Phonion: Frustrating Telephony Metadata Analysis

Stephan Heuser‡, **Bradley Reaves**§, Praveen Kumar Pendyala‡, Henry Carter§, Alexandra Dmitrienko‡, William Enck†, Ahmad-Reza Sadeghi‡, Patrick Traynor§

North Carolina State University†, Technische Universität Darmstadt‡, University of Florida§

Takeaway: Phonion places relays in phone networks to protect against call metadata analysis while preserving call quality.

CDR: Call Data Records

Telephony networks maintain phone metadata in the form of Call Data Records (CDRs).
CDRs are tuples containing:
(Caller Number, Callee Number, Call Start Time, Call End Time, Route)

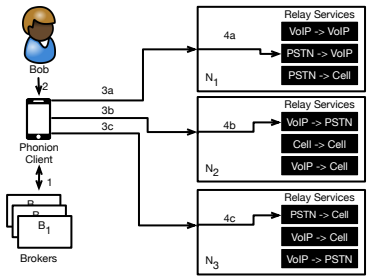
Why Protect Call Metadata?

"Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."
— Stewart Baker, NSA General Counsel

Journalists need to protect the identities of confidential sources
Whistleblowers and **activists** need to disclose issues anonymously
Executives need to discuss confidential agreements

We distinguish adversaries based on the type and amount of CDRs they can obtain.
Nosy associates (**class 1**) can obtain only a few call records
Carriers (**class 2**) can see records for all subscribers, but not other records.
Law Enforcement organizations (**class 3**) can query records within their jurisdictions
Global Adversaries (**class 4**) see all call records

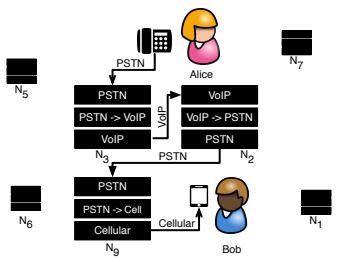
Route Setup



Ahead of an anticipated call, Bob establishes a **Phonion number** by using a **client** to instruct 3 **relays** to route incoming calls along a path that ends in his actual phone number.

Brokers are services that inform Bob's client about available relays.

Placing a Phonion Call



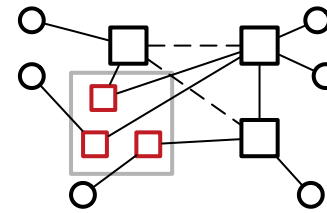
When Alice calls Bob's Phonion number, the call is first delivered to Relay N3.

That relay then creates a *separate* call from N3 to N2, with N2 then calling N9, who finally calls Bob.

Security Properties

A simplistic analysis of Phonion call metadata will simply show calls between users and the Phonion system.

To definitively identify Phonion call source and destination, adversaries will need to recover the complete call chain, which would require visibility into all relays routing the calls.



The adversary could identify probable calls by computing the graph formed by inter-relay connections. In this case, users of calls through connected components in the relay graph form an anonymity set.

Unfortunately, all low-latency anonymity systems are vulnerable to end-to-end timing and long-term intersection attacks.

Call Quality

We have implemented Phonion relays, brokers, and a client for Android to evaluate call quality.

	Cellular	Phonion (3 Hops)	TorFone
Latency (ms)	391	480 (10)	644 (89)
Jitter (ms)	0	0.4 (0.2)	8.5 (5.9)
MOS (call quality)	3.5*(est.)* "Fair"	3 (0.07) "Fair"	2.08 (0.23) "Poor"

Alternatives: Insecure or Unusable

	Caller ID Spoofing	Conference Calls	Disposable Phone	Encrypted VoIP	TorFone	Phonion
Adversary Classes Protected Against		**1**	**1,2**		**1, 2, 3**	**1, 2, 3**
No single point of failure	x	x	x	x	✓	✓
Usable with any carrier worldwide	x	✓	✓	x	x	✓
Supports offline calls	✓	✓	✓	x	x	✓
Supports Landline Phones	✓	✓	✓	x	x	✓
Supports Cellular Phones	✓	✓	✓	x	x	✓
Supports VoIP	x	x	x	✓	✓	✓
High Voice Quality	✓	✓	✓	✓	x	✓

For further information, contact Brad Reaves (*reaves@ufl.edu*).