The IRT Object in the RIPE Database

The direct link from IP numbers to CSIRTs

Don Stikvoort, Elsinore
Wilfried Wöber, Vienna University

vienna university computer center

Problem Outline

- Despite all high tech, wizardry and risk management in today's security handling …
- … incidents still need resolution …
- … and that still involves a lot of handwork
- Incident related questions
  - What is it
  - Where does it go to
    - And who will handle it over there
  - Where does it come from (supposedly)
    - **And who are we going to bother with it there**
  - How are we going to solve it

Problem Statement

- Given you done your job and you translated hostnames, domain names, mail addresses, checked logs etcetera, and finally you have:
- A bunch of IP addresses where the incident might be coming from (or be targeted at)
- What are you going to do ?
- How to find responsible security people who will seriously deal with what you want to give them

= *How to find the good guys to haunt down the bad guys*

Classical Solutions

- Query RIPE NCC / ARIN / APNIC / LACNIC
- FIRST member list
- Trusted Introducer repository
- Use abuse-c address
- Common mailbox names may work
- Hostmaster?postmaster?tech-c?admin-c?
- Your pile of business cards

…. messy ….. inconclusive … unreliable ….

A better solution

- Mapping CSIRT info onto the IP numberspace
- Make tools available that:
  - Take IP numbers as input
  - Give the appropriate CSIRT or CSIRTs as output
  - Give authenticity/reliability information on the CSIRT info output -- when available
- Sounds so simple …

So what happened ?

- 1994 idea by Wöber and Stikvoort
  - Possibly others too? We don't know
- Early implementation around 1995
  - Niels den Otter, CERT-NL (SURFnet-CERT today)
  - Not scalable nor maintainable
- In 2000 taken up again
- Summer 2002 "IRT object in the RIPE database":
  - RIPE technical document
  - implementation in RIPE database

Interludium

Lesson learned :

Don’t try to push things through in a hurry in the Internet, or even within a smaller organisation like FIRST --- it simply takes time … and patience … and convincing … and hard work ☺

What does the IRT object 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

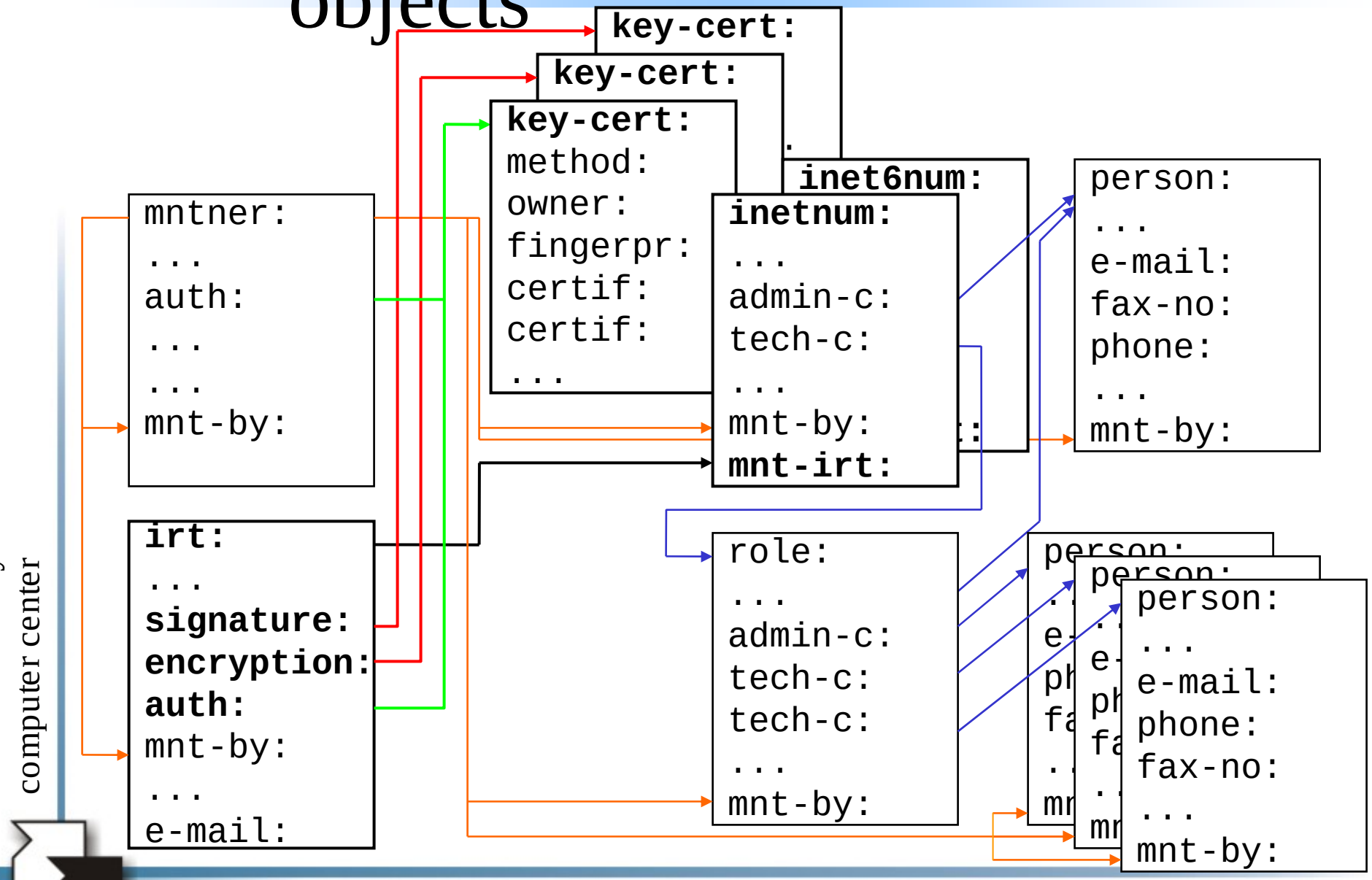
Team's PGP-key used for encryption

Team's PGP-key used to authenticate references

eMail Address to notify about references

vienna university computer center

Relationship between DB objects



How do IP numbers link to IRT objects?

```
inetnum: 192.87.106.0 - 192.87.106.255
netname: SNET-AT-SARA
descr:   SURFnet IP LAN at SARA
descr:   Amsterdam
country: NL
admin-c: SNS1-RIPE
tech-c:  NCC1-RIPE
status:  ASSIGNED PA
mnt-by:  SN-LIR-MNT
mnt-irt: irt-SURFnet-CERT
notify:  lir@surfnet.nl
changed: Derk.Reinders@surfnet.nl 20010326
changed: Rogier.Spoor@surfnet.nl 20020605
changed: Wim.Biemolt@surfnet.nl 20040422
source:  RIPE
```


vienna university computer center

And what does that yield ?

```
irt:          irt-SURFNET-CERT
address:      p/a SURFnet bv
address:      Postbus 19035
address:      3501 DA Utrecht
phone:        +31 30 2305305
fax-no:       +31 30 2305329
e-mail:       cert@SURFnet.nl
signature:    PGPKEY-A6D57ECE
encryption:   PGPKEY-A6D57ECE
admin-c:      SAM36-RIPE
tech-c:       SAM36-RIPE
auth:         PGPKEY-834125A1
auth:         PGPKEY-3D10C493
remarks:      SURFNET-CERT is the Computer Emergency
remarks:      Response Team of SURFnet
remarks:      This is a TI accredited CSIRT
remarks:      (see http://www.ti.terena.nl/teams/level2.html)
irt-nfy:      cert@SURFnet.nl
notify:       lir@SURFnet.nl
mnt-by:       TRUSTED-INTRODUCER-MNT
```


Who can create an IRT object ?

- A recognised organisation with “member teams”
  - Currently the Trusted Introducer only
  - FIRST mentioned as example in RIPE doc
  - Others can apply at the RIPE NCC
- Individual teams
- Creation/modification is done with signed messages

How reliable is an IRT object

- Please note : only *referencing* from inetnum objects makes the IRT object useful
  - Referencing depends on agreement by BOTH the local IP registry AND the IRT-object “auth” i.e. the CSIRT usually
- Value-added information like:
  - `mnt-by:  TRUSTED-INTRODUCER-MNT`
  - Further queries possible based on that
  - E.g. www.ti.terena.nl

Do people use the IRT object ?

- 14 May 2004 :
  - Europe only
  - 49 IRT objects registered
  - 7.1% of all registered IP numbers references an IRT object
- Gradually picking up now, less than 2 years after introduction

Competition

- Why not have a simple “abuse” role …
- … instead of the “complex” IRT object ??
- IRT object gaining momentum again
  - Not so complex after all
  - FAQ, technical howto available at :

    http://www.ti.terena.nl/links/documents.html
  - flexibility
  - Abuse role cannot cope with multiple-team-one-IP-range situations
  - A CSIRT is a whole other ballgame than an IP NOC

Global development

- ARIN implemented a similar mechanism
- APNIC shows interest (and uses same software as RIPE) but no action taken yet
- Only informal contacts with LACNIC thus far
- Different architectures not a problem

Unifying tools needed

- Tool that will take IP numbers as input
- Then search the RIPE and other databases for IRT objects or similar info
- Display this info with any value added info found
  - Like to the TI
  - Give click-on possibility for the value added info
- Need Webform version and sourcecode tool for integration in CSIRT processes
  - TF-CSIRT community (CERT-POLSKA and others) working on it

Thank you

Woeber@cc.univie.ac.at

&

Don.Stikvoort@elsinore.nl

Will answer questions in e-mail with pleasure (or now, the chair permitting).

vienna university computer center