Poster: Exposure Notification at Hand

Patrick Rathje
Kiel University, Kiel, Germany
pra@informatik.uni-kiel.de

Olaf Landsiedel
Kiel University, Kiel, Germany
Chalmers University of Technology, Gothenburg, Sweden
ol@informatik.uni-kiel.de

Abstract

Contact tracing is a tool for controlling infectious disease outbreaks. To foster widespread adoption, established tracing protocols focus on smartphone users. As a result, user groups who cannot afford a compatible smartphone cannot carry it continuously are left out. This work introduces the Contact Tracing Wristband (CWB) and its integration into Google and Apple's Exposure Notification protocol. The wristband's low-cost and versatility bring tracing to additional users and thus enhance the efficacy of tracing.

1 Introduction

The World Health Organization describes contact tracing as an ”essential public health tool for controlling infectious disease outbreaks” [7]. A key element for successful tracing is widespread adoption. Google and Apple unveiled the Exposure Notification protocol (GAEN) for Android and iOS devices building on top of Bluetooth Low Energy (BLE) [1]. The protocol makes contact tracing available to the majority of smartphone owners. However, it neglects a significant number of people: Costs, limited technical knowledge, and just the impracticality or prohibition to carry a smartphone can leave certain groups behind. Elderly, children, or many employees, for example, cannot participate in the tracing process.

Wearables such as smartwatches can extend the reach of contact tracing [2]. EasyBand [6] and P^{3}CT [3] are smartwatches and wristbands for contact tracing based on BLE. However, both do not integrate the devices into existing tracing protocols like the GAEN protocol.

We argue that the reach of existing tracing protocols should be further extended using devices that reside directly at your wrist: With this work, we introduce the Contact Tracing Wristband (CWB), a low-power wristband with low-costs and high versatility. The wristband targets integration into existing tracing protocols. In this sense, we specifically target the integration with GAEN.

Challenges. The wristband needs to balance energy-consumption and costs to be a valuable alternative to smartphones in the mentioned settings. Ensuring compatibility with established protocols such as GAEN poses challenges. The integration into the GAEN protocol requires cryptography, time synchronization, and a network connection to download published keys of infected persons.

Approach. This work presents an extendable, low-power design and our prototype integration into the EN protocol. Besides, we discuss advantages, feasibility, and future work.

2 The Contact Tracing Wristband

The Contact Tracing Wristband (CWB) features a low-cost design with a minimal set of core components (see Figure 1 for an overview). Our prototype builds on an nRF52840-Devkit with a 64 MHz Cortex-M4 microprocessor and runs Zephyr OS. The included persistent storage and BLE allow e.g. contact tracing, synchronization, or firmware updates over-the-air.

3 Exposure Notification At Hand

In the Exposure Notification protocol by Apple and Google [1], devices use BLE to exchange temporary identifiers and store them locally. At the start of the day, each device randomly generates a new daily key. The devices derive the temporary identifiers based on this secret, one for each of the 10 minute periods (144 in total), which it frequently broadcasts. In addition to the identifiers, the broadcasted packet contains encrypted metadata. This metadata includes the actual transmit power and is only readable with access to the daily key. If users get infected, they can upload the relevant daily keys (e.g. last 14 days), which the health authorities then publish. All other users download the daily

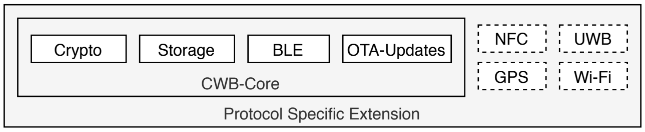

Figure 1. The Contact Tracing Wristband (CWB) builds on a low-power core and integrates seamlessly into tracing protocols like the Exposure Notification protocol by Apple and Google.

International Conference on Embedded Wireless Systems and Networks (EWSN) 2021
17–19 February, Delft, The Netherlands
ISBN: 978-0-9949886-5-2

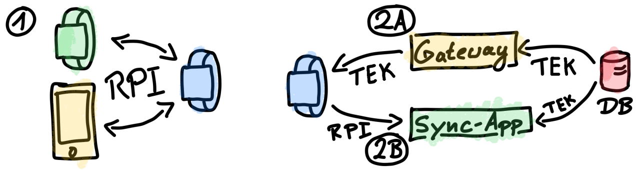

Figure 2. The wristband runs the Exposure Notification protocol and exchanges beacons (RPI) with smartphones (1). It checks for infectious contacts in two modes: In gateway-mode (2A), the device downloads and checks published keys (TEK) itself, whereas, in the companion-mode (2B), it entrusts its received RPIs and the check to a companion device.

Table 1. Devices in the Exposure Notification protocol generate a random secret for each day and derive temporary identifiers from it using cryptographic primitives. Measured times are the average of 100 runs on nRF52840-Devkit (without optimizations).

Interval	Function	Time [ms]
Daily	Generate Random Secret	0.300
Daily	Derive Identifier Key	0.288
Daily	Derive Metadata Encryption Key	0.288
Each Period	Derive Temporary Identifier	0.062
Each Period	Encrypt Metadata	0.066
Check Key	Derive All Temporary Identifiers	8.912

keys and derive the individual temporary keys to check for possible exposure. The devices estimate the exposure's intensity based on the duration and distance.

We implement the Exposure Notification protocol on the resource-constrained wristbands. Our implementation maintains compatibility and is available as open-source[1]. The protocol builds on several cryptographic primitives that we implemented as a standalone library based on Mbed TLS[2]. Table 1 lists the corresponding measurements running on the nRF52840 DK [4]. While the device can handle the generation and derivation of its own keys with ease (assuming a clock accurate to two hours), synchronization and matching with published daily secrets require a connection to the central system. The wristbands could get equipped with cellular connections adding costs and lowering battery life. Instead, we propose two techniques building on the included BLE connection: gateways and companion devices (see Figure 2).

Gateways. Gateways enable the wristband's autonomy: Placed at strategic points such as bus stops, they provide BLE access points to central servers and thus provide synchronization and over-the-air updates without the need for additional devices.

Companion Device. A dedicated companion device serves as a reliable source of time and updates. Moreover, the device could download and check received identifiers from one or multiple wristbands and upload new daily secrets. Recently, Bluetooth SIG drafted an Exposure Notification System (ENS), which enables wearables to share tracing data with devices like smartphones [2].

4 Discussion

Within the same tracing protocol, the wristband offers privacy levels comparable to smartphone implementations. Lower costs, versatile application, and separation of personal and tracing data are direct advantages that could make the wristband accessible and attractive to more users. With an increase in the number of users, the corresponding tracing protocols get more effective, attracting even more users due to increased efficacy and social incentives [5].

However, these statements only hold if the wristband is reliable and continuously used. Users carry their smartphones, whether they trace contacts or not. Not wearing the wristband certainly mitigates its benefits.

5 Future Work

We are conducting a trial with 1000 participants to analyze user acceptance and behavior. Further questions reside in energy consumption and effects on tracing accuracy. Besides, we plan to add compatibility with the Exposure Notification Service [2] for seamless integration with other wearables and the corresponding administration devices. Security and privacy remain essential aspects and require further analysis.

6 Conclusion and Outlook

This work introduces the Contact Tracing Wristband with its integration into the Exposure Notification protocol to extend the reach of existing contact tracing protocols. Neglected participants such as the elderly, children, or employees who may not want or are not allowed to carry a smartphone could benefit from a wristband's versatility and low costs. Further studies may show the actual effect on users and identify benefits and disadvantages.

7 Acknowledgements

This work is supported by the Federal Ministry of Health based on a resolution of the German Bundestag.

8 References

[1] Apple Inc. Privacy-preserving contact tracing. https://covid19.apple.com/contacttracing, 2020 (accessed Nov 28, 2020).

[2] Bluetooth SIG, Inc. Ens wearables. https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-ens/, 2020 (accessed Dec 03, 2020).

[3] P. C. Ng, P. Spachos, S. Gregori, and K. Plataniotis. Epidemic exposure notification with smartwatch: A proximity-based privacy-preserving approach. *arXiv preprint arXiv:2007.04399*, 2020.

[4] Nordic Semiconductor. nrf52840 dk. https://www.nordicsemi.com/Software-and-Tools/Development-Kits/nRF52840-DK, 2020 (accessed Dec 03, 2020).

[5] S. Trang, M. Trenz, W. H. Weiger, M. Tarafdar, and C. M. Cheung. One app to trace them all? examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, 29(4):415–428, 2020.

[6] A. K. Tripathy, A. G. Mohapatra, S. P. Mohanty, E. Kougianos, A. M. Joshi, and G. Das. Easyband: A wearable for safety-aware mobility during pandemic outbreak. *IEEE Consumer Electronics Magazine*, 9(5):57–61, 2020.

[7] World Health Organization. Contact tracing in the context of covid-19. https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19, 2020 (accessed Nov 28, 2020).

[1] https://github.com/CovidBraceletPrj/CovidBracelet

[2] https://github.com/prathje/exposure-notification