Protecting Cryptography Against Compelled Self-Incrimination

Authors:
Sarah Scheffler and Mayank Varia, *Boston University*

Abstract:
The information security community has devoted substantial effort to the design, development, and universal deployment of strong encryption schemes that withstand search and seizure by computationally-powerful nation-state adversaries. In response, governments are increasingly turning to a different tactic: issuing subpoenas that compel people to decrypt devices themselves, under the penalty of contempt of court if they do not comply. Compelled decryption subpoenas sidestep questions around government search powers that have dominated the Crypto Wars and instead touch upon a different (and still unsettled) area of the law: how encryption relates to a person's right to silence and against self-incrimination.

In this work, we provide a rigorous, composable definition of a critical piece of the law that determines whether cryptosystems are vulnerable to government compelled disclosure in the United States. We justify our definition by showing that it is consistent with prior court cases. We prove that decryption is often *not* compellable by the government under our definition. Conversely, we show that many techniques that bolster security overall can leave one more vulnerable to compelled disclosure.

As a result, we initiate the study of protecting cryptographic protocols against the threat of future compelled disclosure. We find that secure multi-party computation is particularly vulnerable to this threat, and we design and implement new schemes that are provably resilient in the face of government compelled disclosure. We believe this work should influence the design of future cryptographic primitives and contribute toward the legal debates over the constitutionality of compelled decryption.

Open Access Media

BibTeX

Scheffler PDF | Scheffler Paper (Prepublication) PDF | View the slides

Presentation Video

ATTEND

Registration Information
Student Grant Application
Diversity Grant Application
Grants for Black Computer Science Students Application

PROGRAM

Technical Sessions
Summer Accepted Papers
Fall Accepted Papers

PARTICIPATE

Call for Papers
Submission Policies and Instructions
Call for Artifacts
Artifact Evaluation Information
Instructions for Presenters
Hack@Sec

SPONSORS

Sponsor Events
Sponsor and Exhibitor Info

ABOUT

Symposium Organizers
Past Symposia
Conference Policies
Code of Conduct
Questions