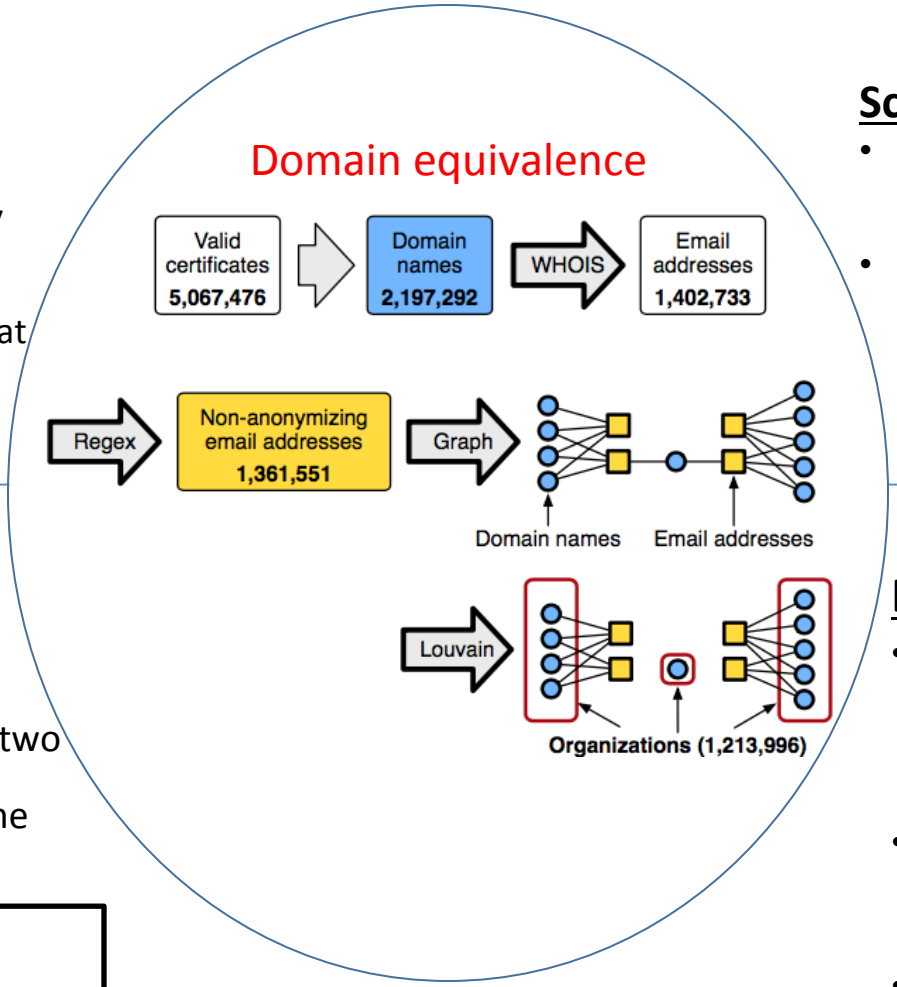
Measuring Key Sharing in the HTTPS Ecosystem

Challenge:

- Sharing private keys threatens the security of the web
- How can we measure its *extent* and *impact* at scale?

Solution:

- Analyze web-wide certificate scans
- New technique to determine whether two domain names are operated by the same organization



Scientific Impact:

- Exposes hidden trust assumptions in the web's public key infrastructure
- "Domain equivalence" technique is broadly applicable to understanding business arrangements on the web

Broader Impact:

- Quantifies an unknown centralization of trust in third-party hosting providers
- Presented to CDNs and working with them to find an alternate design
- Undergrad lead author

CNS-1564143 and CNS-1563320

Dave Levin, Tudor Dumitraş (UMD)
Alan Mislove, David Choffnes, Christo Wilson (NEU)