CoverUp: Privacy Through "Forced" Participation in Anonymous Communication Networks

David Sommer
ETH Zurich
Zurich, Switzerland
david.sommer@inf.ethz.ch

Aritra Dhar
ETH Zurich
Zurich, Switzerland
aritra.dhar@inf.ethz.ch

Luka Malisa
ETH Zurich
Zurich, Switzerland
luka.malisa@inf.ethz.ch

Esfandiar Mohammadi
ETH Zurich
Zurich, Switzerland
mohammadi@inf.ethz.ch

Daniel Ronzani
Ronzani Schlauri Attorneys
Zurich, Switzerland
ronzani@ronzani-schlauri.com

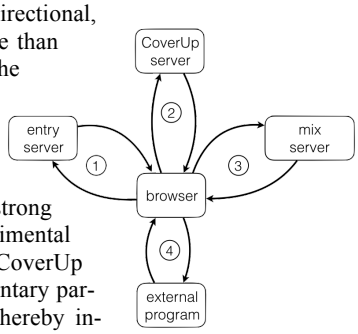
Srdjan Capkun
ETH Zurich
Zurich, Switzerland
srdjan.capkun@inf.ethz.ch

ABSTRACT

Many privacy-enhancing technologies, in particular anonymous communication networks (ACNs) as a key building block, suffer from a lack of a sufficient number of participants. Without high user participation, ACNs are vulnerable to traffic analysis attacks. The only ACN with a high number of participants (around 1.5 million users) is Tor [2]. Yet, Tor is prone to traffic analysis attacks [3,4] traffic pattern attacks. While other ACNs [1] have been proposed that are even secure against global attackers, they are not scalable and suffer from a low number of participants, since even a perfect ACN can at most hide a user among all participating users. These ACNs are in a vicious circle: the lack of participants leads to low degree of anonymity, and a low degree of anonymity makes these ACNs unattractive for users.

In this work, we break this vicious cycle by studying the question: Can an anonymous communication network be strengthened by "forced" participation? What privacy guarantees and performance can such an ACN provide? We develop CoverUp, a system that "forces" visitors of highly accessed websites (entry servers) to become involuntary participants of an ACN. CoverUp triggers users to participate in a centralized, constant-rate mix by leveraging basic functionality of their browsers to execute (JavaScript) code served by the entry servers. Candidates for entry servers could be universities or news sites. They would let a distinct CoverUp server provide (via an iframe, step 1) JavaScript code to the end-users' browsers (step 2), which in turn makes them participate in the ACN via a mix server (step 3). Visitors of these entry servers' websites become (involuntary) participants of an ACN, creating cover traffic for voluntary participants. For voluntary participants, we developed a browser extension that renders their CoverUp requests indistinguishable from the cover traffic of involuntary participants.

We build two applications on top of CoverUp: an anonymous feed and a chat—both use an additional external CoverUp application (step 4). As the feed is uni-directional, we do not need to trust more than the client's machine. As the chat is bi-directional, we do need to trust the CoverUp and the mix server. We show that both achieve practical performance and strong privacy properties via experimental evaluations and an analysis. CoverUp renders voluntary and involuntary participants indistinguishable, thereby including all voluntary and involuntary participants into an anonymity set. Given this, CoverUp provides even more than mere anonymity: the voluntary participants can hide the very intention to use the ACN. As the concept of forced participation raises ethical and legal concerns, we discuss these concerns and describe how these can be addressed.



CCS Concepts/ACM Classifiers

• Security and privacy~Privacy-preserving protocols

Author Keywords

anonymity sets; anonymous communication; forced participation

BIOGRAPHY

Srdjan Capkun (Srđan Čapkun) is a Full Professor at ETH Zurich. See http://www.syssec.ethz.ch/people/capkun for more details.

REFERENCES

[1] H. Corrigan-Gibbs, and B. Ford, "Dissent: accountable anonymous group messaging", in *Proceedings of the 17th ACM conference on Computer and communications security*, ACM, 2010, pp. 340–350.

[2] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second- generation onion router," DTIC Document, Tech. Rep., 2004.

[3] R. Jansen, F. Tschorsch, A. Johnson, and B. Scheuermann, "The Sniper Attack: Anonymously deanonymizing and disabling the Tor network," DTIC Document, Tech. Rep., 2014.

[4] X. Wang, S. Chen, and S. Jajodia, "Network flow watermarking attack on low-latency anonymous communication systems," in *Proceedings of the 28th Symposium on Security and Privacy (SP'07)*. IEEE, 2007, pp. 116–130.

ASIA CCS '17, April 02-06, 2017, Abu Dhabi, United Arab Emirates
ACM 978-1-4503-4944-4/17/04.
http://dx.doi.org/10.1145/3052973.3056126