Roles and responsibilities in an encrypted world

PROMPT

Right now, law enforcement and intelligence agencies around the world are mining data, re-routing internet traffic, and hacking into devices and systems, sometimes on a mass scale. While these tactics may present an alternative to undermining encryption, they each come with their own costs, including serious costs to human rights. Discussants in this track will explore without prejudice the rumored, public, or potential methods and tools that are available to government surveillance agencies; where and how they are explicitly authorized; their costs and benefits; and high-level safeguards that need to be in place if they are carried out.

DISCUSSION LEADERS

Jamie Tomasello, Access Now

Shauna Dillavou, Community Red

WORKSHOP LEADERS

Joe Hall, CDT

Pranesh Prakash, CIS India

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

Key Outcome: Identified a structure by which to compare the relative value of alternatives to mandated access. Identified factors to compare these techniques and applied these factors to government hacking as a case study.

This session began by identifying stakeholders and cataloguing tools and techniques used to undermine encryption. We attempted to determine the needs (one and two) as well as the gaps of each stakeholder. We then identified 24 techniques to undermine strong encryption.

In the workshop, we identified guiding principles for the use of alternative methods of obtaining access to encrypted data. First, we listed a set of factors that governments and law enforcement can and should consider before engaging in an alternate technique to undermine encryption. An example was "resources." To what extent does a given technique require significant budget commitment or equipment outlays? "Possible unintended consequences" was another example. Would a particular technique potentially risk the security of a number of innocent people to get to one person? We identified 14 factors.

We then compared each of the factors to the list of techniques identified during the discussion portion. We used these factors as a lense to compare each of these techniques and determine whether one factor was better than another. Using "lawful government hacking" as an example technique, we tested several of the factors.

Applying Factors to Lawful Hacking

For "lawful government hacking" we identified critical steps. We first noted that law enforcement must obtain a warrant that is as specific as possible, approved by a high-level government entity, and authorized by an independent judge. Then, we considered, without coming to a concrete conclusion, whether law enforcement must disclose the vulnerability to the company and any defendant that evidence was obtained against. There was consensus that evidence obtained should not be used in a court to convict a suspect because it would not meet evidentiary standards. For example, if you deliver malware code over an unencrypted connection, you don't know whether a third party is corrupting the data or otherwise manipulating data. Finally, we considered definitions of appropriate transparency. As a real-world analogue, we know when law enforcement breaks into a home using a battering ram. However, we may not know which "Network Investigating Techniques" are used.

Roles and responsibilities in an encrypted world

PROMPT

Right now, law enforcement and intelligence agencies around the world are mining data, re-routing internet traffic, and hacking into devices and systems, sometimes on a mass scale. While these tactics may present an alternative to undermining encryption, they each come with their own costs, including serious costs to human rights. Discussants in this track will explore without prejudice the rumored, public, or potential methods and tools that are available to government surveillance agencies; where and how they are explicitly authorized; their costs and benefits; and high-level safeguards that need to be in place if they are carried out.

DISCUSSION LEADERS

Jamie Tomasello, Access Now

Shauna Dillavou, Community Red

WORKSHOP LEADERS

Joe Hall, CDT

Pranesh Prakash, CIS India

Discussion/workshop leaders did not review this report. Statements should not be considered the opinion of discussion leaders or workshop leaders unless stated otherwise.

SPECIFIC OUTCOMES

Identified **24** techniques or alternatives to obtain encrypted data.

- Targeted and bulk "lawful" hacking
- Metadata analysis
- Social graph analysis
- Compelled decryption
- Physical intrusion
- Human intelligence
- Black bags
- Extralegal decryption
- Subpoena/Legal process
- Social engineering
- Stealing keys/certificates
- Informants
- Legal/Court mechanisms
- Crypto-analysis
- Brute force
- Creating backdoors
- Not encrypting
- Undermining infrastructure
- Underseas fibers
- Exploiting global networks (getting data overseas)
- Spoofing target
- Man In The Middle attacks
- Impersonation
- Exploit supply chain vulnerabilities

Identified **14** factors by which to consider alternate techniques to obtain encrypted data.

- Severity of the crime
- Necessity of employing the technique
- Proportionality of the crime compared to the severity of the technique
- Credibility of evidence
- Legality of the alternative
- Potential for unintended consequences
- Nature of unintended effects
- Balance of equities
- Resources required
- Broadness (targeted or bulk)
- Abuse — to what extent could the technique be abused once created
- Oversight and accountability
- Efficiency
- Viability

FUTURE WORK

Comparing all **14** factors to all **24** techniques, and ranking these techniques.

Further discussion to examine appropriate disclosure and transparency standards.

This event is brought to you by
accessnow

Access Now (accessnow.org) is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, visit https://www.accessnow.org/crypto-summit-2-0/
or contact Nathan White (nathan@accessnow.org) & Amie Stepanovich (amie@accessnow.org)