Wireguard: A Modern VPN Protocol

Jinank Jain, Rayhaan Jaufeerally

May 15, 2018

ETH Zürich

Introduction

Why VPN?

- Necessary for point to point security between campuses (e.g. DC's, corporate offices, . . .)
  - As early as the 1970's governments have tapped undersea cables for intelligence,
  - Operation Ivy Bells in 1971 tapped Russian communicatioons to millitary bases[1],
- Necessary for end users to get a clean connection:
  - ISP's doing DNS hijacking to serve inappropriate content,
  - Open WiFi networks when travelling,
  - Geoblocking,

[1] https://en.wikipedia.org/wiki/Operation_Ivy_Bells

Necessity in real life

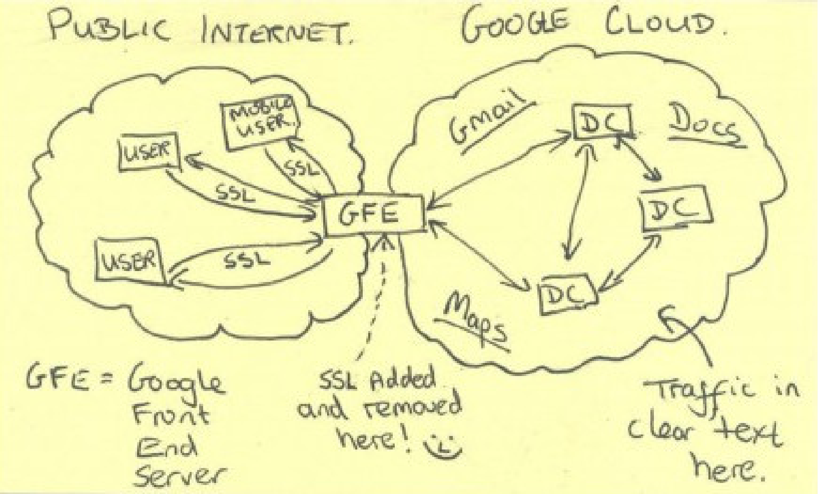
PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
SSL
GFE
Gmail
Docs
DC
DC
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! :)
Traffic in clear text here.

Figure 1: Government attempts to intercept user's content

History of VPN protocols

- IPSEC
    - Popular for site to site connections with dedicated router hardware,
    - Tedious to set up and high degree of complexity,
    - Large attack surface between IKE (v2), SA mechanisms, XFRM in Linux,
    - Legacy protocol support,
- OpenVPN
    - Implemented in userspace with TUN/TAP (slow),
    - Complex confoguration vulnerable to leaks,
    - Stateful protocol which is brittle in real networks,
    - Large codebase / attack surface,