# Key Sharing in the HTTPS Ecosystem

**PIs:** **Dave Levin, Tudor Dumitraş** — University of Maryland
**Alan Mislove, David Choffnes, Christo Wilson** — Northeastern University

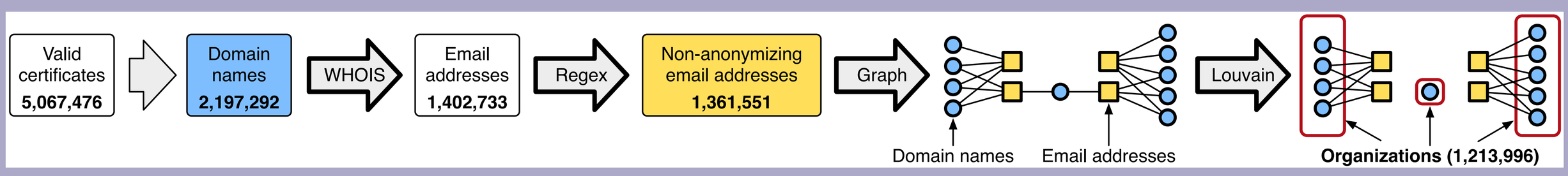
Code and data available at: `securepki.org`

**HTTPS** content is often hosted by third parties such as **CDNs**

To do this, **websites share their private keys**, violating basic assumptions

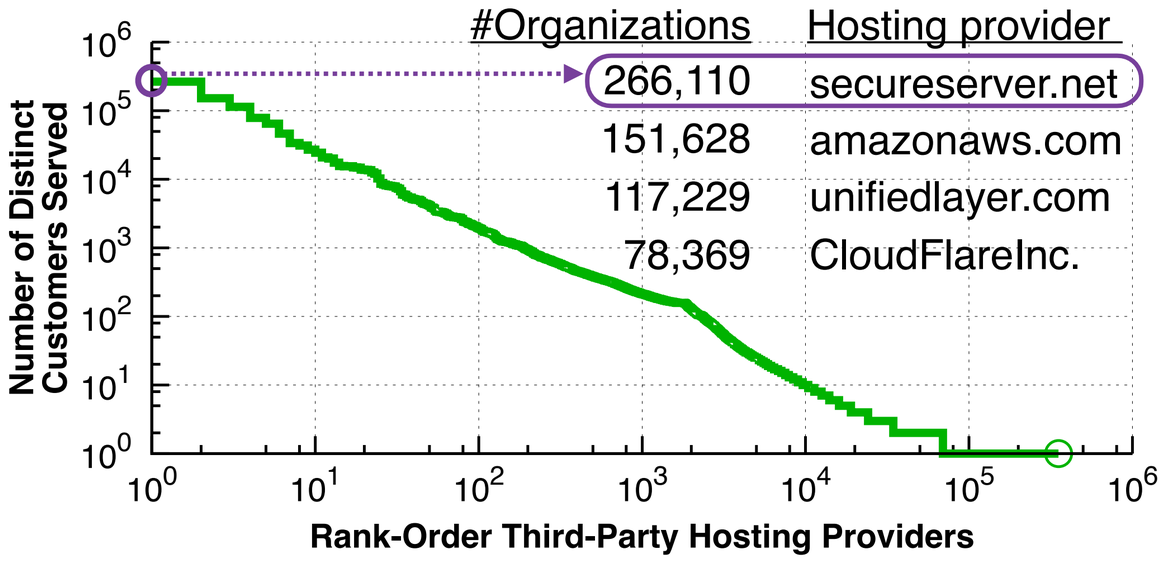
**Our objective: Measure** the *extent* and *impact* of key sharing in the web

## Method: Inferring organizations from whois

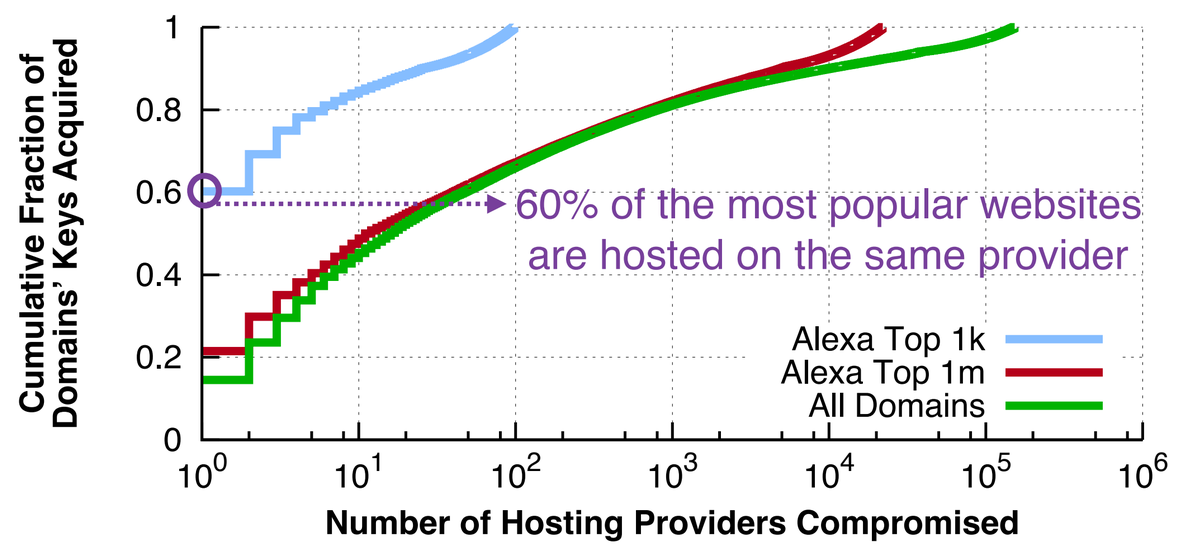



## The extent of key sharing in today's PKI

**Some hosting providers have *hundreds of thousands* of other organizations' keys**

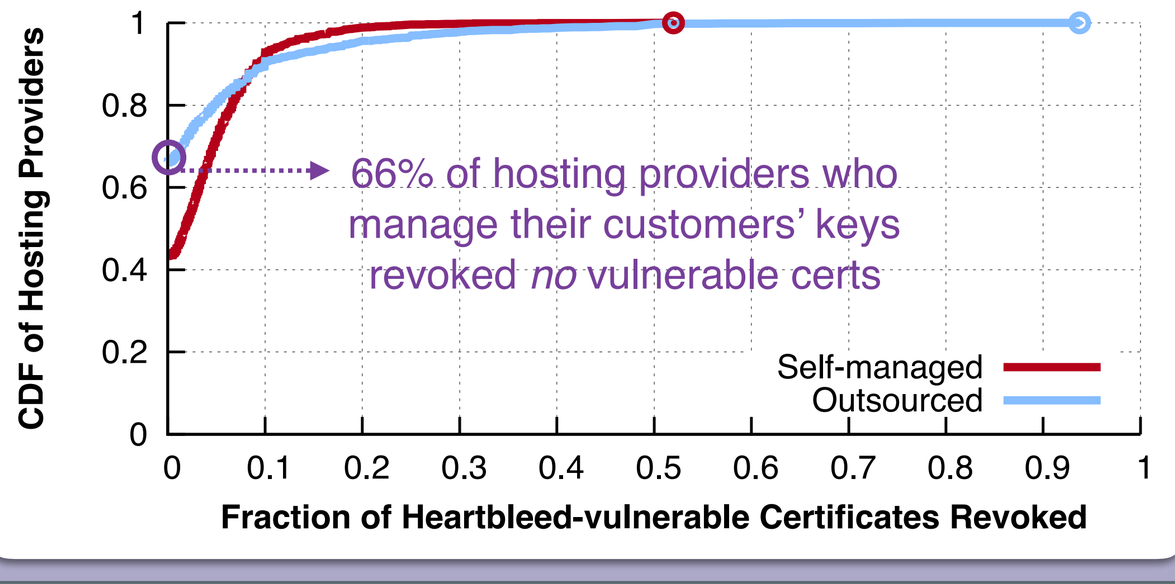



**Compromising 10 hosting providers could yield 40% of *all* private HTTPS keys**

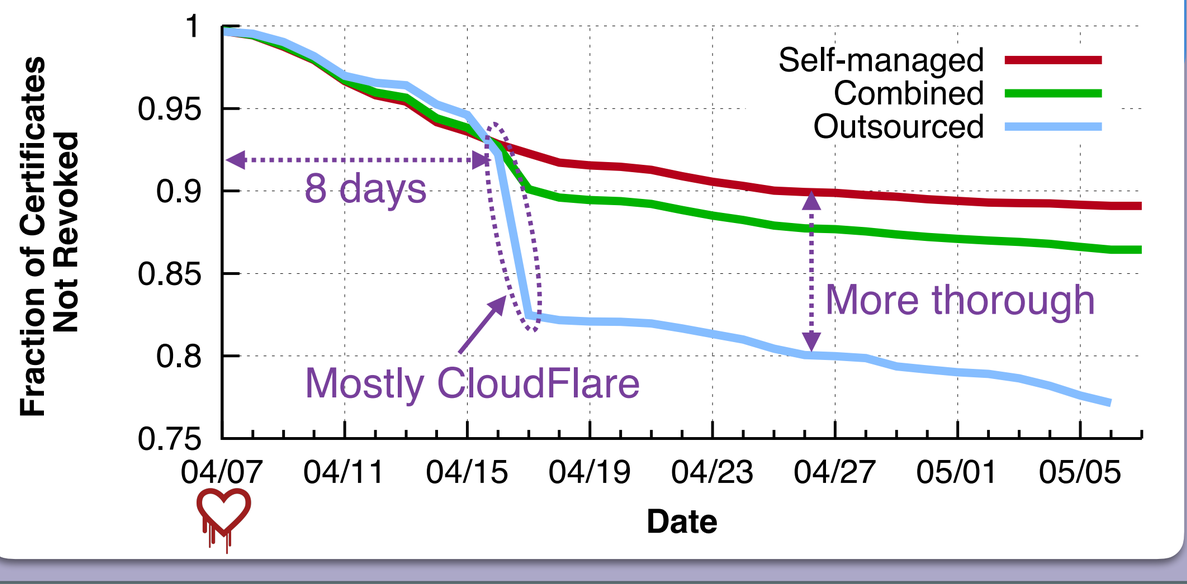



## The impact of key sharing on certificate management

**Certificates managed by third-parties tend to have slightly better revocation rates**




**Third-party hosting providers are *slower* to react, but ultimately *more thorough***




Interested in meeting the PIs? Attach a post-it note below.

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN