Poster: Privacy-Preserving Rapid Traceback of Telephone calls

Dawuda Ahmed
NC State University
dahmed@ncsu.edu

Bradley Reaves
NC State University
bgreaves@ncsu.edu

***Abstract*—Illegal robocalls are a major problem in many countries, disrupting legitimate phone communication and causing financial loss to the industry. Around 25% of subscribers cannot straightaway differentiate between a robocall and a real call hence people fall prey to its related fraud schemes and subsequently reducing the usefulness of the network. Congress has enacted laws and fines in place as deterrents to robocalls but there is no quick way to trace calls back to the lawbreaker as the existing method is a manual process and takes several hours to days to complete. In this paper, we propose the PrivyTrace framework to securely collect and process metadata contained in Call Detail Records (CDR) while obfuscating the metadata with secure cryptographic techniques to render private data inoperable to a high-class adversary with access to all records. We set up and small-scale telephone network emulation to evaluate the performance, security, and privacy guarantees of PrivyTrace, consequently demonstrating that for large datasets containing several millions of records, our technique will trace a call within a few seconds while privacy remains a necessity.**

I. Extended Abstract

Telemarketing is a way for businesses to connect with their customers and learn about their needs. It allows businesses to conduct surveys, sell products directly, and reach a wider audience. Additionally, it provides potential customers with the opportunity to contact the business with any questions they may have. Telemarketing relies on the use of automated calls (robocalls) to deliver important information to subscribers. Legitimate robocalls, under Federal Trade Commission rules such as ones that intend to dispatch informational messages, debt collection, political calls, health care, or charities, do not require subscribers' permissions however, these days majority of robocalls are illegal and scams [3], [4]. These are usually targeted at the elderly, immigrants, and other vulnerable populations to impersonate government officials such as the Internal Revenue Service and Social Security Administration. A recent study [2] collected nearly 1.5 million uninvited phone calls over 11 months period which averages to 4,137.43 calls per day. This adds latency and disrupts legitimate phone communication, causing a loss of revenue to the industry, and consequently reducing the usefulness of the network. In fact, most users now ignore calls from unknown numbers which may sometimes be an important calls from a loved one who needs help.

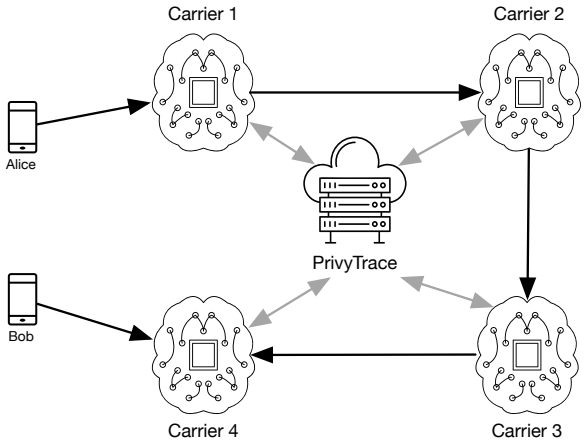


Fig. 1. A high-level overview of call setup

One approach to addressing the robocall problem is the robust tracing of illegal robocalls back to offenders to allow punishment by the law. The US Telecom established the Industry Traceback Group (ITG) [1] which collaborates with companies from across telecom industries to trace robocalls. They do so by sending a notification to the terminating Voice Service Provider (VSP) and each VSP in the call path then determines the identity of the upstream VSP from whom it received the traffic and enters the information into the system until a dead-end is reached or the originating VSP is identified or a non-cooperating VSP is reached. Traceback works this way since each network provider involved with the call only knows its immediate upstream and downstream providers and nothing more. As illustrated in Fig. 1, Carrier 1 knows only Carrier 2 (upstream), Carrier 2 knows only Carrier 1 (downstream) and Carrier 3(upstream), and so each Carrier, C_n knows only C_{n-1} and C_{n+1}. Although this process is successful, it is manual and time-consuming, usually taking several days to complete a single trace-back and this period

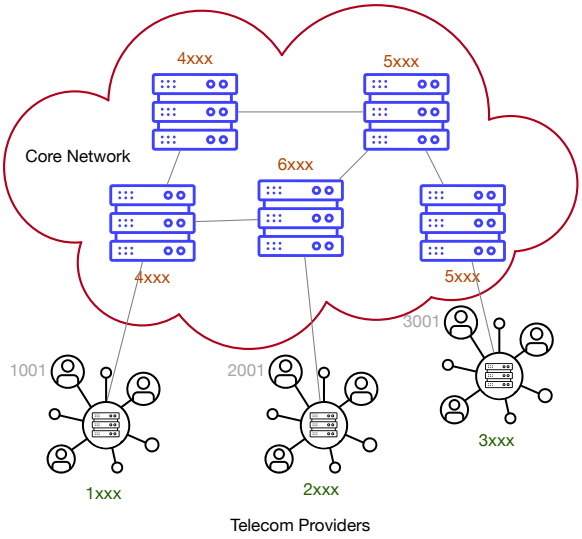


Fig. 2. Test Telephone network Emulate

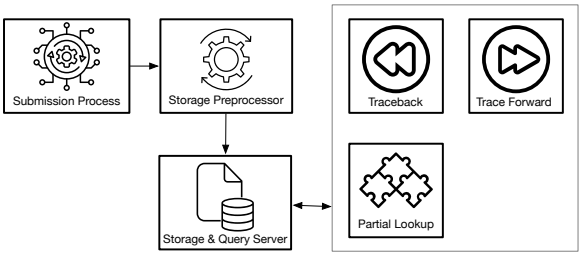


Fig. 3. Components that makeup PrivyTrace

is enough for the offender to no longer be a customer of the originating VSP. Due to regulatory and privacy-related restrictions, collecting real-world CDR data is problematic and has affected the number of academic efforts aimed at addressing the issue of tracing illegal robocalling by analyzing metadata contained in proprietary records.

In this paper, we present PrivyTrace, a system securely designed to provide a rapid trace back of illegal calls to their originator while obfuscating the metadata rendering it inoperable to adversaries. As in Fig. 1 PrivyTrace requires collaboration from voice service providers to contribute routing records related to calls that they route from different carriers in a secure and privacy-preserving way that guarantees caller and callee privacy. The design of PrivyTrace relies on the heavy use of cartographic hash functions and computational puzzles to preserve the privacy of caller, callee, and peer networks. PrivyTrace will have the following functionalities: Traceback, trace forward and partial lookups (particularly important in situations where a number of carriers failed to contribute records).

Our approach as discussed above is of course a trivial database query however for security and privacy there are a few issues to address:

- We need to protect the privacy of the caller and callee thus it should be infeasible for a computationally bound adversary to identify all calls to and from a given telephone number.
- It should be computationally infeasible to determine peers of a given network given the whole database of records that we store.
- We want to eliminate any form of graph analysis on the whole database that can leak information about call volumes between networks.
- We need to provide mechanisms to prevent abusing the infrastructure by a single party or collusion

Our methodology includes creating an insecure strawman solution and a model to generate synthetic Call Detail Records (CDRs). This will serve as a benchmark to assess the feasibility and practicality of our solution. Additionally, we will use this base solution to compare and contrast with our secure scheme, in order to determine its effectiveness and potential for deployment

We are creating a set of protocols for securely submitting, storing, and tracing PSTN, VoIP, or cellular metadata over public channels. To facilitate collaboration, we are developing a hybrid public key encryption technique for key agreement among collaborating carriers involved with a particular call. The key must be unique for each caller, callee, and timestamp tuple to ensure security and privacy

In order to address ethical concerns and restrictions in this area, we are unable to test PrivyTrace in a real-world telephone network. Instead, we are creating a small-scale, toy telephony network using the open-source software Asterisk (as shown in Fig. 2) to emulate real work behavior. This approach has several advantages: it allows us to get a sense of how PrivyTrace will impact the network, identify any challenges network carriers may face when implementing our technique, and accurately measure parameters such as call setup latency.

References

[1] ITG. What is the Industry Traceback Group? https://tracebacks.org.

[2] S. Prasad, E. Bouma-Sims, A. K. Mylappan, and B. Reaves. Who's calling? characterizing robocalls through audio and metadata analysis. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 397–414, 2020.

[3] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad. Sok: Fraud in telephony networks. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 235–250. IEEE, 2017.

[4] TransNexus. Premium rate numbers are begging to be used for telecom fraud.

We propose a collaborative and privacy-preserving system to automate forward or backward tracing of illegal robocalls

PrivyTrace: Privacy-Preserving trace back/forward of phone calls

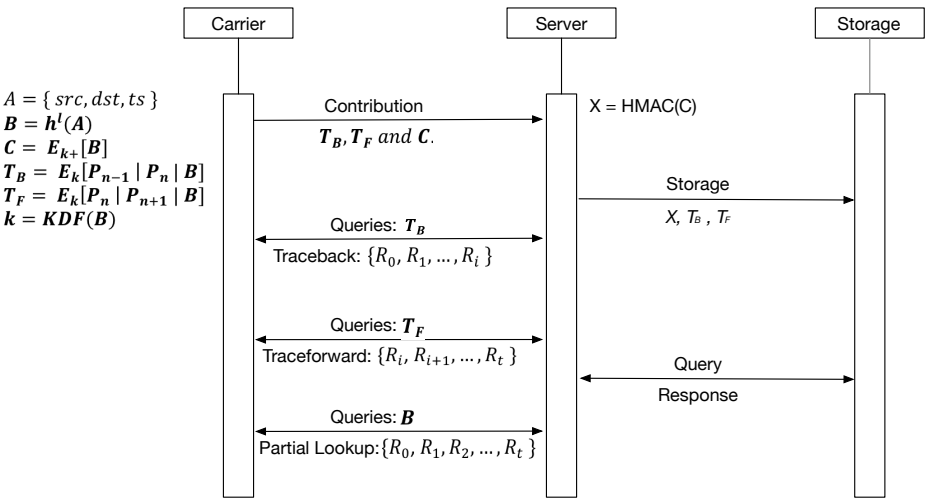
Dawuda Ahmed, Bradley Reaves

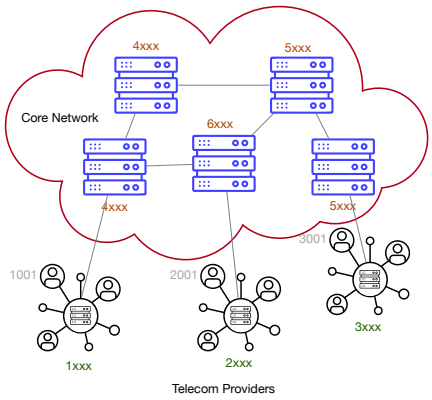
Problem and Motivation

- The upsurge of illegal **robocalls** disrupts the network and reduces its usefulness. Law Enforcement Agencies (LEA) and Telecom providers face difficulties in pinpointing originators of **illegal robocalls** and this frustrates subscribers, consequently reducing the usefulness of the network.
- Ascertaining telecom providers that originate robocalls will motivate robocall detection schemes and assist LEA in prosecuting offenders. Effectively, this will dissuade illegal robocalling.
- We are developing **PrivyTrace**, a privacy-preserving series of protocols and systems to promote collaboration from multiple telecom providers to rapidly trace suspicious calls.

Methods

- We created an insecure strawman solution and a model to generate synthetic CDRs. Benchmarking this solution is necessary to determine if it is reasonable for practical deployment and to compare the secure scheme against.
- We are developing a series of protocols for secure and privacy-preserving submission, storage and reckoning trace backs or trace forwards for PSTN, VoIP or cellular call metadata over public channels.
- To properly evaluate PrivyTrace, we are creating a small-scale toy telephony network with Asterisk to emulate real world telecommunication and to measure how PrivyTrace impacts the network and call setup.





Functional Requirements

- **Trace Back**: Trace call from current voice service provider (VSP) to the originating VSP.
- **Trace Forward**: Trace call from current VSP to the terminating VSP.
- **Partial Lookups**: This is important for situations where 1 or more VSP failed to contribute their routing records.

Security Requirements

- Individual call unlinkability.
- Obfuscate network trends.
- Confuse Network Associations
- Forward secrecy for records
- Protect against abuse by single party.
- Prevent collusion.

NC STATE UNIVERSITY

WSPR