**Anti-Abuse Working Group RIPE 83**

Wednesday, 24 November 10:30 - 12:00 (UTC+1)
Chairs: Brian Nisbet, Tobias Knecht
Scribe: Chris Buckridge
Status: Draft

A. Administrative Matters

The presentation is available at:
https://ripe83.ripe.net/archives/video/663

Brian welcomed participants and discussed administrative matters for the working group. Instructions and reminders were issued, the minutes of RIPE 82 were approved.

Brian noted that Tobias Knecht has put his name forward to carry on as a co-chair of the working group. Alireza is unable to nominate again - Brian thanked him for his contribution, and noted that this meant there were now two co-chairs (Brian and Tobias), which is fine. However, he encouraged anyone interested in being a co-chair to make that interest known.

B. Update
B1. Recent List Discussion

The presentation is available at:
https://ripe83.ripe.net/archives/video/664

Brian made an open call for any issues on the list since RIPE 82 that people would like to discuss further. There were no discussions.

C. Policies
D. Interactions
D.1. RIPE NCC Abuse Handling Training
Gerardo Viviers, RIPE NCC

The presentation is available at:
https://ripe83.ripe.net/archives/video/665

Gerardo presented an update on a training project initiated by the Anti-Abuse Working Group. This training includes awareness-raising about the abuse-c policy and on how to handle abuse complaints (perhaps leading to the development of best practices). Next steps for the RIPE NCC team include further information gathering and analysis of community needs and requirements. They are also developing a webinar, and are keen to hear feedback from the community.

Erik Bais, RIPE Address Policy Working Group co-chair, noted the purpose was really how people can get started in taking practical anti-abuse steps - this could be done in a workshop setting. He suggested the community would strongly benefit this kind of practical session and asked when this might be ready. Gerardo responded that something like this could be ready by Q2 2022. Brian suggested that a workshop at a RIPE Meeting might also be a useful approach (particularly as RIPE Meetings might attract a broader audience). Erik noted that providing people with a sandbox where they can try things out in a hands-on way is really important.

Maximilian Beiche, Irle Moser Rechtsanwälte, suggested that referring to the “abuse c” was too simplistic, and argued that the RIPE NCC should go more deeply into abuse resolution activities. Gerardo noted that the RIPE NCC’s mandate does not really extend to this, and that this currently falls to network operators. Brian also noted that this was a topic that had been discussed in great depth over the past decade (or more). Maximilian noted that he faced some recent challenges in relation to abuse, and that it is very frustrating for victims. Brian provided some background on past policy efforts that did not reach consensus, and the limitations that the community has kept in place regarding the role of the RIPE NCC.

Leo Vegoda, And Polus LLC, asked about the goal of the training and suggested that it should look at how to integrate abuse reporting into broader planning processes. Gerardo agreed that this would be a focus of the training efforts.

Pablo Nieto, IdecNet S.A., suggested that some templates for abuse reporting would be useful. Gerardo agreed that this is the kind of feedback that the RIPE NCC is looking for - would the community find this a useful outcome of these efforts?

Yuriy Bogdanov, IP4MARKET, noted that the RIPE NCC’s role should be limited to maintaining a correct registry, but agreed that the Anti-Abuse Work Group could help develop best practices for how to manage abuse reports.

Niall O’Reilly, RIPE Vice Chair, noted that we should not marginalise some who might be interested in abuse-handling training by focusing exclusively on LIRs - all of the community should be in focus here.

D.2. RIPE Database Purposes in the 2020s and Beyond
Denis Walker

The presentation is available at:
https://ripe83.ripe.net/archives/video/666

Denis discussed the work of the RIPE Database Requirements Task Force, which is now being followed up by the RIPE Database Working Group. Ongoing work includes discussion of what the RIPE Database purposes are now (in the 2020s) and looking ahead. In this session, Denis sought feedback from people handling and managing abuse issues, and asked what people in those roles need from the RIPE Database. He noted that this is not about inventing new purposes, but about documenting existing, but perhaps undocumented or undefined purposes and uses of the database. He asked whether “abuse issues” should be a specifically defined purpose, or whether these can fall under a broader “agreed Internet operational purposes” category, and argued that we need a new consensus on these issues.

Mirjam Kühne, RIPE Chair, thanked Denis, and noted that the task force has just published its report (with various recommendations, that it is presenting). She suggested trying to keep this discussion in the context of the task force’s work, rather than starting a new discussion. Denis noted that there hasn’t been an open community discussion of the database purposes since 2011 and that some of the task force recommendations will require some additional consensus on “new” (or newly documented) purposes. Mirjam strongly urged everyone to read the task force report. Brian agreed that this task force should not be duplicating the work already ongoing in other working groups.

Rüdiger Volk, representing himself, asked about the difference between “purposes” and “requirements”. Denis suggested that the task force took the purposes and built out recommendations regarding requirements and that he is now opening a discussion about the purposes themselves.

Shane Kerr, member of the RIPE Database Requirements Task Force, noted that the task force report is discussed in the (upcoming) RIPE Database Working Group, but agreed that there is a strong argument for revisiting the constraints that past discussion might have placed on the agreed purposes of the RIPE Database. Denis also noted that some of the purposes previously discussed (“agreed Internet operational purposes”) can be quite ambiguous. Shane also noted that there is limited community energy, so it’s important to use that energy wisely.

Niall O’Reilly urged caution in thinking there will ever be a closed list of purposes - this should be a list that evolves to meet the purposes and goals set by the community for itself. Jordi Palet Martínez, Moremar - The IPv6 Company, strongly agreed with this point.

E. Presentation
E.1. The Hijackers Guide to the Galaxy: Off-path Taking over Internet Resources
Tianxiang Dai, Technische Universität Darmstadt

The presentation is available at:
https://ripe83.ripe.net/archives/video/667

Tianxiang presented on his group’s recent research on abuse activities that involve taking over various types of “Internet resources” (including IP address, domains, digital certificates and computing resources). This includes examples of how each of these resources can be taken over and what attackers can achieve via these strategies.

Cynthia Revström, representing herself, asked about the reference to “being able to issue certificates”; Tianxiang noted that if taking over a resource, it might be possible to re-issue other certificates.

Brian asked whether the researchers were seeing a lot of cases where 2FA is not required. Tianxiang noted that in many cases they’d looked at, 2FA was disabled by default. Brian urged everyone to use 2FA, if they’re not already using it.

Rüdiger Volk noted that for RPKI, the hosted RPKI at the RIPE NCC does not allow you to deal with certificates, but security is limited by the security of the LIR Portal (which does not require 2FA). He noted that accounts in the LIR Portal are not publicly documented in the RIPE Database, and may be handled with different addresses in the non-public registry. Tianxiang agreed, but noted that many providers do not hide user information so well - he urged operators to look at how well protected their user information is.

Gert Doering, SpaceNet AG, noted that 2FA is not a perfect solution, and can cause user issues when changing/upgrading mobile devices.

Marco Schmidt, RIPE NCC, clarified that getting access to a RIPE NCC SSO account will not be sufficient to perform significant actions like transfer resources, modify sensitive LIR organisation details or close LIR accounts, and that the RIPE NCC has additional due diligence checks in place to prevent this. He noted though that it is still important to have a strongly protected SSO account and the RIPE NCC urges all members to do so. Tianxiang agreed, but noted that some providers seek to make things easier for their users, which carries a risk of greater vulnerabilities. In response, Cynthia Revström noted that her experience of uneven ticket handling at the RIPE NCC makes it a fair question. Theodoros Polychniatis, RIPE NCC, also noted that the current RIPE NCC Access solution is limited, but there are plans to review it in 2022 and provide more authentication options.

Emile Aben, RIPE NCC, suggested that the presentation seemed to say that all RIRs are vulnerable to prefix hijacking; however, RPKI deployment should make this hard, if not impossible. He asked whether the team tested this, or is it a theoretical possibility of doing this? Tianxiang replied that the limited deployment of RPKI meant that prefix hijacking remained a notable threat.

Denis Walker argued that security issues should not be public in the RIPE Database (security mechanisms, approaches, etc.), and that this practice should be looked at by the community.

Christian Bretterhofer, Andritz AG, noted that registration information should be public and is needed for operations.

Yuriy Bogdanov asked what the RIPE NCC does in case of prefix hijacking in its service region. Emile Aben noted that the RIPE NCC is not the Internet police, but does provide transparency via the Routing Information Service (RIS), which can help people understand what is happening if a hijacking takes place. Erik Bais noted that there are policies and processes in place to handle disputes over registration of resources.

X. A.O.B.

The presentation is available at:
https://ripe83.ripe.net/archives/video/668

Brian sought (and obtained) the working group’s explicit support for Tobias continuing as a co-chair.

Z. Agenda for RIPE 84

Brian asked people to consider possible agenda items for RIPE 84, and expressed his fervent hope that it would be a hybrid (physical/virtual) meeting in Berlin.