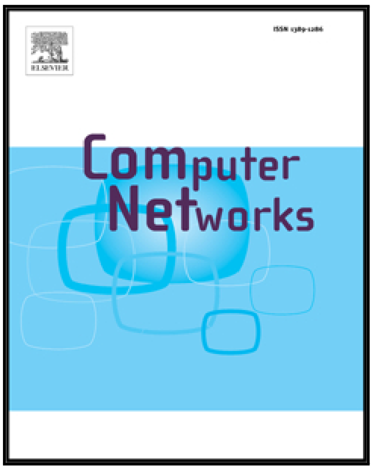

USB Side-channel Attack on Tor

Qing Yang, Paolo Gasti, Kiran Balagani, Yantao Li, Gang Zhou

PII: S1389-1286(18)30264-0
DOI: 10.1016/j.comnet.2018.05.018
Reference: COMPNW 6497

To appear in: *Computer Networks*

Received date: 14 January 2018
Revised date: 19 May 2018
Accepted date: 22 May 2018

Please cite this article as: Qing Yang, Paolo Gasti, Kiran Balagani, Yantao Li, Gang Zhou, USB Side-channel Attack on Tor, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.05.018

USB Side-channel Attack on Tor

Qing Yang[a,*], Paolo Gasti[b], Kiran Balagani[b], Yantao Li[c], Gang Zhou[a]

[a]*Department of Computer Science, College of William and Mary, Williamsburg, VA, USA*
[b]*School of Engineering and Computing Sciences, New York Institute of Technology, New York, NY, USA*
[c] *College of Computer & Information Science, Southwest University, Chong Qing, China*

Abstract

Tor is used to communicate anonymously by millions of daily users, which rely on it for their privacy, security, and often safety. In this paper we present a new attack on Tor that allows a malicious USB charging device (e.g., a public USB charging station) to identify which website is being visited by a smartphone user via Tor, thus breaking Tor's primary use case. Our attack solely depends on power measurements performed while the user is charging her smartphone, and it does not require the adversary to observe any network traffic or to transfer data through the smartphone's USB port. We evaluated the attack by training a machine learning model on power traces from 50 regular webpages and 50 Tor hidden services. We considered realistic constraints such as different network types (LTE and WiFi), Tor circuit types, and battery charging levels. In our experiments, we were able to correctly identify webpages visited using the official mobile Tor browser with accuracies up to 85.7% when the battery was fully charged, and up to 46% when the battery level was between 30% and 50%. Both results are substantially higher than the 1% baseline of random guessing. Surprisingly, our results show that hidden services can be identified with higher accuracies than regular webpages (e.g., 84.3% vs. 68.7% over LTE).

Keywords: Tor, side-channel attacks, de-anonymization, privacy

1. Introduction

Tor is an application-level low-latency network that enables anonymous communication between a client and arbitrary Internet servers. Tor uses a collection of onion routers [1], hosted by a number of volunteers, to unlink the identity and the geographical location of the client from the server, and to conceal the identity of the server to any adversary that can observe the client's network activity (e.g., from the client's Internet service provider). Users rely on Tor to conceal their activities from hackers, governments, employers, and ISPs, since

*Corresponding author
Email address: qyang@email.wm.com (Qing Yang)