Network-Based Website Fingerprinting

draft-wood-pearg-website-fingerprinting-00

Ian Goldberg, Tao Wang, **Christopher A. Wood**

IETF 106 - PEARG - Singapore

Background

Website fingerprinting: class of attacks that use metadata leakage to attack end-user connection privacy

- Use TLS metadata to learn information about encrypted application data
- Use packet IP addresses to learn information about servers

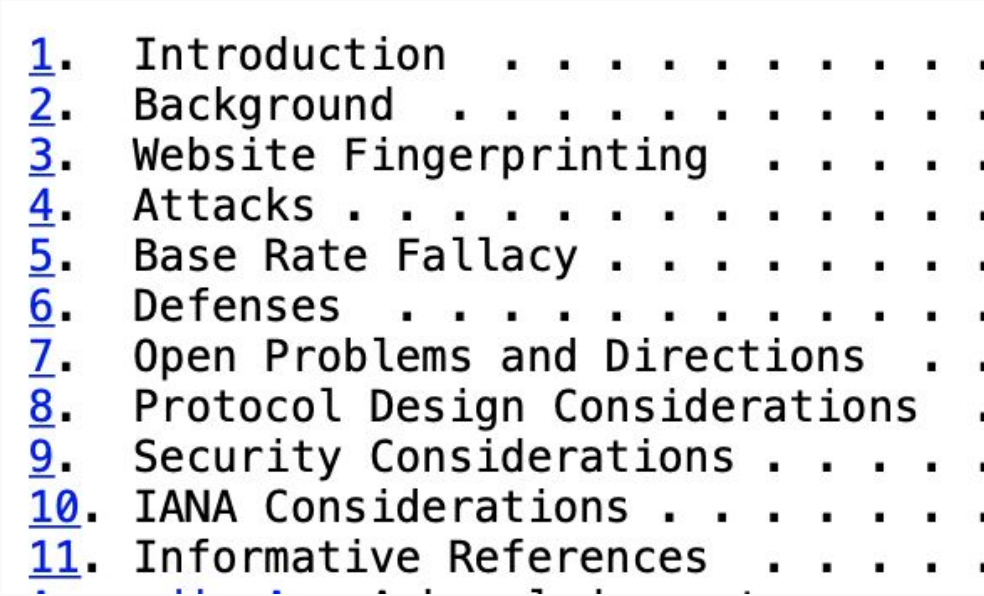
Motivating question: are these attacks possible in practice, and if so, what can be done?

Document Goal

Survey of website fingerprinting research and implications on IETF protocols

Summarize (growing list of) known attacks and their effects

Survey defenses and their limitations



Open Questions

Is this useful for the IRTF and IETF?

Should this work happen in PEARG?

Does the scope need to change?

Similar to `draft-irtf-censorship-tech`, does this need to be regularly updated?