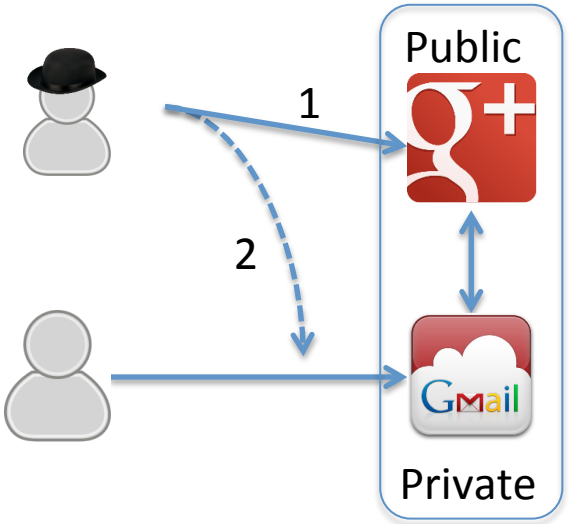
Length Hiding Padding for TLS

draft-pironti-tls-length-hiding-01

Alfredo Pironti
alfredo.pironti@inria.fr
Nikos Mavrogiannopoulos
nmav@gnutls.org

IETF 87 - Berlin

An example problem: Identifying web users



- TLS does not protect message length
- Each profile picture has a different size
- The attacker learns the username

- For every 1000 users: 83% can be uniquely identified
- Similar issues for other protocols
  - At least XMPP, SMPT

A simple fix: Padding

- Pad privacy-sensitive data
  - *How much* to pad?
    - Application-specific privacy policy
  - *How* to pad?
    - TLS can do that once for all applications
    - Ensure there are no timing leaks *(fixes legacy block ciphers!*)
- Similar to encryption
  - Application security policy
    - Encryption: always on; prefer on; prefer off
  - How to encrypt? Use TLS

Roadmap

- Running code ✔
  - GnuTLS – http://www.gnutls.org/
  - miTLS – http://mitls.rocq.inria.fr/
  - Prototype Apache module
- **Discussion**
  - Default in TLS 1.3?
  - Extension?
    - Save bandwidth for non-privacy concerned apps
- Adoption as WG draft