LACIGF 12 Report

Title of the session: Session 8 – Fragmentation of the Internet: Protecting Encryption and Anonymous Communications

Session summary:

Session 8 approached the use of cypher, starting with a technical introduction and then a discussion of topics like cypher regulation and gender inclusion in cryptography.

The first panellist, **Nathalia Sautchuk (Internet Society Brazil, Brazil),** make a technical presentation about cypher. Firstly, she presented the main uses of cypher nowadays: instant messaging apps, e-commerce and Internet banking. Then she proposed a definition for cypher, based in concepts of clear text, ciphertext, key and algorithm. According to her, there's no cypher algorithm 100% safe, but it's possible to reach algorithms computationally secure, considering the time and cost needed to break the cryptography. Besides, Nathalia pointed out that obscurantism is not the best way of having security. So she categorized some cypher algorithms, taking into account the number and kind of keys (symmetric or public), operation mode (substitution or transposition); and processing mode (block or stream). Finally, she mentioned three points to be considered when assessing apps security: whether it has an open-source, end-to-end cypher and forward secrecy.

The debate moderator, **Adela Goberna (ALAI, Argentina)**, thanked Nathalia for her presentation and proposed the following questions: "What are the technical principles of cypher?" and "What is its cost-benefit?".

The panellist **Veridiana Alimonti (EFF, Brazil)** answered mentioning the security attributes of cypher: confidentiality, integrity and authenticity. So, she argued it's possible to use cypher for promoting human rights like freedom of expression. However, she raised the question about how cypher should be regulated, given that an inappropriate regulation could allow for human rights violations.

Daniela Macías (National Direction of Public Data Registry, Ecuador) commented that one of technology's key elements is communication, so we should ensure it is safe. This could be possible, for example, by using the cypher. She also pointed out the importance of initiatives for creating rules regarding cypher, making sure they do not disrespect any human rights standards. Finally, she mentioned cypher is crucial for ensuring personal data protection, therefore we should use other tools together, because cypher is not enough per se.

María Cristina Capelo (Facebook, Mexico) began by saying end-to-end cypher is important for privacy and security, but it's not a perfect technology, so it's necessary to have a social balance. She said WhatsApp uses end-to-end cypher by default, and Messenger offers the possibility of enabling end-to-end cypher. Besides, she argued that all users should be free to choose the platform they want to use. That's because any hacker will exploit any breach and the use of some functionality could create a vulnerability (for example, making a security copy in the cloud may put the cypher at risk).

Angélica Contreras (FemHackPartyLAC and Women SIG, Mexico) focused her speech in matters of gender inclusion in the use of cypher. She said many women are victims of violence and vigilance in the digital environment, so that using cypher may prevent these situations. Last, she mentioned the challenges of digital literacy and linguistic inclusion, given that many cryptographic technology sources are not written in Latin-American languages. Such a lack of linguistic diversity is an obstacle for promoting digital inclusion.

Outputs and other relevant links:

- Full session: https://youtu.be/8TJIzVp_yjE
- Nathalia Sautchuk presentation: https://www.slideshare.net/nathaliapatricio/conceptos-fundamentales-sobre-el-funcionamiento-y-la-utilidad-del-cifrado

By: Gabriel Arquelau Pimenta Rodrigues (Universidade de Brazilia, Brazil), Flavio Andre Garces Heredia (Colombia)

Translation: Giovana Pertuzzatti Rossatto (UFRGS, Brazil)

Revision: Pablo Jordan (Internet Society Bolivia, Bolivia) e Luis Gustavo de Souza Azevedo (UFAC, Brazil)

Coordination and edition: Nathalia Sautchuk Patrício (NIC.br, Brazil) and Guilherme Alves (Youth Observatory, Brazil)