ONBOARDING

Melanie Svab, Katja Keller

18.JULI 2021

INTRODUCTION TO INTERNET AND SECURITY

30526-01

I. Einführung

Das BACNet (BAsel Citizen Network) ist eine von Studierenden umgesetzte dezentrale Netzwerk Implementation auf Basis von Append-only Logs. Im Rahmen des Projektes war es unser Ziel den bisherigen Onboarding Prozess auszubauen um somit ein neues Kennenlernen unter den Usern zu ermöglichen.

Dabei waren die ersten Herausforderungen die bisherige Funktionsweise zu verstehen, den Code zu analysieren und die Problemfelder inklusive den passenden Code-Abschnitten herauszukristallisieren. Danach ging es darum, diese gefundenen Baustellen in einer ergänzenden Implementation zu beseitigen und anschließend in das bestehende Projekt zu integrieren.

Als Grundbaustein diente vor allem die bisherige Arbeit der Gruppe FeedCtrl aus dem Frühjahrssemester 2020. Mit den Schnittstellen zur Gruppe LogStore war es jedoch unumgänglich, auch diese in der neuen Implementation anzugleichen. Für das Kennenlernen nutzten wir Bluetooth.

II. Hintergrund

Die Inspiration für Bluetooth kam uns mit dem Blick auf jetzige Geschehnisse. Erst letztes Jahr kam in der Schweiz mit der SwissCovid-App eine Applikation vom Bund auf den Markt, welches proximity Tracing und presence Tracing verwendet in der Bekämpfung der Ausbreitung der Covid-19 Pandemie. Dafür wurde das für diesen Zweck kreierte offene Protokoll Decentralized Privacy-Preserving Proximity Tracing (DP-3T) verwendet [1], welches auf Basis von Bluetooth Low Energy (BLE) sogenannte local generierte ephemeral Identifiers (EphIDs) austauscht.[2] Im selben Kontext wurde nahezu zeitgleich das konkurrierende Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) Protokoll entwickelt [3]. Der größte Unterschied liegt in der Speicherung der Daten. Das DP-3T implementiert ein dezentrales Verfahren. Dabei wird ein geheimer Seed Key erstellt, aus dem sich die flüchtigen EphIDs generiert. Nur bei einer bestätigten Infektion und einer Zustimmung werden die einzelnen Seed Keys beim BackEnd-Server hochgeladen. Andere Nutzer laden regelmäßig die neuen Daten vom BackEnd-Server herunter und können so benachrichtigt werden bei einem Match, siehe Appendix A für eine grafische Darstellung. Dabei können in keinem Schritt die Daten der Identität einer Person zugeordnet werden und es wird verhindert, dass einerseits nicht Infizierte Daten an den BackEnd-Server weitergeleitet werden oder sich aus den Daten ein Social Graph ableiten lasse [2]. Beim PEPP-PT wird ein stärkerer zentraler Ansatz verfolgt. Ursprünglich war die Schweiz in das PEPP-PT Projekt involviert, entschied sich aber wegen Kontroverse bezüglich Transparenz für das DP-3T [4][5].

Weitere nennenswerte Protokolle, welche im Rahmen der Pandemie entwickelt wurden und allesamt BLE als Grundlage verwenden, wären das Temporary Contacts Name (TCN) Protokoll, das BlueTrace Protokoll oder das (Google/Apple) Exposure Notification (GAEN) Protokoll [6][7][8].

Es gibt viele Vorteile von Bluetooth. Diese sind vor allem bei dem Austausch einer nicht allzu grossen Datenmenge und bei einer überschaubaren Entfernung zweier Geräten ersichtlich. Dabei wird wenig Strom verbraucht und die Übertragung ist nicht nur einfach, sondern auch schnell. Außerdem wurde in den letzten Jahren die Sicherheit von Bluetooth

verbessert und die Übertragungsrate markant erhöht. Diese Vorteile machen Bluetooth heute zu einer der verbreitetsten Formen des Nahfunks [9]

Dabei verwendet Bluetooth eine Vielzahl von verschiedenen Protokollen. Bei unserer Implementation verwendeten wir das etablierte RFCOMM (Radio frequency communication) Protokoll. Dieses ermöglicht eine drahtlose Kommunikation über Bluetooth. Die verbreitete Unterstützung und die unter den meisten Betriebssystemen öffentlich zugängliche Programmierschnittstelle sind die wichtigsten Vorteile von RFCOMM. Außerdem ist RFCOMM abwärtskompatibel. Das bedeutet, dass es auch zu älteren Versionen oder deren Schnittstellen verträglich ist [10][11].

Relevant für den Hintergrund des Projektes ist es auch die bisherige Funktionsweise des Onboardings beim BACNet zu erläutern. Dieses beschäftigt sich diskreter mit dem Austausch von Feeds, welche alle relevanten Informationen der gemeinsamen Kommunikation beinhalten. Dabei sind diese gegliedert durch eine überstehende Master-Feed Methode, welche zu jeder Applikation einen eigenen Feed erstellt und die einzelnen Applikations-feeds in diesem speichern. Der bisherige Ansatz basierte auf einem greedy-Verfahren. Beim Importieren werden alle Master-feeds auf die Datenbank übertragen und beim Exportieren alle in der Datenbank hinterlegten Master-Feeds mitübertragen [12]. So wird versucht, so viele Nutzer wie möglich kennenzulernen, und möglichst effizient anderen Nutzern alle Teilnehmer, die einem User bekannt sind, mitzuteilen. Dabei wird jedoch die Idee des Datenschutzes komplett ignoriert. Die einzelnen Nutzer können so nicht entscheiden, welchen anderen Teilnehmer ihre Feeds weitergegeben werden. Man kann also nicht kontrollieren, wer die eigenen Daten erhält. Zusätzlich resultiert aus diesem Ansatz bei einer grossen Anzahl von Nutzern auch ein Speicherplatzproblem. Dadurch, dass jeder Nutzer alle Master-Feeds erhält, und diese auch gespeichert werden, ist der Speicherverbrauch sehr gross.

Diese Probleme galt es in der Implementation zu lösen.

III. Implementation

Für die Implementation nutzten wir zusätzlich zu den schon bestehenden Packages die beiden Packages pybluez2 in der Version 0.41 und openpyxl 3.0.7. Ersteres implementiert Bluetooth Funktionalitäten in Python während sich zweiteres nützlich für das Speichern und das Auslesen der Master-IDs von einer Excel-Datei erwies.

Als Kern unserer neuer Onboarding Erweiterung fungiert der Austausch der Master-IDs via Bluetooth über einen RFCOMM Kanal. Dabei werden die beiden Kommunikationspartner in Server und Client unterteilt, wo der Server auf die Verbindung beim passenden Port wartet und der Client die Verbindung anhand des Device Namens des Partners und der gefunden Adresse aufbaut. Die Master-ID wird dann über diese aufgebaute Verbindung ausgetauscht und direkt in die nächste freie Zeile einer generierten Excel-Datei gespeichert. Dadurch bleiben die gespeicherten Master-IDs auch nach Beenden der Applikation gespeichert. Abgesehen von diesem werden keine weitere Daten gespeichert. Wenn zwei Kommunikationspartner nun zum ersten Mal die Feeds austauschen möchten müssen diese normalerweise den Master-feed über “Trust” validieren. Bevor dies allerdings möglich ist, muss der überstehende Master-feed ausgetauscht sein. In einem weiteren Zwischenschritt werden nun bei der Übertragung der Daten vom USB-Stick zuerst gefiltert, welche Master-feeds mit den gespeicherten Master-IDs aus der Excel-Datei übereinstimmen. Alle gespeicherten Master-IDs aus der Excel-Datei werden dabei mit den Werten der

Master-feeds auf dem USB Stick verglichen und nur bei Übereinstimmung übertragen. Somit werden nur Master-feeds im FeedCtrl User Interface angezeigt, welche sich zuvor über das Onboarding kennengelernt haben. Erst mit diesem Zwischenschritt ist es damit nun möglich den vollständigen Austausch der Feeds durchzuführen.

Für die Integration in das bisherige User Interface von FeedCtrl haben wir dazu zusätzlich noch das bestehende Design per TKinter ausgebaut. Dabei haben wir beim Startbildschirm einen neuen Button “Bluetooth-Onboarding” hinzugefügt, welcher bei Betätigung ein neues Fenster öffnet und die Auswahl zwischen Client und Server für den Austausch der Master-IDs ermöglicht.

IV. Resultat

Unser Projekt führte zu einer Erweiterung des Onboardings, welche die analysierten Problemfelder der bisherigen Umsetzung behebt. Das Problem mit dem Datenschutz wird umgangen, in dem einerseits die einzelnen User nun im Vorfeld kontrolliert ihre Kommunikationspartner per Austausch des Master-IDs auswählen und somit auch nur die zugehörigen Feeds übertragen bekommen. Damit löst sich auch das Problem der Speicherkapazität. Durch diese vorhergehende Filterung reduziert sich die Anzahl vom USB-Stick übertragene Feeds auf die ausgetauschten Kontakte. Des Weiteren gewährleistet die Speicherung der Master-IDs als einzelnes eine gewisse Anonymität der Kommunikationspartner, da diese allein keine Rückschlüsse auf die Identität bekannt gemachter Kommunikationspartner bietet.

V. Diskussion / Lessons learned

Alles in allem war das Projekt eine gute Möglichkeit, uns in neue Themen einzuarbeiten und an einem praktischen Beispiel das erlernte Wissen aus der Vorlesung und Übung zu übertragen und anzuwenden. Wir haben viel über aktuelle Protokolle und deren Umsetzung lernen können und dieses erlernte Wissen an einem praktischen Projekt anzuwenden und uns auch vertiefter mit einem grösseren dezentralen Netzwerk vertraut zu machen und einzufinden. Des Weiteren ermöglichte uns das Projekt auch über eine größere Distanz unsere Fähigkeiten von Teamwork, Planung und Kommunikation auszubauen.

Der Onboarding Prozess an sich wäre dabei immer noch ausbaufähig. Der Austausch über Bluetooth ist von der Nutzerfreundlichkeit noch umständlich und auch die Speicherung per Excel nicht ideal. Bei der Eingabe des Partner Device Namens muss auf Seiten des Clients in der UI auf das Terminal ausgewichen werden und der Austausch funktioniert nicht, wenn das Excel File nicht geschlossen ist zum Zeitpunkt der Übertragung und muss dann zuvor manuell geschlossen werden. Die Zeit, diese Feinschliffe umzusetzen, fehlte uns leider im Rahmen dieses Projektes. Grosse Mühe bereitete uns auch das Einfinden in das Thema. Wir bedanken uns bei den Betreuern, welche uns in spannenden Diskussion schlussendlich auf den richtigen Pfad führen konnten.

VI. Referenzen

[1]https://github.com/SwissCovid/swisscovid-doc (abgerufen 07.07.2021)

[2]https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf (abgerufen 10.07.2021)

[3]https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany.pdf (abgerufen 10.07.2021)

[4]https://www.nzz.ch/technologie/streit-um-das-corona-tracing-der-schweizer-epidemiologe-salathe-verkuendet-den-ausstieg-aus-dem-paneuropaeischen-projekt-ld.1552279?reduced=true (abgerufen 10.07.2021)

[5]https://www.covid19healthsystem.org/countries/switzerland/livinghit.aspx?Section=1.4%20Monitoring%20and%20surveillance&Type=Section (abgerufen 10.07.2021)

[6]https://github.com/TCNCoalition/TCN (abgerufen 10.07.2021)

[7]https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf (abgerufen 10.07.2021)

[8]https://www.google.com/covid19/exposurenotifications/ (abgerufen 10.07.2021)

[9]https://praxistipps.chip.de/bluetooth-einfach-erklaert_100370 (abgerufen 11.07.2021)

[10]https://de.wikipedia.org/wiki/Liste_der_Bluetooth-Protokolle#Radio_Frequency_Communication_(RFCOMM) (abgerufen 11.07.2021)

[11]https://www.elektronik-kompendium.de/sites/kom/0803301.htm (abgerufen 11.07.2021)

[12]BACnet-Report IAS 2020 - Gruppe 14 Feed-Ctrl

Appendix A.