PairSonic: Helping Groups Securely Exchange Contact Information

Florentin Putz
Technical University of Darmstadt
Darmstadt, Germany
fputz@seemoo.de

Steffen Haesler
Technical University of Darmstadt
Darmstadt, Germany
haesler@peasec.tu-darmstadt.de

Thomas Völkl
Technical University of Darmstadt
Darmstadt, Germany
tvoelkl@seemoo.de

Maximilian Gehring
Technical University of Darmstadt
Darmstadt, Germany
gehring@cs.tu-darmstadt.de

Nils Rollshausen
Technical University of Darmstadt
Darmstadt, Germany
nrollshausen@seemoo.de

Matthias Hollick
Technical University of Darmstadt
Darmstadt, Germany
mhollick@seemoo.de

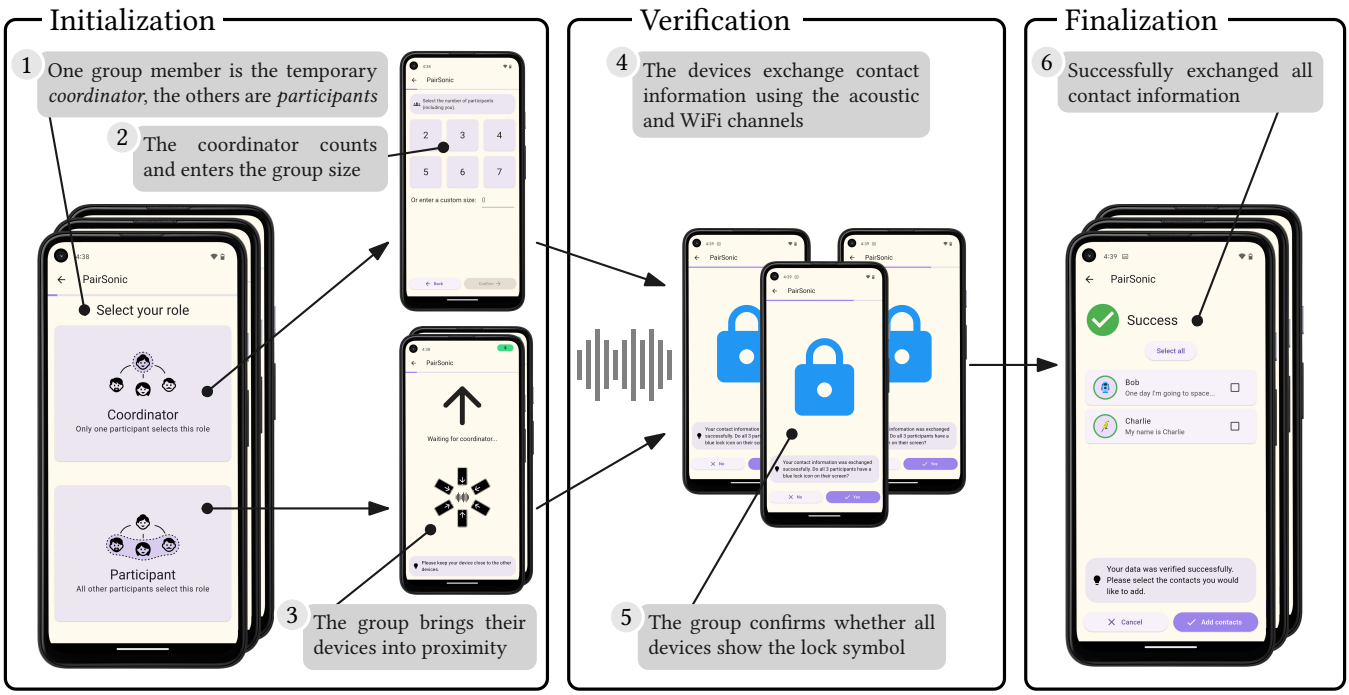

Figure 1: The PairSonic user interface, demonstrated for a group of three users wanting to exchange their contact information.

Abstract

Securely exchanging contact information is essential for establishing trustworthy communication channels that facilitate effective online collaboration. However, current methods are neither user-friendly nor scalable for large groups of users. In response, we introduce PairSonic, a novel group pairing protocol that extends trust from physical encounters to online communication. PairSonic simplifies the pairing process by automating the tedious verification tasks of previous methods through an acoustic out-of-band channel using smartphones' built-in hardware. Our protocol not only facilitates connecting users for computer-supported collaboration, but also provides a more user-friendly and scalable solution to the authentication ceremonies currently used in end-to-end encrypted messengers like Signal or WhatsApp. PairSonic is available as open-source software: https://github.com/seemoo-lab/pairsonic

CSCW Companion '24, November 9–13, 2024, San Jose, Costa Rica.

CCS Concepts

• **Human-centered computing** → **Computer supported cooperative work**; *Open source software*; **Collaborative interaction**; **Smartphones**; Mobile computing; • **Security and privacy** → **Authentication**; *Usability in security and privacy*.

Keywords

usable security; group pairing; secure device pairing; trust establishment; acoustic communication; data-over-sound; authentication ceremony; public-key cryptography; end-to-end encryption; instant messaging; online collaboration; contact management; key verification; peer-to-peer-authentication; MitM attacks; device association; binding; bonding; coupling; smartphone; prototype; security; privacy; social cybersecurity; interoperability; ad-hoc; decentral; spontaneous; nearby; proximity; open-source; WiFi; NFC; Android

ACM Reference Format:

Florentin Putz, Steffen Haesler, Thomas Völkl, Maximilian Gehring, Nils Rollshausen, and Matthias Hollick. 2024. PairSonic: Helping Groups Securely Exchange Contact Information. In *Companion of the 2024 Computer-Supported Cooperative Work and Social Computing (CSCW Companion '24), November 9–13, 2024, San Jose, Costa Rica.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3678884.3681818

1 Introduction

Effective communication and collaboration require a trusted environment where participants clearly know each other's identities and do not have to fear unauthorized access [4]. This trust is vital for facilitating open discussions among friends, family, colleagues, business partners, and especially vulnerable groups like journalists and activists [2, 3, 7]. While end-to-end encrypted (E2EE) messengers like Signal support group collaboration through real-time messaging and video calls, they cannot, by default, protect against unauthorized access and impersonation by active adversaries. These threats include rogue service operators and machine-in-the-middle (MitM) attacks. Active MitM attacks in particular have become more prominent due to reports of law enforcement agencies compromising app providers, highlighting a practical and concerning risk for privacy infringements by malicious actors in the future [2].

To mitigate these risks, E2EE tools require users to perform a manual contact verification process known as the *authentication ceremony* [8]. Only after this ceremony is completed is the communication fully protected. The current design of authentication ceremonies in E2EE tools has two major shortcomings: First, they have low usability, requiring considerable user interaction, time, and effort [2, 4, 8]. Second, they do not support larger groups, functioning only between two users [6]. This limitation is significant because collaboration often involves multiple participants. Performing bilateral authentication ceremonies between each pair of group members is infeasible, as the number of required manual verifications scales quadratically with the group size.

To address both challenges, we designed PairSonic, a novel pairing protocol for the fast and secure exchange of contact information that scales efficiently to multiple participants. Our prototype implementation allows users to extend trust from physical encounters to online communication by simply holding their devices together for a few seconds, aligning with intuitive association behavior. This demo accompanies our full paper at CSCW 2024 [6], where we evaluated PairSonic's usability in a lab study, finding it to be highly effective for groups. PairSonic automates the tedious verification tasks required by previous approaches, greatly enhancing usability and making secure group communication more accessible.

2 System Design

PairSonic is a group pairing protocol that enables two or more users meeting in person to spontaneously exchange or verify their contact information. Each participant obtains authentic and verified contact details of all other participants, including their cryptographic public keys. Importantly, our protocol does not rely on external key management infrastructure, prior associations, or shared secrets.

2.1 Protocol

The PairSonic protocol is based on the cryptographic foundation of the SafeSlinger protocol [1], but improves its usability and deployability [6]. Our protocol operates in three main phases (Figure 1):

(1) **Initialization:** A group of users initiates PairSonic on their smartphones to exchange contact data. One member is selected as the temporary *coordinator* while the others become *participants*. The coordinator inputs the total group size and ensures that all participants' smartphones are ready and within proximity. The coordinator's smartphone sets up a temporary ad-hoc WiFi network and transmits the network details over an acoustic out-of-band (OOB) channel, allowing the other smartphones to connect automatically.

(2) **Verification:** Once connected, the devices use this WiFi network to perform a cryptographic protocol derived from the SafeSlinger protocol [1]. Participants send nested commitments, containing their contact data and cryptographic public keys, to the coordinator's smartphone. The coordinator aggregates these commitments into a hash value and transmits it over the acoustic OOB channel. All devices monitor this channel, ready to abort the process if an incorrect message is detected.
Upon verifying the correct hash value, a blue lock symbol appears on each smartphone, prompting users to confirm the matching symbols on all other devices. If confirmed, the smartphones use the WiFi network to distribute success nonces, allowing the display of verified exchanged contacts. If the lock symbol confirmation fails, abort nonces are released, halting the protocol and ensuring the integrity of the contact exchange. We changed the verification symbol based on feedback from our user study, because some participants misunderstood the previous checkmark as indicating protocol completion without verifying the symbol.

(3) **Finalization:** Each participant now sees a list of all received contacts and can select which to import.

2.2 Acoustic Out-Of-Band Channel

Previous user studies have indicated that performing authentication ceremonies with current E2EE tools like Signal or WhatsApp is often challenging due to the time and effort required [2, 4, 8]. Our protocol, PairSonic, addresses these issues by automating manual verification tasks such as comparing phrases, digits, or pictures. PairSonic utilizes an acoustic location-limited channel, leveraging the smartphones' built-in speakers and microphones to exchange data within a range of approximately one meter. This method simplifies the inclusion of multiple devices at once, a distinct advantage over near-field communication (NFC) or quick-response (QR) codes, which typically handle one device at a time. Moreover, unlike WiFi

Table 1: Selection of devices where we have verified compatibility with PairSonic, indicating support for audible and inaudible modes. In principle, any smartphone with WiFi Direct and running at least Android 6.0 (released in 2015) should be compatible.

Model	OS	SDK	Audible	Inaudible
Google Pixel 4	Android 13	33	✓	✓
Google Pixel 4a	Android 13	33	✓	✓
Google Pixel 5	Android 13	33	✓	✓
Google Pixel 6 Pro	Android 13	33	✓	✓
LG Nexus 5	Android 6.0.1	23	✓	✓
Motorola Edge	Android 10	29	✓	✓
OnePlus 10 Pro	Android 12	31	✓	✓
Oppo Reno 6	Android 11	30	✓	✓
Redmi Note 9 Pro	Android 10	29	✓	✓
Samsung Galaxy A32	Android 12	31	✓	✓
Samsung Galaxy A52s 5G	Android 14	34	✓	✓
Samsung Galaxy S10e	Android 12	31	✓	✓
Samsung Galaxy S20 Ultra 5G	Android 10	29	✓	✓
Samsung Galaxy S22	Android 13	33	✓	✓

or Bluetooth, the acoustic physical layer in our system is inherently location-limited and software-defined, allowing for the incorporation of advanced physical layer security techniques [5]. These enhancements can significantly strengthen the protocol's defense against sophisticated attacks on the acoustic channel, thus providing an additional layer of security for group pairing.

3 PairSonic Prototype

Our prototype of PairSonic is implemented as an Android app using the Flutter framework. For communication, we utilize two channels: a local ad-hoc WiFi connection, provided by the Android WiFi Direct API, and the acoustic OOB channel for data transmission via sound waves, provided by the ggwave library.[1] During our user study [6], we employed audible frequencies ranging from 1875 Hz to 6375 Hz to evaluate user perceptions of this communication method. Participants expressed concerns about the appropriateness of audible noises in quiet settings like museums or libraries. In response, we developed a variant that uses inaudible near-ultrasonic frequencies between 15 000 Hz and 19 500 Hz. Our testing revealed that these inaudible frequencies not only mitigate the issue of noise in quiet environments but also enhance the robustness of the communication. This improvement addresses another concern raised in our lab study, which noted occasional failures in acoustic communication that required restarting the pairing process.

The combination of an acoustic channel with WiFi Direct in our prototype forms a novel communication stack. To ensure functionality and compatibility, we conducted tests using smartphones from various manufacturers (Table 1). The prototype functioned effectively on all devices tested that support WiFi Direct, provided they run at least Android version 6.0 (API level 23, released in 2015). PairSonic is interoperable, meaning that different device models within the exchange can interact seamlessly.

4 Applications

PairSonic is designed to assist users in establishing trustworthy digital communication channels, making it especially useful for forming ad-hoc collaboration groups among multiple users [3]. This makes PairSonic particularly adaptable to various computer-supported collaboration tools, including group work platforms, educational hubs, and video conferencing systems. Furthermore, our protocol could be integrated into E2EE messengers like Signal, WhatsApp, or Matrix, providing a more user-friendly authentication ceremony to support effective and trustworthy online collaboration.

[1]Data-over-sound library ggwave: https://github.com/ggerganov/ggwave

Our study [6] highlights these potential applications: participants identified multiple scenarios where PairSonic could serve as a secure method for contact exchange. These include forming private chat groups on Signal, managing participants in Zoom video conferences, and enhancing interaction within online collaboration tools.

Availability

Together with this paper, we provide an overview of the PairSonic project online at https://seemoo.de/s/pairsonic. PairSonic is available as open-source software on GitHub: https://github.com/seemoo-lab/pairsonic

Acknowledgments

This work has been funded by the LOEWE initiative (Hesse, Germany) within the emergenCITY center [LOEWE/1/12/519/03/05.001(0016)/72].

References

[1] Michael Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, and Adrian Perrig. 2013. SafeSlinger: Easy-to-Use and Secure Public-Key Exchange. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking (MobiCom '13)*. Association for Computing Machinery, New York, NY, USA, 417–428. https://doi.org/10.1145/2500423.2500428

[2] Matthias Fassl and Katharina Krombholz. 2023. Why I Can't Authenticate — Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Hamburg, Germany. https://publications.cispa.saarland/3895/

[3] Moses Namara and Bart P. Knijnenburg. 2021. The Differential Effect of Privacy-Related Trust on Groupware Application Adoption and Use during the COVID-19 Pandemic. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2, 405:1–405:34. https://doi.org/10.1145/3479549

[4] Sean Oesch, Ruba Abu-Salma, Oumar Diallo, Juliane Krämer, James Simmons, Justin Wu, and Scott Ruoti. 2022. User Perceptions of Security and Privacy for Group Chat. *Digital Threats: Research and Practice* 3, 2 (Feb. 2022), 15:1–15:29. https://doi.org/10.1145/3491265

[5] Florentin Putz, Flor Álvarez, and Jiska Classen. 2020. Acoustic Integrity Codes: Secure Device Pairing Using Short-Range Acoustic Communication. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20)*. 31–41. https://doi.org/10.1145/3395351.3399420

[6] Florentin Putz, Steffen Haesler, and Matthias Hollick. 2024. Sounds Good? Fast and Secure Contact Exchange in Groups. In *Proceedings of the ACM on Human-Computer Interaction 8 (CSCW2)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3686964

[7] Erica Shusas, Patrick Skeba, Eric P. S. Baumer, and Andrea Forte. 2023. Accounting for Privacy Pluralism: Lessons and Strategies from Community-Based Privacy Groups. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3544548.3581331

[8] Elham Vaziripour, Justin Wu, Mark O'Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jordan Whitehead, Nick Bonner, Kent Seamons, and Daniel Zappala. 2018. Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security (SOUPS '18)*. USENIX Association, USA, 47–62.