Summary of the paper Tor: Second-Generation Router

anonymous authors

1 Introduction

The paper *Tor: Second-Generation Onion Router* was written by Roger Dingledine, Nick Mathewson and Paul Syverson in the year 2004. It describes a circuit based low-latency anonymous communication system called Tor. Tor based on the concept of Onion Routing, which was first published in the paper *Hiding routing information* in 1996 [1]. Onion Routing is also a low latency and circuit based communication system. A low latency network is a network that experiences small delay times [2]. Because of that Tor is able to anonymize interactive network traffic and can used in the world wide web. Circuit based means that Tor establishes circuits across the network to communicate.

2 Onion Routing/Technical background

The goal of onion routing is not to provide anonymous communication. The goal is to limit the traffic analysis in that way to make it impossible to determine who is communication with whom through a public network. In the onion routing network an initiating application make connections through a sequence of machines called onion routers. Each onion router knows only its adjazent onion routers. Because of that an onion router is not able to know who is communication with whom. The data which is sent by the application is layerd like an onion.Each layer of the onion is encrypted by one onion router and contains the next hop in the route. [3]

3 Tor

Tor works on the real-world Internet and requires no special privileges or kernel modifications to increase the usability. In case of Tor the usability is a security requirement because it hide users among users and a system with fewer users provides less anonymity. Additionally to onion routing, Tor added perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies and a practical design for location-hidden services via rendezvous points.

Perfect forward secrecy: In the original onion routing design a single hostile node can record traffic and later compromise succesive nodes in the circuit. To avoid this Tor uses an incremental path building design. Thant means, that the initiator negotiates session keys with each succecive node in the circuit. If these keys are deleted, the compromised nodes are not able to decrypt old traffic.

Congestion control: If many users choose the same OR-to-OR connectionin their circuits, that connection can be saturated. Without any congestion control this bottleneck can propagate through the whole network. To avoid this, Tor is able to control the circuits bandwidth in each OR.

Directory servers: Both Onion routing and Tor has to send periodically state informations (known ORs with their current states) to their users. In the onion routing design they flood their network with these state informations. Tor uses so called *directory servers* to distribute this informations through the network. The users download them periodically every 15 minutes via HTTP.

Integrity checking: Tor uses TLS between its nodes. Because of that an adversary is not able to change the content of the data.

Rendezvous points: If a user wants to connect with a hidden server the onion routing design uses long lived "reply onions", which are used to build a circuit to a hidden server. This is bad because the onion routing design does not provide forward security. For a connection between an user and a hidden server, tor uses so called rendezvouz points. If a user wants to create a connection to a hidden server, it uses the introduction points of this hidden server to send them a rendezvous point. The user and the hidden server uses this rendezvous point to create a circuit between them. Every hidden server has circuits to ORs, which are introduction points.[4]

4 Importance/Impact

This paper has a big impact on the computer since and was cited more than 3000 times by other papers. A wide area onion routing network was briefly deployed but it was not really used because it required a seperate "application proxy" for each supported application protocol and most of them where never written. Tor uses the standard and near-ubquitous SOCKS proxy interface, which support most TCP-based programs without modification. Because of that tor is used in the world wide web since 2004 for anonymous connections. Individuals use Tor for censorship circumvention to reach othervise blocked content, to keep websites from tracking them or their family members, to publish services without needed to reveal the location of them or for sensitive communication. Tor is also used by companies or Journalists to communicate with whistleblowers[5]. But Tor is also used by criminals to sell drugs, child porns, weapons or other illegal things.

References

[1] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information," in *International Workshop on Information Hiding*, pp. 137–150, Springer, 1996.

[2] "Introduction to latency on computer networks." `https://www.lifewire.com/latency-on-computer-networks-818119`. Accessed: 2016-11-17.

[3] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected areas in Communications*, vol. 16, no. 4, pp. 482–494, 1998.

[4] "Tor: Hidden service protocol." `https://www.torproject.org/docs/hidden-services.html.en`. Accessed: 2016-11-17.

[5] "Tor: Overview." `https://www.torproject.org/about/overview.html.en`. Accessed: 2016-11-17.