



Beyond E2E

Breaking and Remaking Modern Secure Communications
Matt Weeks, technology fellow, Deloitte & Touche LLP
October 29, 2021

Introduction



- Prior work
 - Enumeration attacks
 - DoS (Denial of Service) attacks
 - Zero-click remote code execution (RCE) attacks against popular end-to-end (E2E) encrypted messengers by CVE (Common Vulnerabilities and Exposures):
 - CVE-2018-10994, CVE-2018-11101
 - CVE-2021-24035
 - Supply chain risks

Phone-dependent system exploitation



- Identification
- Burner tracking:
 - 2010 killer arrest
 - 2014 investigation
 - 2019 investigation
- Alternative phone and geolocation exploitation
- SIM (Subscriber identity module) and registration attacks

Anonymity networks



- I2P (Invisible Internet Project) chat
- Tor (The Onion Router) messenger
- Ricochet
- Tor hidden service enumeration

Fixing the issues



- Better identity and identifiers
- Metadata security
- Sybil resistance
- User enumeration resistance
- Features

Identity



- Cryptographic public key identifiers
- Not phone trackable
- Not enumerable
- Disadvantage (advantage): where are my friends?
- Share via QR (quick response) code or link
- Non-enumerable discovery
- Avoid user enumeration by derived keys

Metadata security



- Node mesh functions as relays
- Conversations brokered by meet nodes, which store and forward encrypted messages but never have the key or know participants
- Onion routing means meet nodes don't see real client internet protocol addresses (IPs), which use relays

Sybil resistance



- What if an attacker just spins up a million nodes?
- This attack is hard to prevent in any anonymity network, including Tor and I2P
- Avoid forged and duplicate nodes: verify each
- Reduce impact by increasing friction; mass node spinups are easiest (and have happened in the past) from cloud providers operating from a defined set of ranges
- Randomize networks reducing influence
- Seed from different clouds and regions

Resilience



- In contrast with centralized **and federated** systems, meet nodes are expendable
- Encrypted conversation data is replicated transparently to standbys
- Conversation participants, who hold a private key the meet nodes don't, negotiate rollovers and new standby selections transparently to the user

Resilience



- Congestion control and loss recovery
- Authenticated; prevents on the side attacks
- Round trip time (RTT) based system
- Algorithm inspired by Vegas congestion control algorithm
- Dynamic detection of congestion
- Performs well in lossy yet high bandwidth environments (often wireless) and long fat pipes

Functionality – Audio and Video



- Audio & Video:
 - UDP (User Datagram Protocol)-backed protocol, optional lossy
 - Constant bitrate audio avoids passive attacks
 - Screen sharing
 - Video groups of any size
 - Avoiding WebRTC (Web Real-Time Communication) and its vulnerabilities and information leaks

Functionality – other additions



- Multi-device sync:
 - Communicate, turn off one device, turn on the next, sync all messages
 - This requires data storage on the network
- File storage/syncing:
 - Block-level crypto and auth, random access, supports git

Meet node incentives and risks



- Untrusted meet nodes may delete data they hold, but messages and files can be checked by client code and meet nodes can be rolled
- Storage risks:
 - Nodes won't store unlimited data
 - Trimming policy based on total database size, per-conversation, or by expiration date
 - Current lack of reservable space

Future directions



- Reservable space by microtransaction – already working in storage blockchains
- Mutually-authenticated contact discovery:
 - Avoids enumeration attacks
 - Register by validated phone number
 - Bidirectional contact relationships hashed, validated – you can only discover contact X if you are in X's address book, too

Demo





This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Inclusion does not constitute an endorsement of the product and/or service.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2021 Deloitte Development LLC. All rights reserved.