Poster: Phonion: Frustrating Telephony Metadata Analysis

Stephan Heuser*†, Bradley Reaves‡, Praveen Kumar Pendyala*, Henry Carter‡,
Alexandra Dmitrienko§, William Enck††, Ahmad-Reza Sadeghi*†, and Patrick Traynor‡
* TU Darmstadt
† Intel CRI-SC
‡ University of Florida
§ Fraunhofer Institute SIT
†† North Carolina State University

A. Introduction

Phone companies record network use by individual customers via Call Detail Records (CDRs). CDRs contain important metadata ranging from call source and destination to duration of the connection, route through the network and identification of the network device writing the call record. Historically, CDRs have served as a means of not only properly billing customers for the services they use, but also as a way of identifying and debugging network errors.

This metadata has most recently been associated with large-scale collection campaigns by intelligence agencies. While these organizations often assert that such programs are necessary to prevent crime and terrorism, privacy advocates argue that the complete cataloging of telephony actions erode civil liberties. However, what researchers and policy makers have generally failed to consider is that a range of other adversaries may also use CDRs to violate the privacy of targeted individuals. In 2006, for example, detectives hired by executives at HP were able to use social engineering to acquire phone records and determine the identity of an anonymous corporate board member who leaked sensitive information to journalists. Such attacks are not limited to private detectives, but have also been executed by jealous spouses, curious neighbors, companies paying for employee cell phones, rogue employees at cellular providers and more. In fact, last September it was revealed that Vodafone scoured a journalist's personal phone records to discover her sources on a story about Vodafone security problems [1] . Accordingly, strong mechanisms for making analysis of CDRs difficult is crucial to the privacy of citizens across the world.

Taking the importance of call metadata for user privacy into consideration, there are prior attempts to build anonymous telecommunication systems based on Voice over IP (VoIP) and anonymization networks like Tor. However, these solutions do not provide adequate quality of service for voice calls. Moreover, they require fast and reliable Internet connectivity, which might not always be available. For instance, Internet access in countries with a repressive regime can be shut down to prevent dissemination of non-censored information. Further, even if Internet access is generally available, access to the Tor network could be censored.

NDSS '16, 21-24 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2016.23xxx

B. Accomplishments To Date

In this project we address limitations of existing anonymous telecommunication systems. To this end, we present Phonion – a solution for anonymous phone calls which uses the high-quality telephony infrastructure and does not require Internet connectivity during calls.

In a nutshell, Phonion separates call setup from call delivery functions. This separation allows individual telephony service providers only to see the next hop in a call circuit, but never the entire circuit from source to destination. To establish a call circuit, a user (the callee) connects to broker nodes, which list available call relays. The user then performs call setup by reserving connections between relays via secure Internet links. This step can be performed hours or days before the circuit is used. Finally, a caller dials into the pre-established circuit using a standard landline or cellular phone and his call is delivered to the callee. Phonion can be used to contact crime tip lines, conduct sensitive business transactions, and even to use common services like WhatsApp with unlinkability against a wide range of adversaries.

We make the following contributions to date:

- *Design and implementation of Phonion:* We define the spectrum of adversaries and design and implement a system of loosely cooperating telephony devices to establish and relay calls so that the source and destination of a call are unlinkable using CDRs. Our system combines existing building blocks for call obfuscation in a novel way to create an out-of-band signaling overlay network, and takes into account the vast diversity of phone technologies, ranging from rotary dialing to VoIP.

- *Comparison against a range of proposed alternatives:* We discuss the limitations of current solutions, which range from Caller ID suppression to "burner" phones that are only used a small number of times. To the best of our knowledge, our analysis for the first time demonstrates that the current state of the art fails to address all but the simplest adversaries and fails to scale. A substantial novelty of Phonion is that it can use dedicated high-quality telephony services instead of congestion-prone IP anonymization networks, and hence does not require constant Internet connectivity.
- *Extensive evaluation:* We use call quality tools and metrics from the audio analysis community to demonstrate that in contrast to VoIP over Tor, Phonion maintains call fidelity when compared to standard phone calls.

We note that attacks against call metadata are far simpler legally and technically than full audio capture. Our system is designed to make the former extremely difficult, but explicitly does not address the latter distinct attack. As the first systematic analysis and solution in this space, we note that effectively frustrating telephony metadata analysis is a significant and larger problem than what can be addressed in any single academic paper. However, we carefully define adversary classes and discuss how Phonion prevents attempts to link phone communications between parties.

C. Future Plans and Objectives in Presenting

We are currently developing a theoretical analysis of the anonymity guarantees, and we hope to provide both an analytical model and results of simulation.

While the Phonion project is approaching maturity, it has yet to be published. We believe that the opportunity to present this work at NDSS will bring to the conference an interesting and novel technical approach to a subject that is at the forefront of discussion worldwide. Additionally, we believe that feedback from the diverse community present at NDSS will help us further improve the performance and presentation of this system.

REFERENCES

[1] B. Doherty, "Vodafone Australia admits hacking Fairfax journalist's phone," *The Guardian*, Sep. 2015. [Online]. Available: http://www.theguardian.com/business/2015/sep/13/vodafone-australia-admits-hacking-fairfax-journalists-phone