Jacek Hoła, 194128

Projekt informatyczny – specyfikacja

1. Opis ogólny

1.1. Nazwa aplikacji: Aplikacja będzie się nazywała *The Onion Phone*.

1.2. Cel aplikacji: Aplikacja ma umożliwić przeprowadzenie szyfrowanej, anonimowej rozmowy głosowej za pomocą zdecentralizowanej infrastruktury. Aplikacja jest przeznaczona dla systemu Android.

1.3. Użytkownik docelowy: Aplikacja jest przeznaczona dla użytkowników, którzy z różnych powodów potrzebują sposobu na nawiązanie połączenia głosowego nie ujawniając swojej lokalizacji, tożsamości i treści rozmowy podmiotom trzecim.

1.4. Zakres aplikacji: Aplikacja będzie zapewniać wszystkie funkcjonalności niezbędne do przeprowadzenia szyfrowanej, anonimowej rozmowy głosowej (w tym: odpowiednie połączenie z siecią anonimową, szyfrowanie end-to-end, implementacja kodowania mowy dostosowana do wysokich opóźnień)

1.5. Licencja: Aplikacja będzie dostępna na jednej z otwartych licencji (w zależności na co pozwolą użyte biblioteki)

1.6. Repozytorium: https://github.com/jaczula/the-onion-phone

2. Wymagania funkcjonalne

2.1. Stworzenie nowego identyfikatora do przyjmowania połączeń

2.2. Import i eksport identyfikatora

2.3. Nawiązanie połączenia z innym użytkownikiem

- Użytkownik wprowadza identyfikator innego użytkownika, z którym chce się połączyć
- Użytkownik wybiera, czy chce przekazać użytkownikowi , z którym się łączy, swoją tożsamość (przez udowodnienie, że jest się posiadaczem danego identyfikatora)
- Aplikacja nawiązuje połączenie z wybranym użytkownikiem lub wyświetla błąd, jeśli użytkownik o danym identyfikatorze nie odpowiada

2.4. Wysłanie wiadomości tekstowej do innego użytkownika

- Użytkownik wprowadza identyfikator innego użytkownika, do którego chce wysłać wiadomość tekstową
- Użytkownik wybiera, czy nadawca ma pozostać anonimowy dla odbiorcy, czy wiadomość ma zostać podpisana
- Aplikacja wysyła wiadomość tekstową do danego użytkownika lub wyświetla błąd, jeśli użytkownik o danym identyfikatorze nie odpowiada (odbiorca w momencie wysyłania musi być dostępny, ponieważ nie istnieje żadna infrastruktura, która mogłaby przechowywać wiadomość do momentu pojawienia się odbiorcy)

2.5. Odbieranie połączenia od innego użytkownika

- Aplikacja wyświetla powiadomienie o rozmowie przychodzącej (jeśli użytkownik dzwoniący wysyła swój identyfikator, jest on wyświetlany, jeśli w telefonie istnieje kontakt z tym identyfikatorem, aplikacja wyświetla dane tego kontaktu)
- Użytkownik może odebrać połączenie lub je odrzucić

Jacek Hoła, 194128

3. Wymagania niefunkcjonalne

3.1. Aplikacja wymaga telefonu z systemem Android w wersji 4.2 lub wyższej, dostępu do roota (obejście tego wymagania będzie inwestygowane)

3.2. Aplikacja wymaga połączenia z internetem. Wskazana jest sieć zapewniająca niewielkie opóźnienia.

3.3. Siecią anonimową będzie TOR, z tego powodu wymagana będzie obecność oficjalnego klienta sieci TOR: Orbot

3.4. Aplikacja będzie korzystać z biblioteki Codec2 do kodowania dźwięku (z możliwością wprowadzenia innych bibliotek)

3.5. Do komunikacji zostanie użyty protokół SRTP. Uzgadnianie klucza odbędzie się za pomocą protokołu ZRTP, szyfrowanie za pomocą AES-128 w trybie ICM lub f8, autentyczność i weryfikację danych zapewni HMAC-SHA1. Aplikacja będzie korzystać z biblioteki libSRTP.

4. Harmonogram prac

4.1. Analiza wymagań – do 29.10

4.2. Opracowanie projektu aplikacji – do 12.11

4.3. Implementacja szkieletu aplikacji i interfejsów – do 3.12

4.4. Tworzenie implementacji dla poszczególnych interfejsów – do 7.01

4.5. Podstawowe testy aplikacji – 7.01 – 28.01

4.6. Stworzenie przyjaznego użytkownikowi GUI - do 21.01

4.7. Stworzenie dokumentacji i instrukcji – do 28.01

4.8. Opcjonalnie: implementacja dodatkowych funkcjonalności – do 28.01