration support**
 - routing registry aka “IRR”
- **Internet Operations Support**
 - reverseDNS delegations (IPv4 and IPv6, part of “arpa.” tree)
 - ENUM registry (RIPE NCC: e164.arpa. tree)



The Background (3)

The architecture and the structure of the Database:

- „Objects“, stored and handled as monolithic entities

- attribute/value pairs **as-block: AS1853 - AS1854**
- templates, mandatory and optional attributes
- syntax
- semantics
- „something“ that makes an object unique
 - a „handle“, **e.g. nic-hdl: WW144**
 - a type + name, **e.g. irt: IRT-UK**



The Background (Example 1: A Template)

```
$ whois -t irt
```

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



The Background (Example 2: Syntax, Semantics)

```
$ whois -v irt
```

The irt class:

An irt object is used to define a Computer Security Incident Response Team (CSIRT).

irt:	[mandatory]	[single]	[primary/look-up key]
< >			
mnt-by:	[mandatory]	[multiple]	[inverse key]
changed:	[mandatory]	[multiple]	[]
source:	[mandatory]	[single]	[]

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.

< >



The Background (4)

The architecture and the structure of the DB:

- **structured and flat resource spaces**
 - IP-Address blocks are part of a distribution hierarchy or tree
 - IANA → RIR [→ NIR] → LIR → „Site“
 - AS Numbers are picked from a „flat“ pool of 16bit numbers
 - asn32 proposals being discussed
 - managed as individual entities (but there may be „ranges“)
- **there are relationships between objects (links / references)**
 - the most simple case: a contact person for a resource



The Background (Example 3: References)

```
$ whois -r irt-uk
```

```
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:        X509-342
encryption:       X509-343
signature:        PGPKEY-708C030A
encryption:       PGPKEY-708C030A
admin-c:          UK3
tech-c:           UK3
irt-nfy:          Ulrich.Kiermayr@UniVie.ac.at
auth:             PGPKEY-A8D764D8 # UK6107-RIPE (deprecated)
auth:             PGPKEY-708C030A # UK6107-RIPE
mnt-by:           UK-MNT
source:           RIPE # Filtered
```



The Background (Example 4: „Recursion“)

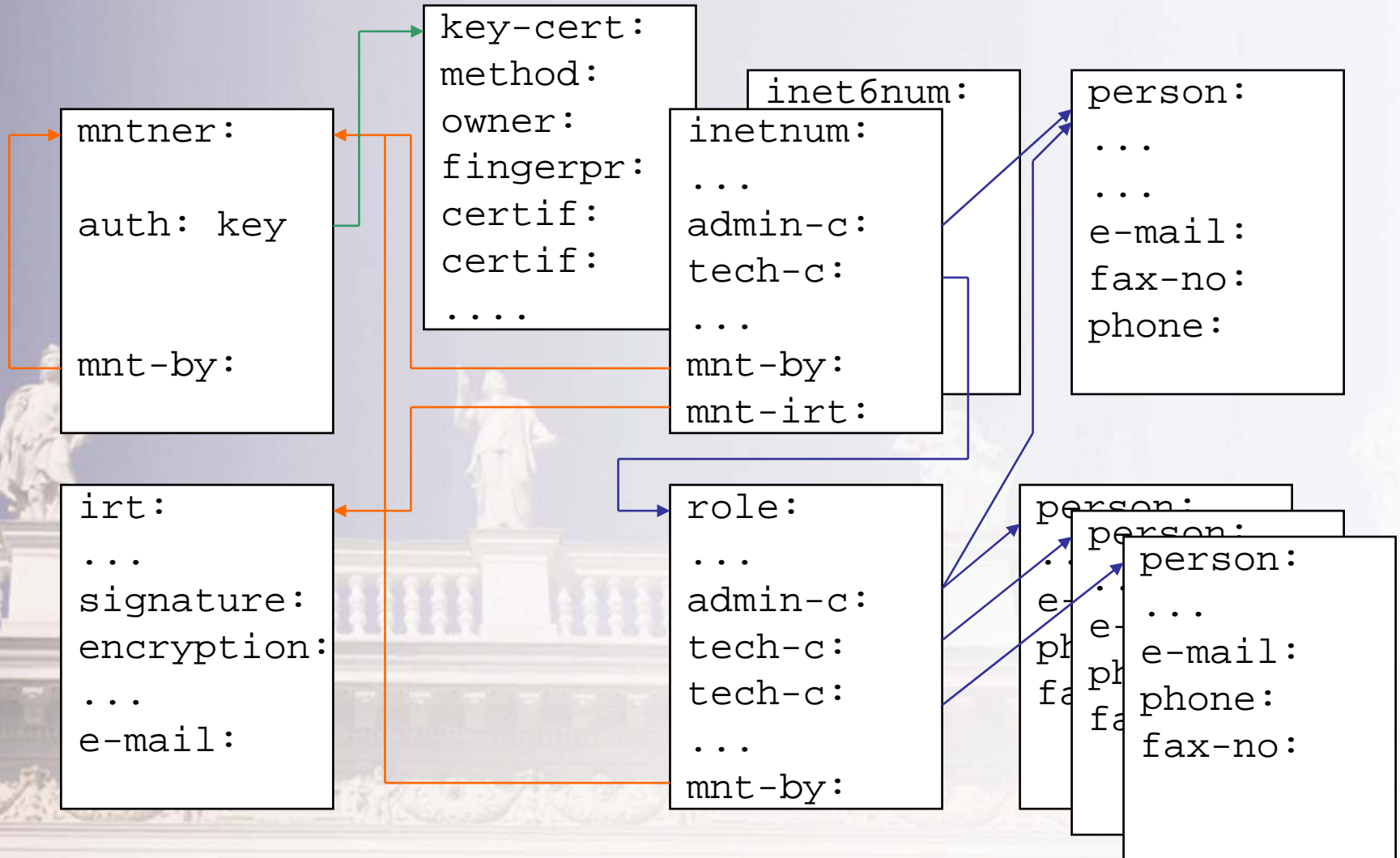
```
$ whois -B irt-uk
```

```
irt:                IRT-UK
address:            Lacknergasse 71/23
< ..... >
auth:               PGPKEY-708C030A # UK6107-RIPE
notify:             Ulrich.Kiermayr@Univie.ac.at
mnt-by:             UK-MNT
changed:            Ulrich.Kiermayr@Univie.ac.at 20020820
changed:            Ulrich.Kiermayr@Univie.ac.at 20050425
changed:            Ulrich.Kiermayr@Univie.ac.at 20051121
source:             RIPE
```

```
person:             Ulrich Kiermayr
address:            Lacknergasse 71/23
< ..... >
remarks:            GPG-Key: PGPKEY-A8D764D8
mnt-by:             UK-MNT
notify:             Ulrich.Kiermayr@Univie.ac.at
changed:            Ulrich.Kiermayr@Univie.ac.at 20020723
source:             RIPE
```



Relationship between DB objects





Interaction with the Database (1)

- **How to load and modify information?**

- initially, e-mail only

- auto-dbm@ripe.net (you talk to a robot)

- ripe-dbm@ripe.net (you talk to a human)

- „Web-Update“ e.g. RIPE Web-Site, LIR-Portal

- „Synch-Update“ as a special case to support interactive scripts

- **How to obtain information from the Database?**

- `$ whois -h whois.ripe.net` Or `$telnet whois.ripe.net 43`

- Web-Queries

- „NRTM“: Near RealTime Mirror

- ftp access to (most) bulk data, aka „split files“



Interaction with the Database (2)

- **How to control type and amount of information returned?**
 - include “command line” flags with the query
 - **-r** disables recursion, **on** by default
 - **-B** disables filtering of e-mail addresses, **on** by default
 - **-T** selects a particular type of objects, e.g. role:, person:
 - **-a** asks to search „all“ sources, **off** by default (see **-h** flag)
 - **-i** perform an „inverse“ search
 - (e.g. `$ whois -Ti admin-c,tech-c WW144`)
 - **-c** look for CERT, i.e. irt: objects, but – see next slides!
- **How to select a particular Registry Database?**
 - `$ whois -h whois.apnic.net`



Interaction with the Database (3)

- **Lookup “Magic”**

- the lookup mechanism knows about and can track
 - references (contact info, “related” info, and irt: objects)
 - ranges and hierarchy in resource space → „tree-walk“

- `$ whois -B -Tinetnum 131.130.1.200`

- does not exist, the range 131.130.0.0 - 131.130.255.255 does

- this is legacy space, so we have to deal with ranges

- **Tree-Walk in „modern“ LIR address space?**

- `$ whois -B -Tinetnum 193.171.1.5`

- does not exist, but the range 193.171.1.0 - 193.171.1.255
- is part of a distribution tree IANA → RIR → LIR → Site → Host



Interaction with the Database (4)

- **Less Specific vs. More Specific**

- an individual host address is the *most specific* piece of data
- the whole IP address space is the *least specific* piece of data
 - starting at the bottom or root of the tree you can query for
 - **-m** or **-M** i.e. more specific information
 - starting at a host address you can ask for
 - **-l** or **-L** i.e. less specific information

- **Tree-Walk in „modern“ LIR address space?**

- `$ whois -rLTinetnum 193.171.1.5`

```
inetnum: 193.171.1.0 - 193.171.1.255
```

```
inetnum: 193.170.0.0 - 193.171.255.255
```

```
inetnum: 193.0.0.0 - 195.255.255.255
```

```
inetnum: 0.0.0.0 - 255.255.255.255
```



Interaction with the Database (5)

- Tree-Walk in „modern“ LIR address space?

– \$ whois **-rMT**inetnum 193.170.0.0/15

inetnum: 193.170.79.0 - 193.170.79.255

inetnum: 193.170.237.0 - 193.170.237.63

inetnum: 193.171.92.0 - 193.171.94.255

inetnum: 193.170.8.0 - 193.170.11.255

< >



Interaction with the Database (6)

- Looking for CERT Contact(s)?

- \$ whois **-rc** 193.170.0.0/15

```
inetnum:          193.170.0.0 - 193.171.255.255
org:              ORG-AA1-RIPE
netname:          AT-ACONET-193-170-193-171
< ..... >
mnt-by:           RIPE-NCC-HM-MNT
mnt-lower:        ACONET-LIR-MNT
mnt-irt:          IRT-ACOnet-CERT
source:           RIPE # Filtered

irt:              IRT-ACOnet-CERT
address:          Vienna University Computer Center
< ..... >
mnt-by:           TRUSTED-INTRODUCER-MNT
source:           RIPE # Filtered
```



Technology: Protection & Authentication (1)

- **In the Previous Century the Internet was a cosy place...**
 - Protection? Wich protection? Why? We are collaborating!
 - Protection Mechanism: NONE (deceased 😊)
- **The primary update mechanism (still) is eMail**
 - everyone knows me, it is my job, so a mail from „me“ is OK!!
 - Protection Mechanism: MAIL-FROM (deceased 😊)
- **eMail is easy to forge (telnet 25, SMTP's mail from: anyone?)**
 - we need passwords, yeah, like Unix does it, ´course
 - Protection Mechanism: CRYPT-PW (being killed 😞)
 - Protection Mechanism: MD5-PW (just a tad better...)
- **How about doing it „right“, eventually?**



Technology: Protection & Authentication (2)

- **digital signatures, please!**
 - 1st implementation: GPG/GnuPG asymmetric cryptography
 - Protection Mechanism: PGPKEY-DEADBEEF
 - public key is stored as a regular database object

```
key-cert:      PGPKEY-DBC579D4
method:       PGP
owner:        AConet Local-IR Domain-Admin@UniVie.ac.at
fingerpr:     87BF 7119 1BC8 A146 36FA 4F7A 9643 017A DBC5 79D4
certif:       -----BEGIN PGP PUBLIC KEY BLOCK-----
< ..... >
certif:       iQA/AwUYNr7yNJZDAXrbxXnUEQJ2qgCdGFn7tqgt1L+hdSO8...
certif:       yR6OSyYvXouBbvB1/ghC42Rw
certif:       =3Xx/
certif:       -----END PGP PUBLIC KEY BLOCK-----
mnt-by:       ACONET-LIR-MNT
source:       RIPE # Filtered
```



Technology: Protection & Authentication (3)

- **digital signatures, please!**
 - more recently support for X.509 certificates was added
 - Protection Mechanism: X509-...99...
 - public key is stored as a regular database object

```
key-cert:      X509-342
method:        X509
owner:         /C=AT/ST=UK/L=UK/O=Univie/OU=VUCC/CN=uk@uk.atat.at/e...
fingerpr:      64:4E:9A:51:7E:6D:12:03:01:51:B5:37:0E:05:60:D0
certif:        -----BEGIN CERTIFICATE-----
< ..... >
certif:        -----END CERTIFICATE-----
remarks:       sample Signing Certificate
admin-c:       UK3
tech-c:        UK3
mnt-by:        UK-MNT
source:        RIPE # Filtered
```



Technology: Protection & Authentication (4)

- **Each object has to be „properly“ protected**
 - Prevent tampering with registry data
 - Authenticate update (and delete) transactions
- **How to register Protection&Authentication settings?**
 - individually, on each object we want to configure
 - how many objects do we have in the Database? Your guess?
- **This needs to be streamlined - definitely!**
 - usually, a collection of objects is maintained by **one** (or a few) entities. The same mechanisms should apply to the collection.
- **Maintainer Object**
 - describes an entity that is allowed to modify and/or
 - to register (additional) objects in a structured resource space



Technology: Protection & Authentication (5)

- **A Maintainer Object is just „another“ regular object**
 - It needs to be protected, can point to itself
 - It has to be modified now and then, → authentication required
- **The same maintner: Object is referenced**
 - by *all* objects being controlled by that entity, by using mnt-by:
 - privilege changes can be managed in a single place
 - changes become effecive immediately for all controlled objects
- **Sharing responsibilty is (easily and selectively) possible**
 - by referencing *more* than one maintainer in an object „[multiple]“
 - but use the notification mechanisms!
 - CAUTION: the weakest protection mechanism always wins!!!



Technology: More than 1 set of credentials (1)

- **Sometimes it takes two to party...**
 - E.g. for a routing registry entry you need agreement from
 - the AS operator, the „origin:“
 - the holder of the address space, IPv4 and IPv6
- **how to state „consent“?**
 - add your authentication credentials:
 - manufacture the object locally
 - add your password
 - forward to the „other“ party
 - other party adds password and
 - forwards to database
- **Hey – wait – they get to know my password? Yes-Indeed!**



Technology: More than 1 set of credentials (2)

- **A clumsy work-around...**
 - If at least one party uses digital signatures, then *sign* first
 - forward to 2nd party, *then* add password and
 - forward to database robot
 - It is just a weird hack, so...
- **Use digital signature authentication - please**
 - manufacture object and digitally sign (don't encrypt!)
 - forward to other party
 - other party adds signature
 - anyone can submit to the database
- **AND: it is protected en-route! 😊**



Technology: What's an IRT Object?

- **Management Summary: very similar to a maintainer**
 - Meant to be referenced by a set of objects
 - Controls protection and authentication
 - But:
 - in many organisations there are separate entities that manage:
 - IP-Address Space, Routing Configuration
 - Security and Abuse Complaints
- **irt: is similar to mntnr:, which some differences**
 - a query for irt: triggers a „tree-walk“ towards the root
 - it is still evolving, e.g. dig.certif.s have been made optional
 - proposal for modifying the template, syntax and semantics



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



Example

```
[uk@worf AcoNet]$ whois -r irt-aconet-cert
```

```
irt:                IRT-ACOnet-CERT
address:            Vienna University Computer Center
address:            Universitaetsstrasse 7
address:            A-1010 Vienna
address:            AUSTRIA
phone:              +43 1 4277 14045
fax-no:             +43 1 4277 9140
e-mail:             cert@aco.net
signature:          PGPKEY-B06F5077
encryption:         PGPKEY-B06F5077
admin-c:            TI123-RIPE
tech-c:             TI123-RIPE
auth:               PGPKEY-B06F5077
remarks:            Emergency telephone number +43 1 4277 14045 (GMT+1/GMT+2 with DST)
remarks:            http://www.trusted-introducer.org/teams/aconet-cert.html
remarks:            This is an accredited IRT (level 2)
irt-nfy:            cert@aco.net
notify:             tiirt@stelvio.nl
notify:             cert@aco.net
mnt-by:             TRUSTED-INTRODUCER-MNT
changed:            gert-henk.bakker@stelvio.nl 20030813
source:             RIPE
```



Technology: How do you create an IRT Object?

- **1A: „Roll your own“**

- Perform all your internal logistics homework
 - still using passwords?
 - PGP/GnuPG (can be clumsy in a big shop, b.t.a.d.s.)
 - X.509 (can be a can of worms, but that's a different story...)
 - Personal or Role keys? Backup? Revocation?
- Check/create the persons (or role/s) you are going to reference
- Create and submit the certificates
- Create the irt: object and submit to the database

- **1B: Become accredited by the TI-Process**

- take care of the internal logistics, submit data to TI
- have it registered for you

- **2: Tag your resource objects!**



Technology: Some more ancilliary objects

- **role:**

- Provides a mechanism to maintain contact data in **one** place

- **organisation:**

- used by the NCC, but usable everyone
- another mechanism to „tag“ stuff for easy lookup
- works across structured and unstructured resource spaces
- pretty new...

- **route:**

- to label Routing Registry entries, e.g. `route: 193.170.0.0/15`

- **domain:**

- e.g. `domain: 3.4.e164.arpa`, `domain: 171.193.in-addr.arpa`



**universität
wien**

Thank you very much!

Wilfried Wöber <Woeber@CC.UniVie.ac.at>

Vienna University, Central IT Services

Universitätsstrasse 7

A-1010 Vienna, AT

+43 1 4277 14033