

Team Meeting

26 January 2021

Attendees

Tim April

Gavin Brown

Merike Kão (coordinator)

Rod Rasmussen

Marc Rogers

Katrina Sasaki

Robert Schischka

Duane Wessels

Sally Newell Cohen (ICANN support)

Heather Flanagan (ICANN support)

Steven Kim (ICANN support)

Wendy Profit (ICANN support)

Samaneh Tajalizadehkhoob (ICANN support)

Regrets

John Crain

Agenda

Session 1:

1. Briefly review the Vector of Attack priority list
2. Presentation from Individuals
3. Discussions on presentations

BREAK (TBD)

Session 2:

1. Continue discussions on presentations

2. Discuss and document commonalities in attack vector mitigations
3. Identify main gaps
4. Discuss unique characteristics that attracts security problems

Note: Link to the working document will be shared via Slack.

Notes

1. In between the two workshops, each TSG member was assigned two attack vectors from those identified by the members in the previous sessions based on the TSG charter. Each TSG member researched known mitigation techniques and the deployment gaps associated with each attack vector, as an assignment.
2. During the meeting, the TSG discussed the attack vector assignments.
 - Having explored various attack campaigns on previous calls and in the previous workshop, the TSG continued their conversation regarding the different attack vectors (e.g., Impersonating Recursive Resolvers, TTL issues, Vulnerability Exploitation, Fate Sharing, and Protocol Weaknesses), and their relation with other attacks.
 - Within the discussion of each attack vector, the TSG members then went one step further and began to answer questions from the charter:
 - Known mitigation techniques associated with the attack vector.
 - Gaps in techniques and deployment.
3. **Next steps**
 - The TSG will start discussions on what should be captured in the final report.

Action Items

1. ICANN org support staff will pull together an outline for the report.
2. ICANN org support staff will go through the currently identified attack vectors, mitigation strategies and gaps and complete the three remaining ones that were briefly discussed but were not fully completed by the TSG members in the two dedicated workshops.
3. ICANN org support staff will go through all the attack vector synopsis and add information to the known mitigation techniques as well as gaps, if and where need be.