CENSUS
IT Security Works

Tor's Threat Model

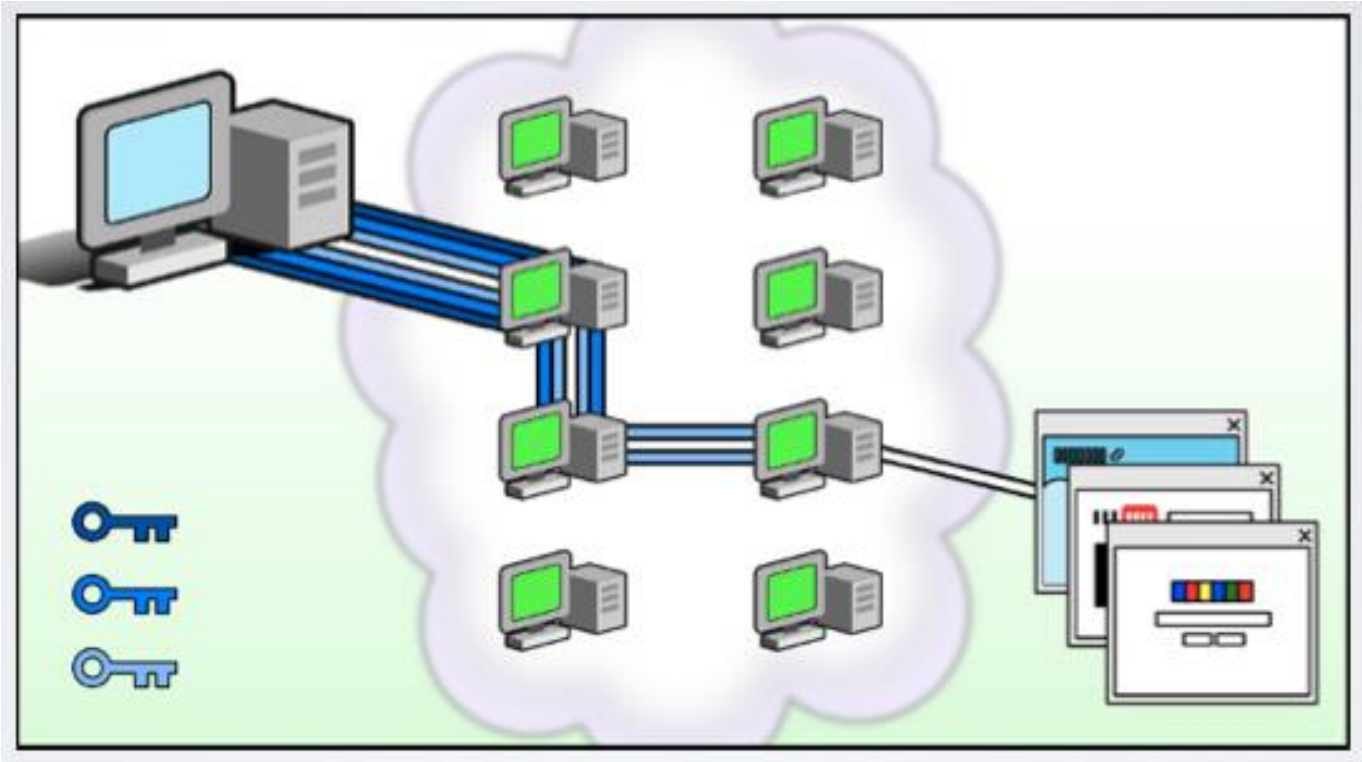
DEVSTAFF 2017

GEORGE CHATZISOFRONIOU (@_sophron)
sophron@census-labs.com
www.census-labs.com

> WHOAMI

- Security Engineer at CENSUS S.A.
  - Infrastructure and software security testing for clients around the world
  - cryptography, WiFi hacking, web security and network security
- Lead author of Wifiphisher
- Academic Research
  - Design of Privacy-enabling / Anonymity-providing protocols

> Tor Network



Picture by duo.com

> Types of anonymity

- Sender Anonymity
- Receiver Anonymity
- Sender – Receiver Anonymity

> Threat model

- Defines the strength of the attacker against whom we want to be protected
- Several properties
  - Internal – External
  - Passive – Active
  - Static – Adaptive
  - Local – Global

> Brute Force Attack

- Attacker sends a 5 GB to a hidden service
- Attacker eliminates all peers who did not receive 5 GB of data

> Tagging Attacks

- Attacker modifies a message so it can be later identified further along the circuit

> Timing Attack

- Application-layer protocols follow patterns
  - E.g. HTTP starts with a small message (HTTP Request) with a large sequence (HTTP response)
- An attacker that monitors every endpoint may determine patterns

> Tor against Tagging & Timing Attacks

- Tor can't afford extra overhead and hours of additional delay that are used in high-latency anonymity-providing networks to protect against these kind of attacks

> Predecessor Attacks

- If you happen to be an entry node for a hidden service, and you connect to that same hidden service, you can tell you're its entry node (and what its IP is)
  - by correlating the traffic you're sending to the hidden service with the traffic you're sending to a client (which is the hidden service).
- With entry guards (few relays that act as entry points), the risk of end-to-end correlation for any given circuit is the same, but the cumulative risk for all her circuits over time is capped.

> Identification through traffic analysis

- Inspect traffic into and out of host may identify that host is running Tor
- Bridge relays to connect to the network
- Pluggable Transports against DPI

> Sybil Attack

- By deploying many relays an attacker is increasing the chances of a client using the attackers evil relays

> Other Vulnerabilities

- Cryptographic
- Development
- Implementation (Bugs)

> Tor's Threat Model

- Assumes an adversary who can observe some fraction of network traffic
- Does not protect against global passive adversary
- Tor focuses on traffic analysis (where an attacker tries to learn whom to investigate), but not on traffic confirmation (aka end-to-end correlation)

> Is Tor safe to use?

- Depends on who *you* are and *your* threat model
  - Tor with a VPN seems safe when it comes to individual entities (e.g. one specific person, your ISP or a group of people)
  - If government agencies are after you, they still may find you

> Conclusions

- Tor (as any other low-latency anonymity-providing network) does not offer “perfect” anonymity
- Using Tor protects you against a common form of Internet surveillance known as "traffic analysis“
  - It is *fairly* the recommended anonymity & privacy solution for millions of users ☺

Thank you!

CENSUS

IT Security Works