Measuring and Improving the Management of Today's PKI

Motivation:

- **A SSL certificate** is to secure communication channel
- Prior studies ***almost exclusively*** focus on *valid* certificates
- How's the rest of the SSL ecosystem?

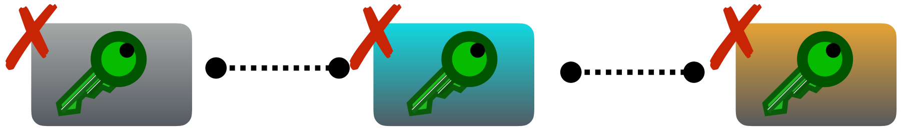
Analysis:

- Validate ***all certificates*** from IPv4 spaces
- 88% of certificates are ***invalid*** and reissued regularly
- They can be ***grouped together*** and used to track devices

Project Number	CNS-1563320
Institution	Northeastern University
Contact	amislove@ccs.neu.edu

HTTPs (Secure Communication)

(1) 88% certs are invalid reissued on a regular basis
(2) They are mostly from end-user ISPs



Multiple different certs can be linked by grouping a shared field (e.g., public key)

Devices can be tracked as they are moved in IP/AS space

Scientific Impact:

- Research community needs to focus on not only valid certificates but also ***invalid ones***
- SSL ecosystem has significant *management* problems, exemplified here

Broader Impact:

- The SSL ecosystem secures most common internet protocols; improving it improves security for millions of users
- *Management* is often-overlooked, with significant issues caused by poor practices and hard-to-manage certificates