THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 4

Busting barriers: Identifying and conquering the obstacles to widespread adoption of encryption

PROMPT

Encryption is well known as the best and most reliable (though not completely reliable) way of protecting sensitive data. However, too few companies are using it, and they are implementing it only sporadically, and sometimes in outdated forms. This track will explore why that is, and what the best ways may be to overcome the barriers and move toward a future where encryption, particularly for our most sensitive data, is ubiquitous.

DISCUSSION LEADERS

Kevin Bankston, New America's Open Technology Institute

Carolina Botero, Karisma

WORKSHOP LEADERS

Julian Sanchez, Cato Institute

Nick Grossman, Union Square Ventures

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: A short list of fundable projects that could overcome real-world barriers to the expansion and adoption of encryption.

In this track, we examined the barriers to widespread deployment and adoption of encryption. We broke up the discussion between deployment of end-to-end encryption, full disk encryption, and deployment of internet traffic encryption.

There were no shortage of barriers for encryption, including obvious political and legal barriers. However, we decided that solutions to these barriers were out of scope for our work and already being discussed in detail elsewhere.

Barriers also exist in technical performance issues. Simply stated, we need faster chips so that even the cheapest Android phones can encrypt and decrypt on the fly without causing huge performance problems.

User interface and usability is another barrier for the adoption of encryption. Unfortunately, encryption and device security has not been a significant commercial differentiator. We looked at examples suggesting that the most successful and widely adopted encrypted products are those that the consumer don't even know are encrypted, such as the WhatsApp service or default encrypted smartphones. There are also tradeoffs when it comes to key management. Simple, transparent key management gives the user little control and poses authentication problems. However, more secure key management systems can be harder to use.

In this track, we chose not to try to address problems we would not be able to solve within the session, e.g., we cannot makes chip faster. Instead, we tried to identify things that the people in this room could significantly impact with modest funding.

A SHORT LIST OF FUNDABLE PROJECTS

Advocacy:

- Campaigns to get platforms and apps to ship with encryption turned on by default. This could be end-to-end or simply full disc encryption.
- Apples-to-apples comparison guides for how various applications handle security issues as a whole.
- "Walls of Shame" about breaches and security.
- Conduct a survey of state and local governments to identify where they stand on HTTPS and other data management practices. Identify the universe of policy options currently under consideration by state, local, and other national governments.
- Take the federal government's "HTTPS Everywhere" program and campaign state and local governments to adopt.

THE CRYPTO SUMM1T 2.0

BROUGHT TO YOU BY ACCESSNOW.ORG

OUTCOMES REPORT TRACK 4

Busting barriers: Identifying and conquering the obstacles to widespread adoption of encryption

PROMPT

Encryption is well known as the best and most reliable (though not completely reliable) way of protecting sensitive data. However, too few companies are using it, and they are implementing it only sporadically, and sometimes in outdated forms. This track will explore why that is, and what the best ways may be to overcome the barriers and move toward a future where encryption, particularly for our most sensitive data, is ubiquitous.

DISCUSSION LEADERS

Kevin Bankston, New America's Open Technology Institute

Carolina Botero, Karisma

WORKSHOP LEADERS

Julian Sanchez, Cato Institute

Nick Grossman, Union Square Ventures

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

Connecting Security with Design:

- Host a security bootcamp for designers.
- Work on open source design for security toolkits.
- Conduct UX studies into how users respond to information about security. (For example, studying the effect that using colored address bars or other representations of security have on users.)

Education:

- Encryptionary.com - Urban dictionary for encryption. An illustrated guide to complex security topics to make them easier to understand (already under development; needs funding).

Other sectors/industries that manage sensitive data include the legal, healthcare, and education sectors. Organizations in these sectors may not be steeped in best practices. **Fundable projects to improve security here include:**

- Develop a professional code of ethics for managing sensitive data, for example, a "hippocratic oath" for data and security.
- Develop checklists for professionals for managing cryptographic protocols and handling client data.
- Identify and fund individuals who can act as "Johnny Cryptoseeds" — advocates who will find opportunities to educate people and activate these industries. We've seen this in the library and media space, but not in other critical areas.

Barriers to End-to-End Encryption:

- Cost - ISPs do not know how to transfer the cost to consumers
- End-to-end can be difficult to use, which creates a "first mover" problem
- Lack of industry-wide standards
- Key distribution
- Political threats
- Trust of users
- Heterogeneity of platforms

Barriers to Full Disk Encryption:

- Recoverability/Back up
- Key storage
- Defaults
- Performance
- Cost
- Access to data for enterprises
- Confusing terms
- "Settings risk"

Barriers to Encrypting Internet Traffic:

- Enterprise private networks
- Lack of transparency
- Compatibility with third party content
- Lack of government leadership
- Latency
- Hardware/Software upgrades necessary
- Cost to implement

This event is brought to you by accessnow

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