Next Steps for abuse-c

Christian Teuschel, Denis Walker
RIPE NCC

RIPE 68 | Warsaw - Poland | 15 May 2014

Next Steps for abuse-c

Address validation

Contact Address Validation

- ripe-563 mandates any resource be covered by a dedicated contact for reporting abuse
  - Full coverage is nearly completed
  - Data quality can be improved
- Contact addresses are only syntactically checked, but they could be non-existent
- Validation of the contact can help increase data quality and lower frustration on the user side

Contact Address Validation

- Possible forms of validation (to be discussed)
  - Callback verification (no email is sent)
  - Send an email and check the reply
- Results of the validation can be used to:
  - Notify the resource holders privately and ask them to correct the contact in case validation fails
  - Display the validation result with the contact (e.g. in the RIPE Database, Abuse Contact Finder, etc.)

Next Steps for abuse-c

Collaboration with national CSIRTs

Collaboration with National CSIRTs

- By design, ripe-563 does not mention what can be expected if an incident is reported
- From user feedback, we see that failed attempts to report abuse are increasing
- Multiple reasons:
  - Email bounces
    - Incorrect email address
    - Technical issues (MX record, mail server, etc.)
  - Emails simply get ignored

Collaboration with National CSIRTs

- Proposed solution: provide the user with an alternative contact to the one given in abuse-c
- CSIRT = Computer Security Incidence Response Team
- “National CSIRT” = CSIRT with national responsibility
  - Network monitoring and analysis
  - Vulnerability analysis
  - Research on trends, threats, risk assessment

Collaboration with National CSIRTs

- How are we going to do that?
  - Add support to the Abuse Contact Finder tool
    - abuse-c contact will still be provided
    - Contact details to the national CSIRT responsible for the resource (RIR-Stat based)
- What can we expect them to do?
  - Analysis and assessment of the reported incident
  - CSIRT can contact team responsible for abusing network
  - CSIRT can advise and share technical expertise with affected parties (end users or network operators)

Collaboration with national CSIRTs

- Benefits
  - CSIRT can act as a pre-filter, only passing genuine cases to network operators
  - CSIRTs maintain a network to share information
    - Quick and efficient action on an incident
    - Reports can indicate trends at an early stage so prevention mechanisms can be set

Next Steps for abuse-c

Extend role Object

Extending The Abuse Role Object

- Abuse can have multiple forms:
  - Spam
  - Hacking
  - Copyright infringement
  - Other types
- The single “abuse-mailbox:” attribute in the abuse **role** object does not allow different contact addresses for various forms of abuse
- CSIRT community ask for coverage of additional abuse cases

Extending The Abuse Role Object

- Proposed solution
  - Abuse **role** object can be extended with new attributes:
    - Example: “copyright-abuse-mailbox:”

Next Steps for abuse-c

Handling More Specifics

PI Resources and abuse-c

- Currently in progress – contacting resource holders and sponsoring LIRs
- Currently 33% of IPv4 and 44% of IPv6 PI objects covered by “abuse-c:”
- Deadline is end of September 2014
- After deadline, LIRs abuse contact added to remaining PI assignments who don’t have one

Old Abuse Data Clean-up

- After PI deadline (September) clean-up starts
- Remove old “abuse-mailbox:” attributes from:
  - **person**, **organisation**, **mntner**, **irt** objects
- Remove “abuse-mailbox:” attributes from **role** objects not referenced by “abuse-c:” attribute

Handling More Specifics

- Two issues raised
  - Same organisation with different subnet abuse-c needs
  - End User organisations handling own abuse
- For subnets, propose additional “abuse-c:” in LIRs **organisation** object:

```
organisation:  ORG-LIRA-RIPE
org-type:      LIR
abuse-c:       AH9936-RIPE                      <--- default
abuse-c:       AH9955-RIPE {10.0.0.0/16}   <--- an LIR subnet
abuse-c:       AH8888-RIPE {fd30::1/64}     <--- another subnet
```

Handling More Specifics (2)

- For End Users, we propose a wizard to set up the necessary additional objects from basic info
- Wizard will also delete unnecessary objects if End User no longer handles abuse
- See RIPE Labs article for more details on both issues:
  - https://labs.ripe.net/Members/denis/suggestions-for-improving-abuse-handling

Questions?