IGF 2015 Brazil, Joao Pessoa (November 2015)

REPORT:
Workshop 141 - Law enforcement in a world pervasive encryption

Report by: Nicolas Seidler, with input from Jairus Pryor

Organiser: The Internet Society

Moderator: Nicolas Seidler, Policy advisor, the Internet Society
Speakers

- Mr. Frank Pace, Sergeant, Digital Forensics Investigative Unit, Strategic Information Bureau, Phoenix Police Department
- Mr. Ted Hardie, Executive Director, Internet Architecture Board
- Ms. Carly Nyst, civil society, former Privacy International, international privacy expert
- Mr. Michael Nelson, Internet-related global public policy issues, CloudFlare
- Ms. Sanja Kelly, Project Director, Freedom on the Net report
- Ms. Xianhong Hu, intergovernmental, Division for Freedom of Expression and Media Development, Communication and Information Sector, UNESCO

Summary of discussion

- The session focused on the broader and growing interest in the use and the availability of encryption solutions, particularly those that provide end-to-end protection.

- The question posed to the forum focused on how to reasonably achieve public policy objectives such as law enforcement/national security in the scenario of a world where encrypted Internet traffic is the norm.

- Key issues highlighted by the panelists included: How long it will take until encryption is reasonably ubiquitous, the moral and ethical differences between targeted and pervasive surveillance, the role of traditional law enforcement mechanisms in combating criminal activity which uses encrypted communications, and how to build encryption systems that the public can trust.

- All panelists agreed that there is both a need to ensure the security of citizens and to protect the confidentiality of online communications. Views diverged however on whether exceptional access for governments to encrypted material, which is generally requested by law enforcement agencies to facilitate their work, would be effective, technically feasible and proportionate.

- Many speakers agreed that drivers that could lead to a world of pervasive encryption could include public scandals that could trigger policy change (e.g. broad legislation restricting encryption, CEO or political figure being victime of hack due to weak encryption, similar cases to US Office of Personnel Management data hack). Pull factors could include companies further deploying end-to-end encryption as a competitive advantage to foster customer trust.

- An important distinction was made between what law enforcement does in the investigation of specific crimes and what intelligence services might do as a matter of bulk data collection and the interception of signals, whether that be encrypted or not, for the use of objectives that are different. Crime investigation would usually focused on data at rest (mobile device, computer, etc).

- The discussion raised the fact that while full access to unencrypted data would likely make LEA's job easier, there are alternative means that law enforcement can use, and is using, to target criminals. This includes targeting other parties that are involved in crimes, using metadata to track patterns and relationships, and the employment of malware in exceptional cases. However, all these means usually require extensive legal thresholds for their use. Some raised that the increasing number of connected objects will also offer LEA with new means to investigate crimes (while also raising further privacy concerns). It was also raised that technological means may not always replace investment in employing human intelligence. A related point was made that there should be a similar level of barriers that were there before the Internet when it comes to intrusion in people's privacy to investigate crimes. Social practices should not change as a result of technical aspects.

- Several voices raised questions on whether it would be possible for governments to have exceptional access to encrypted material, as there does not seem to be an effective and widely acceptable solution currently. Technical insights indicated that strong encryption with forward secrecy would likely be unbreakable. However, data sitting at rest usually needs some credentials that could be retrieved from a device. Example was given about banks that are required to build their data systems in ways that will support law enforcement when requested.

- In addition, it was highlighted that many countries actually use national security arguments as a way to censor information and track political dissent, so it is important to contextualize the debate on the understanding that exceptional access to encrypted material, assuming it was possible and desirable, might sometimes be used in ways that will explicitly restrict fundamental rights, including freedom of expression.

- Eventually, with the likelihood that encryption will more widely spread and available in the next 5 to 10 years (with possible different types of encryption at different layers), a key conclusion from the workshop was that the debate should

also focus on building new trust frameworks between law enforcement and citizens. A suggestion was made that the vision of a world with encryption by default (that protects users' confidentiality and trust) could be compatible with systems where citizens could have the opportunity to contribute to community efforts towards crime prevention.