Recommendation for publishing “Abuse Contact Information” (RIPE)

Version:	0.01
Date:	07.09.09
Editor:	Tobias Knecht abusix.org

Abstract

This document defines a recommendation for publishing abuse contact information in the RIPE Whois database. This recommendation is intended to give easy human and machine readable access to all needed abuse contact information published in the Whois records.

1. Introduction

As the abuse problem continues to expand, network operators, organizations and private people are increasingly sending abuse reports to responsible parties. However, the first step of reporting abusive behavior is to find the responsible abuse contact in the Whois Database of the RIRs. This is not as easy as it sounds. Several problems may occur within this process.

First part of the problem are infrastructure problems. Since RIRs restricting access to Whois Servers it is nearly impossible to get abuse contact information, especially for high volume reporting, of IP addresses.

The second part of the problem is on the data side. The data provided by RIPE Whois Servers are not standardized, what means that there are several ways (IRT-Object, abuse-mailbox attribute, remark and description fields) to publish one and the same abuse contact information. This makes automatic contact detection very complicated or even impossible in some special cases.

This document defines a best practice for publishing abuse contact information in the RIPE Database.

2. Intent

The recommendation defined in this document is intended for several purposes:

- Use already existent, by RIPE offered objects and attributes.
  - no infrastructure changes are needed by RIPE.
  - implementation can start immediately.
- Establish one place within the Whois Dataset, where abuse contact information can be found.
- Guarantee access to abuse contact information without restrictions by RIPE.

3. Requirements

The following requirements are necessary for publishers and the way of publishing itself:

The contact information must be both human and machine readable.
The publisher must be responsible for at least one inetnum-object.

4. Objects and Attributes

RIPE offers the so called IRT-Object (Incident Response Team Object) and abuse-mailbox attribute. The following recommendation is fully based on these already existent parameters.

The IRT-Object contains beside other for this purpose not necessary attributes an “e-mail” attribute. This “e-mail” attribute is mandatory.

In addition it is possible to add the “abuse-mailbox” attribute to the IRT-Object. The “abuse-mailbox” attribute is optional.

5. Recommendation

This document recommends the usage of an IRT-Object with an included “abuse-mailbox” attribute.

The mandatory “e-mail” attribute SHOULD be used as a contact address for CERT, Abuse Department or other responsible Security Departments.

The optional “abuse-mailbox” attribute SHOULD be used to publish the address on which abuse reports and complaints shall be received.

6. How creation works

Information about creating an IRT-Object can be found here:
http://www.ripe.net/db/support/security/irt/irt-h2.html

Information about adding a abuse-mailbox attribute to the IRT-Object can be found here:
http://www.ripe.net/db/news/abuse-implemented-20050421.html