ContraIL: Privacy First Protocols for Digital Contact Tracing

Ahmad Dinkins

University of Illinois at Urbana–Champaign

Professor Madhusudan Parthasarathy

University of Illinois at Urbana–Champaign

Professor Ugo Buy

University of Illinois at Chicago

Gladys Dennyson Thomas

University of Illinois at Chicago

Abstract

We are currently amidst the COVID-19 pandemic, so safe and reliable forms of contact tracing are more important than ever. Manual contact tracing has been the primary mode for monitoring exposure to this disease. This form of tracing is done by interviewing infected patients and accessing travel records to create a list of contacts. The contacts are then notified of possible infection and would continue to be monitored . Digital contact tracing (DCT) can do much of the same, only in a more secure and reliable manner. Humans are error prone (we may forget or not even notice those whom we have come in contact with), so automating the tracing process would be more effective. We have developed a protocol for digital contact tracing that recognizes several privacy policies. Our goal is to provide a method of contact tracing that is more effective and more secure than manual contact tracing.

Keywords: Digital Contact Tracing, Privacy, Bluetooth Low Energy, Relay Attack

ContraIL: Privacy First Protocols for Digital Contact Tracing

Although Digital Contact Tracing is safer in terms of record keeping, it is still vulnerable to various security attacks. In order to ensure the integrity of the digital contacts, we developed and iterated on protocols that negate Relay Attacks.

Approach

In our approach, we use Bluetooth Low Energy to perform an exchange between two potential contacts, where a contact occurs between two phones running our application and in range. Each contact locally generates a “Day” key from a predetermined master key. We then perform a Diffie Hellman Key Exchange with users encrypting their approximate location along with their other data. Once the location is verified by both users, each user records the other user’s Day key to show that a legal contact was made. By verifying the location of contacts, we can ensure that malicious users cannot successfully perform relay attacks. When a user reports that they are infected, they upload their aggregated set to a centralized server. The server then takes all such sets that were sent to it and performs a private set intersection with the sets of other users on the server. The private set intersection does not reveal any of the information within the sets, but will notify the user of a potential infection if the set intersection is not zero.

Experiment

We measured the computational time of the private set intersection on a Galaxy J3 Achieve (Android 9) and varied the size of the server and client sets. Client sizes ranged based on how active different users could be during a pandemic.

Results

On really small client or server sets (less than 1000 key entries), the application ran without any noticeable delay regardless of the size of the other set. When the magnitude of each input set reached over 1000, the time it took to complete the intersection exponentially increased.

Conclusion

Ultimately, from our experiments, we believe that the cost in computational time is worth given the security the protocol provides. Unfortunately, since we require the user's approximate location in our protocol, we cannot make much progress until concerns about location sharing are mitigated in the future.

References

Loiseau, L. L., Bellet, V. B., Bento, T. S. B., Teissonniere, E. T., Benoliel, M. B., Kinsman, G. K., & Milne, P. M. (2020). Whisper tracing version 3 - an open and privacy first protocol for contact tracing. https://docsend.com/view/nis3dac