Big Aggregation and Intermediaries: threat or menace?

Jan Seedorf, Eliot Lear, Joe Hildebrand, Barbara Fraser
(Moderated by Barry Leiba)
One take on the problem

• Most Secure Communication Protocols have been designed with strict end-to-end security in mind
  – No intermediary entity on the path is supposed to read or modify communications exchanged over these protocols
  – This is the security paradigm behind the design of TLS, IPSec, ...
    • Valid at the time when these protocols were designed

• Reality has significantly changed since the design of these protocols
  – Very often these days, middleboxes on the path need to read and modify communications
    • Caching, (dynamic) web traffic optimizations, congestion handling, ...

• Result
  – ‘Good Guys’ are forced to bypass the end-to-end security mechanisms
    • Option 1: Employ Man-in-the-Middle attacks to redirect traffic over a proxy under their control
    • Option 2: Provide full keying material to middleboxes, enabling these entities to fully impersonate a server

♫ Obviously, both options are not desirable!
Assumptions

• Meta-data matters
  – When you communicate
  – With whom
  – What protocol you use to communicate
  – How much data you transmit
A view of the attacker

- Targeted means that efforts may be focused
- Meta-data includes pervasive surveillance
- Everything means processing of **content**
- Costs go up at least geometrically
Defending through Intermediaries

- End to end crypto will expose a lot of meta-data
- Local proxies provide some aggregation, but will still leak some meta data
- Global protection means complete L3 overlay
Aggregation

- Aggregation may
  - Anonymize
  - Time shift
  - Pad
  - Suppress
- Some access may be needed
Concentration versus Distribution?

- Whose service is more secure?

Eliot’s Email Service

- Whose service will get attacked more?
Some Key Points

• It is highly unlikely that the attacker has access to everything
• Every user/admin will have their own risk tolerance
  – The threat will differ for different users
  – The cost to mitigate that threat will vary
• Overlay networks do not come for free
• Cost is not always in £ but may be in trust
  – Do you trust Google with your mail?
  – Do you mind some monetization of your information?
• Problem can be considered at different layers
One Way Forward: ‘Interferable Secure Communication’?

• Fact is: Internet reality has changed
  – e.g. more middleboxes, traffic optimizations also needed for encrypted traffic, ...

• But at the same time: Cryptography has advanced recently
  – Functional Signatures / MACs
    • Sender can allow intermediary to modify certain parts of a message, while client can verify that any modification was done with consent of the sender
  – Functional Encryption:
    • Decrypted ciphertext is plaintext modified with a given function
  – (Fully) Homomorphic Encryption:
    • Applying a function on the plaintext without decryption

• General Solution: ‘Interferable Secure Communication’
  – Dedicated, controlled decryption and/or modification of certain parts of the payload by intermediate entities, while preserving message integrity and confidentiality for the rest of the payload
  – This would allow to technically distinguish between dedicated intermediaries that are allowed to read/alter certain parts of messages and actual attackers that intend to monitor/modify encrypted communications
On the other hand...
Middlebox Hit and Run

- Can't tell if this is an attack or not
- Many different breakages = developer $$
- Complex to diagnose
- Shifts support costs
Questions

• What knobs do we need in our protocols to allow users to satisfy their own risk tolerance?
  – Do we need knobs to deal with different jurisdictions?
    • I might trust Country A but not Country B
• What are the user interface issues associated with those knobs?
• From an attacker perspective, when is PS a good use of resources?
• Can aggregation/concentration actually harm the end to end model from a development perspective?
  – Arguably it may have already