



Projekt Nr. 1701

– Projektendbericht –

Vorbemerkung

Dieser Endbericht basiert auf dem Zwischenbericht vom 7. August 2017 und erweitert diesen um die Tätigkeiten im Projekt, welche im Zeitraum August 2017 bis Februar 2018 durchgeführt wurden.

Administratives

Das Projekt verläuft entsprechend der ursprünglichen Planung. Lediglich personell mussten Anpassungen vorgenommen werden. Da die Akquise des Junior Researchers, der ursprünglich ab Monat 2 am Projekt arbeiten sollte, mangels BewerberInnen längere Zeit in Anspruch genommen hat als erwartet, wurde personell wie folgt umgeplant. Anstelle des Junior Researchers wurden studentische Mitarbeiter für das Projekt eingestellt (Peter Kopciak, Florian Taurer und Kevin Pirner). Mit April ist dann schließlich der neu an der FH St. Pölten angestellte Junior Researcher (Alexis Ringot) in das Projekt eingestiegen. Sowohl Florian Taurer als auch Alexis Ringot haben das Projekt bis zum Ende des Förderzeitraums begleitet. Inhaltlich läuft das Projekt entsprechend der Planung. Alle Arbeitspakete konnten erfolgreich abgeschlossen werden und alle angefallenen Meilensteine wurden erreicht. Der Abruf der letzten Förderrate ist derzeit in Vorbereitung.

Zielsetzung und Fragestellung

Mobile Endgeräte können über Lautsprecher und Mikrofon im Ultraschallbereich akustisch Daten übertragen (auch „data over audio“ genannt). Diese Technologie wird mittlerweile auch von großen Anbietern wie etwa Google aktiv genutzt, etwa um genauerer location-based Services zu realisieren. Mit Hilfe von akustischer Datenübertragung kann jedoch auch NutzerInnenverhalten verfolgt (getracked) werden. Akustisches Tracking ist besonders gefährlich und attraktiv für Contentprovider, weil die User von der unhörbaren Datenübertragung nichts mitbekommen. Darüber hinaus können mit akustischem Tracking UserInnen über mehrere Geräte hinweg verfolgt werden. Ziel des Projekts SoniControl ist es Bewusstsein für akustisches Tracking zu schaffen und die Privatsphäre der Internetnutzerinnen durch Erkennung und Filterung von akustischer Datenkommunikation gezielt zu schützen. Im Projekt SoniControl soll eine mobile Anwendung entwickelt werden, die akustische Kommunikation aufspürt, die NutzerInnen darauf aufmerksam macht und auf Wunsch blockiert. Damit möchten wir den NutzerInnen mehr Kontrolle über ihre Privatsphäre im Internet geben.

Verlauf

AP 0: Projektmanagement

Das Projektmanagement beinhaltet unter anderem die regelmäßige Kommunikation mit den Projektmitarbeitern. Dazu wurde ein wöchentliches Jour Fixe eingerichtet, bei dem der aktuelle Status und alle weiteren Schritte besprochen werden. Zum Projektmanagement zählt außerdem das Berichtswesen (Zwischenbericht und Endbericht) sowie die finanzielle Planung, Zusammenstellung von Belegen und Stundenlisten sowie das Controlling. Weitere Aktivitäten beinhalten die Öffentlichkeitsarbeit sowie regelmäßige Updates der Webseite und des Blogs der netidee Webseite.

AP 1: Erstellung Webseite (1.-2.2017)

Zu Beginn des Projekts wurde eine auf Wordpress basierende Webseite für das SoniControl Projekt erstellt, sowie das Logo überarbeitet und an das neue Farbschema der Webseite angepasst. Die Webseite orientiert sich von der Struktur her an einem One-Pager und beinhaltet aktuelle News (Blog), einen „About-Block“ über das Projekt, einen Team-Bereich mit allen Projektmitgliedern inkl. Foto, einen Hinweis auf die Projektfinanzierung (Netidee Logo), sämtliche Ressourcen (Audioaufnahmen, Links, Literatur, eine einseitige Projektbeschreibung mit allen zu erwartenden Projektergebnissen, und zukünftig auch Quellcode und die damit verbundene Dokumentation), ein Kontaktformular und Kontaktdaten. Für die Webseite wurde eine Subdomain an der FH St. Pölten eingerichtet: <http://sonicontrol.fhstp.ac.at>, die auch nach offiziellem Projektende erhalten bleiben wird.

AP 2: Datenakquise (2.-3.2017)

Ziel von AP2 war die Erstellung eines umfangreichen Datensatzes an Ultraschallaufnahmen verschiedener aktueller Ultraschalltechnologien, wie Lisnr, Prontoly und Google Nearby. Der Datensatz soll der Entwicklung des Ultraschalldetektors sowie der Maskierungsalgorithmen (Spoofing) dienen. Durch die Aufnahmen sollen die unterschiedlichen Frequenzen identifiziert werden, welche von verschiedenen Technologien benutzt werden, sowie die Übertragungstechnologie analysiert werden (z.B. Frequency Shift Keying bei Lisnr und Prontoly, Amplitudenmodulation bei Google Nearby).

Im Zuge von AP2 wurden unterschiedliche Typen von Ultraschalldatenkommunikation mithilfe von Apps systematisch im Labor sowie in natürlichen Umgebungen aufgezeichnet. Dabei kamen zwei Nexus 5X Smartphones und zwei Grenzflächenmikrofone zum Einsatz. Zur Überwachung des Aufnahmeprozesses wurde auf einem Mobiltelefon zusätzlich ein Echtzeitspektrogramm¹ angezeigt, um die versendeten Ultraschallsignale auch während der Aufnahmen sichtbar zu machen. Es wurden Aufzeichnungen über verschiedene Abstände (Zentimeter bis mehrere Meter) zwischen Sender und Empfänger erstellt sowie für unterschiedliche Technologien Daten aufgezeichnet (Lisnr, Prontoly, Nearby). Weiters wurde getestet wie weit Ultraschallsignale übertragen werden können. Um ein Set von „sauberen“ (rauschfreien) Signalen zu erhalten, wurden die versendeten Signale außerdem direkt vom Audioprozessor der Smartphones abgegriffen. Dazu mussten die Geräte erst „gerootet“ werden. Zur Aufnahme wurde die Anwendung „RecMe Free Screen Recorder“² verwendet. Für die Ultraschallkommunikationsexperimente haben sich die Apps „Radon“³ und „Thought“⁴ (beide basierend auf Google Nearby) und die „Prontoly“⁵ App als am geeignetsten herausgestellt und wurden

¹ <https://play.google.com/store/apps/details?id=net.galmiza.android.spectrogram>, 7.2017

² <https://play.google.com/store/apps/details?id=com.mobzapp.recme.free>, 7.2017

³ <https://play.google.com/store/apps/details?id=com.nam.radon.app>, 7.2017

⁴ <https://play.google.com/store/apps/details?id=com.exsubstantia.phait.thought>, 7.2017

⁵ <https://play.google.com/store/apps/details?id=com.prontoly.app>, 7.2017

daher in Folge für die Datenakquise verwendet. Die Apps „Drop“ und „Card Case“ wurden ebenfalls getestet, waren aber zu unzuverlässig in der Kommunikation (häufige Abbrüche) und wurden daher nicht für die Datenakquise verwendet. Alle aufgenommenen Signale wurden strukturiert nach Technologie, Übertragungsdistanz und Signalqualität zu einem Audiodatensatz kompiliert. Zusätzlich wurden für alle Audio-files Spektrogramme erstellt, um die Ultraschallsignale sichtbar zu machen. Der Audiodatensatz wurde inklusive Dokumentation auf der SoniControl Webseite unter http://sonicontrol.fhstp.ac.at/wp-content/uploads/2017/04/audio_resources.zip der Öffentlichkeit zur Verfügung gestellt.

AP 3: Literaturrecherche (2.-3.2017)

In AP3 wurde eine umfassende Recherche zum Thema Ultraschalltracking und Ultraschalldatenübertragung durchgeführt, um relevante Technologien, themenverwandte Projekte, sowie wissenschaftliche Arbeiten zu dem Thema zu identifizieren. Im Zuge der Recherche wurden zahlreiche wissenschaftliche Publikationen (vor allem aus dem Sicherheitsbereich) gefunden, welche sich mit „exploits“ (Sicherheitslücken) durch Ultraschallkommunikation beschäftigen. Des Weiteren haben wir zahlreiche Patente z.B. von IBM und Facebook zum Thema Ultraschallkommunikation gefunden. Darüber hinaus konnten neue Technologien (z.B. CopSonic) identifiziert werden, welche Ultraschallkommunikation für location-based Services anbieten. Die Ergebnisse der Studie wurden strukturiert in einem Wiki auf der SoniControl Webseite zusammengestellt. Das Wiki gliedert sich in unterschiedliche thematische Bereiche wie z.B. wissenschaftliche Arbeiten, Technologien, Frameworks (SDKs), Patente, etc. Jeder Literatureintrag beinhaltet u.a. Namen, Beschreibung, optional einen Kommentar und einen Link zur Quelle. Das Wiki ist über den Ressourcenteil der Website erreichbar bzw. unter <http://sonicontrol.fhstp.ac.at/soniwiki>.

AP 4: Prototyp Erkennung (4.-5.2017)

Die Erkennung von codierter digitaler Information im Ultraschallband ist ein nicht-triviales Mustererkennungsproblem, welches besonders dadurch erschwert wird, dass die spezifische Charakteristik der gesendeten Nachrichten sehr unterschiedlich sein kann und im Allgemeinen nicht vorab bekannt sind. Ein guter Detektor muss daher allgemein genug gehalten werden, sodass er nicht nur bereits bekannte Technologien erkennen kann, sondern auch neue, bisher ungesehene Übertragungsformate bzw. Protokolle. Für die Entwicklung des Detektors haben wir eine „Rapid Prototyping“-Plattform (GNU Octave⁶) eingesetzt. Damit konnte viel Entwicklungszeit gespart werden und unterschiedliche Strategien systematisch mithilfe des in AP 2 zusammengestellten Audiodatensatzes ausgetestet werden. Zunächst wurde basierend auf [1] und [2] ein energiebasierter Ansatz implementiert. Es hat sich jedoch herausgestellt, dass dieser Ansatz sehr fehleranfällig in der Gegenwart von Hintergrundrauschen ist was zu vielen Falscherkennungen führt. Basierend auf diesen Erkenntnissen, wurde eine statistische Methode, basierend auf der Divergenz spektraler Verteilungen entwickelt. Außerdem wurde ein spektrales Hintergrundmodell hinzugefügt, welches permanent das Hintergrundrauschen modelliert und sich dynamisch an die Umgebung anpasst. Damit konnte die Erkennungsgenauigkeit signifikant erhöht und die Fehlerrate fast gegen Null gebracht werden. Um einen Test des Detektors unter realistischen Bedingungen zu ermöglichen wurde eine Echtzeit-Implementierung des Detektors basierend auf der GNU LTFAT Audio Bibliothek⁷ in GNU Octave implementiert. Der Echtzeit-Detektor nimmt kontinuierlich vom Mikrofon auf, analysiert das einkommende Audiosignal und erkennt umgehend Aktivität im Ultraschallbereich. Ein Screenshot des Detektors ist in Abbildung 1 dargestellt.

⁶ <https://www.gnu.org/software/octave/>, 7.2017

⁷ <http://ltfat.sourceforge.net/>, 7.2017

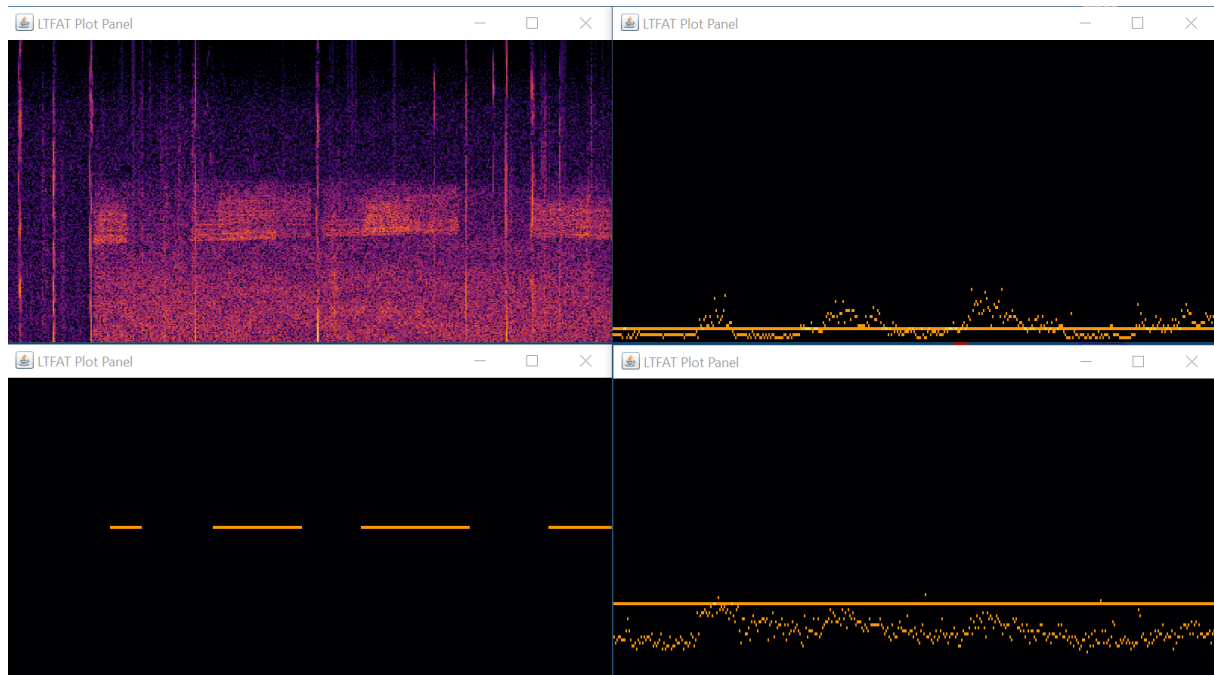


Abbildung 1: Screenshot des prototypischen Echtzeit-Detektors. Oben links ist das eingehende Ultraschallsignal als Spektrogramm zu sehen (vertikal: Frequenz, horizontal: Zeit). Rechts oben und rechts unten sind unterschiedliche Erkennungsmetriken über der Zeit dargestellt, sowie die entsprechenden Erkennungsschwellwerte (horizontale Linien). Der Output des Detektors ist schematisch unten links dargestellt. Die horizontalen Balken in der Mitte des Bildes entsprechen jeweils einer erkannten Nachricht. Im Spektrogramm sind 4 Google Nearby Nachrichten zu sehen. Alle vier können erfolgreich und zeitlich akkurat erkannt werden.

Der entwickelte Prototyp dient als Vorlage für die Implementierung des SoniControl Detektors auf der Zielplattform (Android).

Der Detektor Prototyp ist unter GNU Lizenz auf dem Sourcecode Repository des Projekts (<https://git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl>) öffentlich zugänglich.

AP 5: Prototyp Maskierung (5.-6.2017)

Die Entwicklung des Maskierungsprototypen (Ultraschall-Spoofers) erfolgte parallel in GNU Octave und in Java (Android). Octave diente dabei als Plattform, zur Überprüfung der Werte, die mit dem Android-Prototyp errechnet wurden. Zunächst wurde ein Generator für weißes Rauschen basierend auf der schnellen Fourier Transformation (FFT) implementiert. Die Idee dahinter ist, dass man mit weißem Rauschen bestimmte Frequenzen bzw. Frequenzbänder maskieren kann, sodass auf diesen dann keine Information mehr übertragen werden kann.

Zunächst wurde basierend auf der nativen Audio Library Superpowered⁸ versucht, die gewünschte Funktionalität zu implementieren. Erste Tests zeigten jedoch, dass die notwendige Flexibilität, die wir im Projekt für das Spoofen von unterschiedlichen Übertragungstechnologien benötigen, nicht von Superpowered erfüllt werden kann. Um einen Audiospoofers in Java ohne native Audiobibliothek zu realisieren, wurde die Java Bibliothek JTransforms⁹ verwendet. So konnte eine reine Java-basierte Lösung gefunden werden. Der Spoofers wurde anschließend erweitert, sodass er beliebige Frequenzen und Frequenzbänder separat bespielen kann sowie zeitlich permanent oder alternativ pulsierend (mit

⁸ <http://superpowered.com/>, 7.2017

⁹ <https://github.com/wendykierp/JTransforms>, 7.2017

Pausen) senden kann (zur Energieersparnis). Um hörbare akustische Artefakte des Spoofing-Signals zu eliminieren, wurde eine Hüllkurve über die Amplitude des Signals definiert, welche ein kontinuierliches Ein- und Ausblenden (fade in / fade out) des Maskierungssignals bewirkt. Um Energie zu Rechenzeit zu sparen, wird das Maskierungssignal nur einmal dynamisch erzeugt und dann kontinuierlich beliebig oft und lange abgespielt. Um eine bestimmte Technologie zu maskieren, kann eine vordefinierte Liste von Frequenzen/Frequenzbändern eingelesen werden. Der Spoofer erstellt dann automatisch ein optimales Maskierungsmuster.

Es wurden bereits erste Tests mit dem Spoofer durchgeführt. Dabei wurden zwei Mobiltelefone wie folgt konfiguriert: Beide Telefone betreiben aktiv eine Ultraschallkommunikationsanwendung (z.B. die Prontoly- oder Lisnr-App). Eines der Telefone betreibt zusätzlich den Spoofer auf den entsprechenden Frequenzen. Anschließend wird für unterschiedliche Distanzen und Lautstärken des Spoofing-Signals getestet, ob die Kommunikation zwischen den Apps erfolgreich unterbrochen werden kann. Die Tests waren weitgehend erfolgreich. Ein sensibler Parameter ist die Lautstärke des ausgesendeten Spoofing-Signals. Diese muss zumindest gleich hoch sein, wie jene des Ultraschallsignals der App, damit eine Maskierung erfolgreich ist. Der Prototyp des Spoofers ist in Abbildung 2 zu sehen.

Die Implementierung des Spoofers als Android Komponente ist unter GNU Lizenz auf dem Sourcecode Repository des Projekts (<https://git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl>) öffentlich zugänglich.

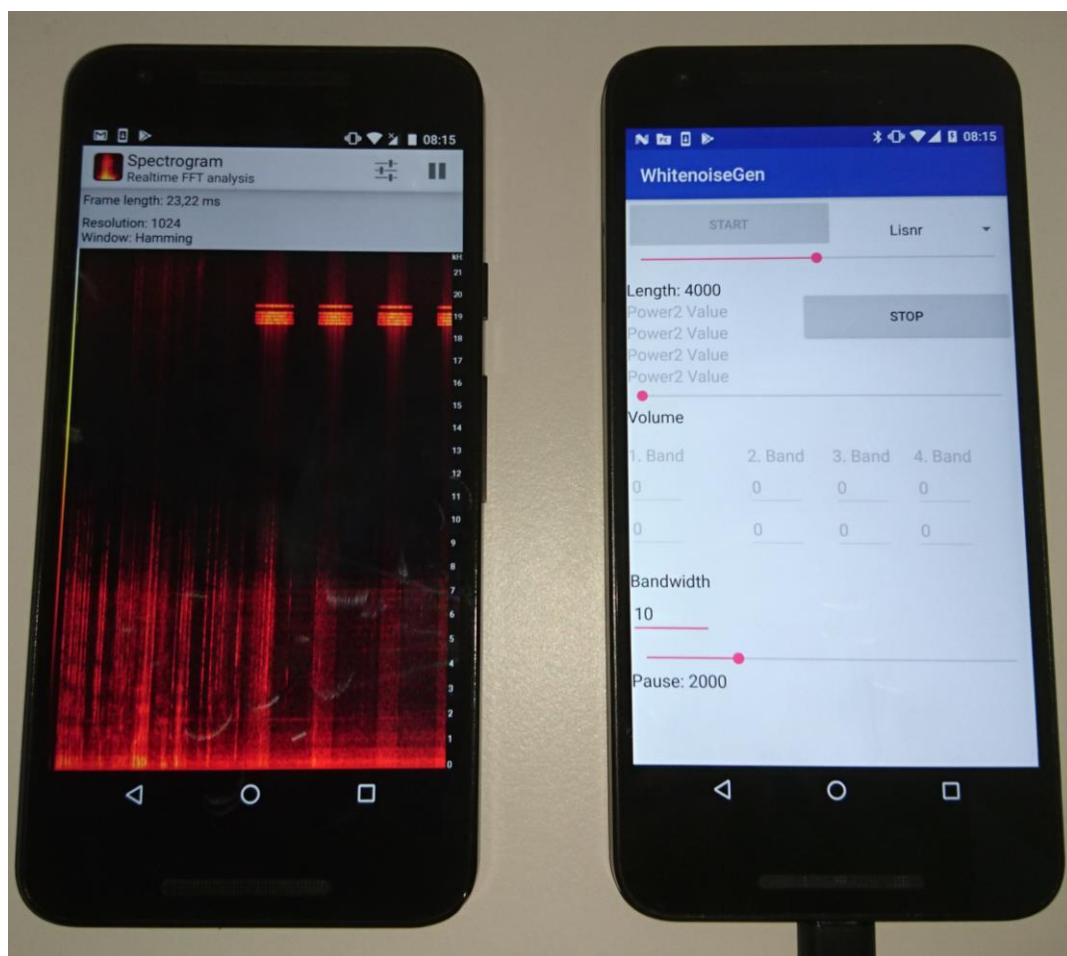


Abbildung 2: Prototyp für die Audiomaskierung. Rechts: das graphische Interface des Prototyps mit allen einstellbaren Parametern. Links: ein Live-Spektrogramm das die ausgesendeten Störsignale (oberer Bereich des Spektrogramms bei 19kHz) in Echtzeit darstellt.

AP 6: Entwicklung Applikationsprototyp (7.-9.2017)

Als Vorbereitung auf die Entwicklung eines Applikationsprototypen und des SoniControl Detektors wurden unterschiedliche Audiobibliotheken für Java, C# und C++ hinsichtlich ihrer Kompatibilität und Audioanalysefunktionalität evaluiert. Abhängig vom Ergebnis dieser Studie wurde dann die endgültige Zieplattform definiert. Folgende Bibliotheken wurden getestet: „Juce“¹⁰, „Superpowered“, „Exocortex DSP“¹¹, „OpenSL ES“¹² und „CSCore“¹³. Das Ergebnis fiel wie folgt aus:

- Juce: sehr gute C++ Bibliothek, leider nicht uneingeschränkt frei nutzbar und teilweise schwer einzubinden.
- Superpowered: sehr umfangreiche C++ Bibliothek, leicht in Java einzubinden (Android Native Interface), Verarbeitungspipeline ist wenig flexibel und schwer an die eigenen Bedürfnisse anzupassen.
- Exocortex DSP: relative alte Implementierung der FFT in C#. Kann theoretisch in cross-platform Entwicklungsumgebungen wie Xamarin integriert werden, allerdings keine weiteren Signalverarbeitungsmethoden.
- OpenSL ES: direkt integriert in Android, vor allem für die Wiedergabe von Audio geeignet, wenig Signalverarbeitungs- und Analysemethoden.
- CSCore: reichhaltige C# Audiobibliothek, leider nicht einbindbar in Xamarin.

Basierend auf dieser Vorstudie fiel die Wahl auf die Superpowered Library für den SoniControl Detektor und auf Android als Zielplattform für die SoniControl Applikation. Cross-Plattform Entwicklung (z.B. mit Xamarin) wurde verworfen, da der damit verbundene Vorteil angesichts der tiefen Verankerung unserer Applikation in das jeweilige Betriebssystem kaum gegeben ist.

Anschließend wurde ein Entwurf für die Softwarearchitektur entwickelt sowie Mockups für die grafische Oberfläche der SoniControl App erstellt. Der Entwurf für die Architektur ist in Abbildung 4 als erweitertes Flussdiagramm dargestellt. Mockups sind in Abbildung 3 zu sehen.

Die Implementierung der SoniControl App wurde in Android durchgeführt. Die gesamte Audioverarbeitung und Detektorlogik wurde nativ in C++ mit Hilfe der Superpowered Bibliothek implementiert und mit dem Java Native Interface (JNI) eingebunden. Der Detektor sowie der Spoofer wurden in separate Threads ausgelagert, um den Applikationsthread für das GUI freizuhalten.

Um einen ersten Prototyp zu erhalten wurde zunächst die Main-Activity implementiert und anschließend der Spoofer aus AP5 als eigener Thread integriert. Anschließend wurde in einem separaten Thread der Detektor implementiert. Bei der Implementierung des Detektors wurde besonders darauf Wert gelegt, dass die Ergebnisse möglichst exakt jene des Detektor-Prototypen in Octave reproduzieren.

¹⁰ <https://www.juce.com>, 7.2017

¹¹ <http://www.exocortex.org/dsp>, 7.2017

¹² <https://developer.android.com/ndk/guides/audio/opensl-for-android.html>, 7.2017

¹³ <https://github.com/filoe/cscore>, 7.2017

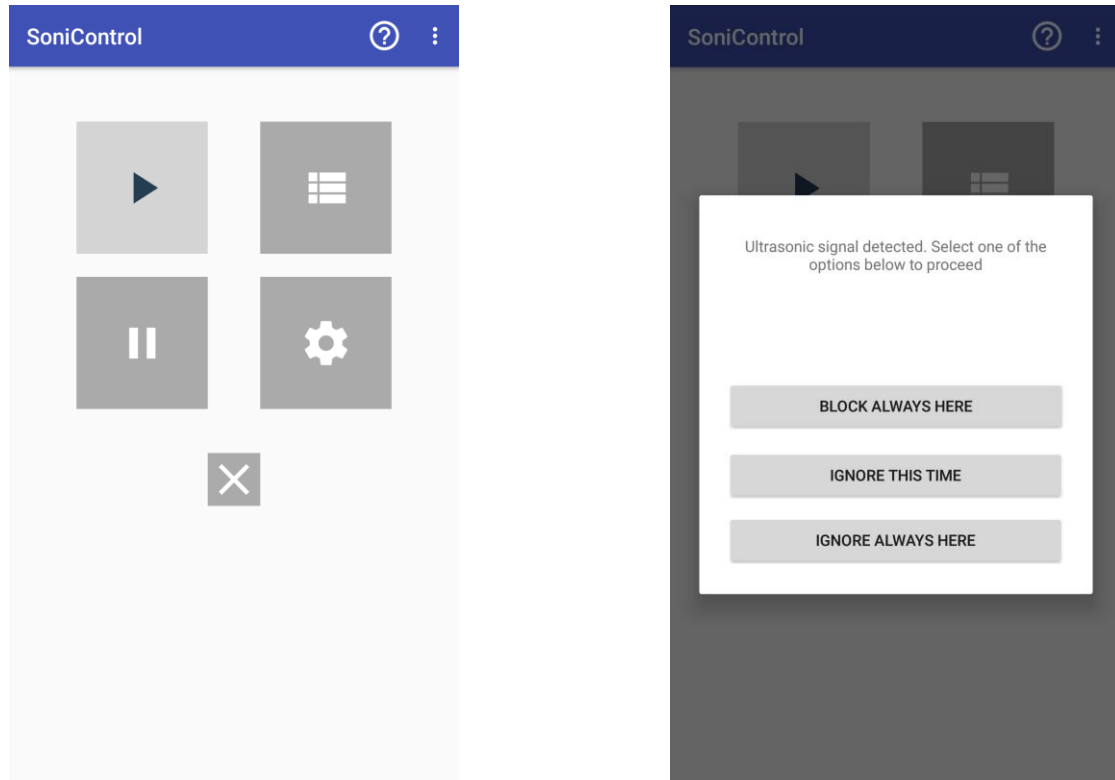


Abbildung 3: Mockups für das grafische Userinterface der SoniControl Firewall

SoniControl System Architecture

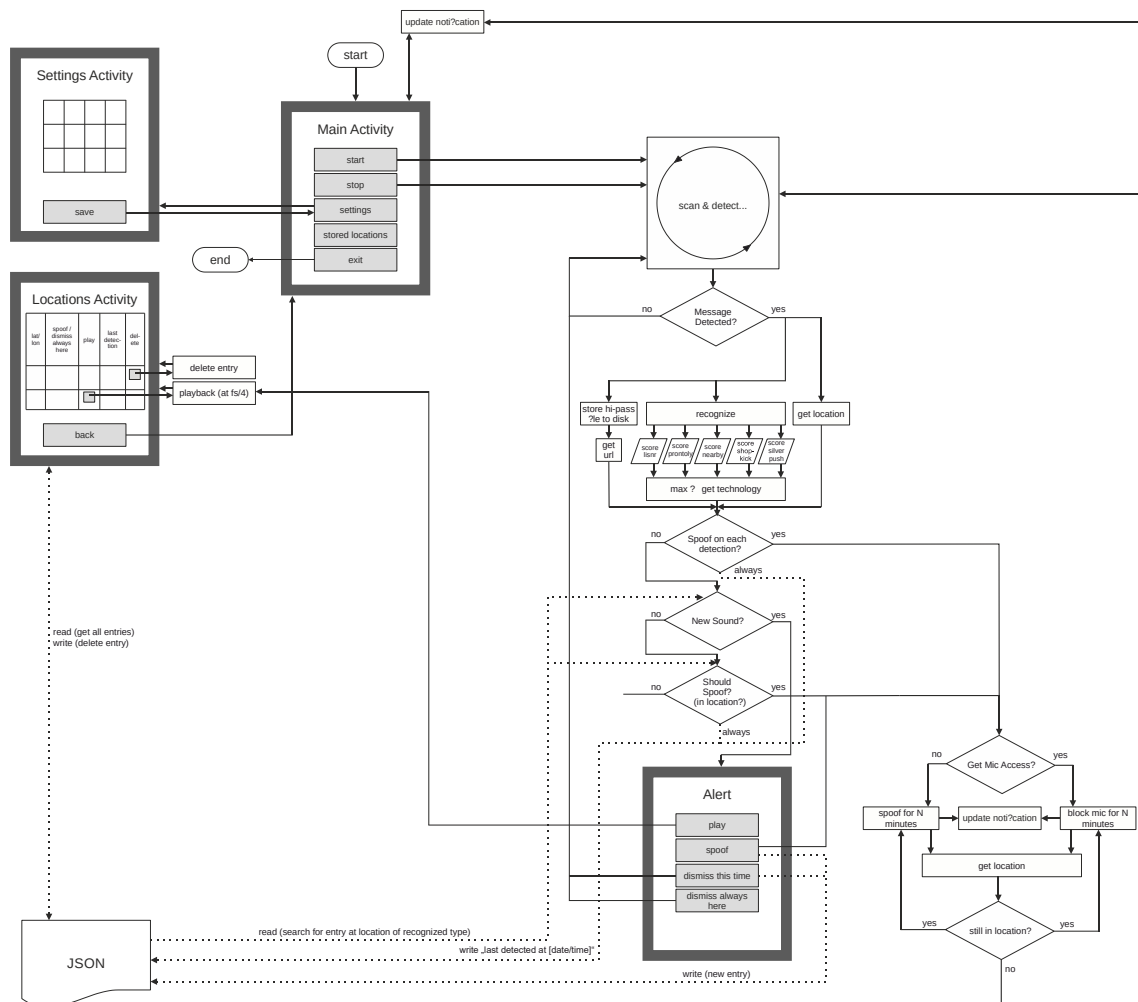


Abbildung 4: Systemarchitektur der SoniControl Firewall

AP 7: Entwicklung Applikation (10.-11.2017)

Die SoniControl Firewall wurde direkt aufbauend auf dem Android-Prototypen aus AP6 entwickelt. Zu der Main-Activity wurde eine Settings-Activity hinzugefügt, über die sämtliche Programmparameter eingestellt werden können. Eine weitere Activity (Location Activity) zeigt alle gespeicherten Erkennungen an. Damit zu jeder Erkennung auch der Ort gespeichert werden kann wurde ein Standortzugriff über wahlweise GPS und/oder das Mobilfunknetz in die Applikation integriert. Jede Erkennung wird zusammen mit dem Ort (sofern von der BenutzerIn erlaubt) lokal gespeichert (als JSON Datei). Auf diese Art und Weise kann in Zukunft automatisiert Kommunikation an bestimmten Orten geblockt werden, sofern eine UserIn das möchte.

Im Falle einer Detektion von Ultraschallkommunikation wird automatisch eine Warnung (Alert) gezeigt. Dieser Alert ermöglicht vier verschiedene Auswahlmöglichkeiten: im Falle einer gewünschten Kommunikation kann die UserIn wählen, die Kommunikation an diesem Ort immer zuzulassen oder nur jetzt Zulassen (das nächste Mal wird dann wieder nachgefragt). Falls die Kommunikation

unerwünscht ist, kann sie permanent blockiert werden (jedes Mal, wenn man an der gegebenen Location ist, z.B. ein bestimmtes Geschäft oder ein bestimmter Ultraschallbeacon an einem Gebäude). Alternativ kann man die Kommunikation auch nur einmalig blockieren.

Die Implementierung lief weitgehend nach Plan. Da SoniControl permanent im Hintergrund läuft mussten besondere Maßnahmen ergriffen werden, dass die Applikation nicht von außen (z.B. vom Android Runtime Management) beendet wird. Die verwendeten Threads alleine stellten sich dafür nicht als hinreichend stabil heraus. Deshalb wurde ein „Foreground“-Service implementiert, welches permanent im Hintergrund läuft und den Status der Applikation konsistent und persistent zur Verfügung stellt.

Zur Reduktion des Energieverbrauchs wurde neben dem akustischen Spoofing eine alternative und besonders effiziente Blockierungsmethode implementiert. Durch Zugriff auf das Mikrofon kann sichergestellt werden, dass keine andere Anwendung ein Ultraschallsignal empfangen kann (da immer nur eine Applikation auf das Mikrofon zugreifen kann, mit Ausnahme der Telefonierfunktion des Smartphones). Durch gezielten Zugriff auf das Mikrofon (jedoch ohne Verarbeitung der einkommenden Daten) kann eine wirksame Blockade erzielt werden. Sollte das Mikrofon jedoch bereits von einer anderen Applikation reserviert sein, ist es nach wie vor notwendig mit Hilfe des akustischen Spoofers eingehende Nachrichten abzuwehren.

Zur besseren Transparenz wurde ein permanent sichtbares Symbol in der Benachrichtigungsleiste eingeblendet, welchen den jeweiligen Status der SoniControl Anwendung darstellt sowie textuelle Benachrichtigungen (Notifications), welche Zusatzinformationen anbieten, siehe Abbildung 5:



Abbildung 5: Statusicons der SoniControl App (von links nach rechts): Ultraschallnachricht erkannt, SoniControl App pausiert, SoniControl App läuft (Detektionsmodus), SoniControl App blockiert aktiv (akustisches Spoofing oder Mikrofonblockierung)

AP 8: Veröffentlichung (12.2017 bis 2.2018)

Nach der Implementierungsphase folgte eine längere Testphase, bei der kleinere Funktionen ausgetauscht, verbessert und hinzugefügt wurden. Seit Jänner 2018 befindet sich die SoniControl App im Google Playstore als „Alpha“-Testversion und wird derzeit von mehreren BenutzerInnen aktiv und kontinuierlich getestet. Die bisherigen Ergebnisse sind vielversprechend. Falscherkennungen sind sehr selten und bisher nur unter extrem schwierigen akustischen Bedingungen zustande gekommen. Die Anwendung läuft sehr stabil, reagiert auch nach langen inaktiven Phasen sofort auf Ultraschallkommunikation und passt sich adaptiv an die umgebende Geräuschkulisse an. Abbildung 6 zeigt wie auf ein einkommendes Ultraschallsignal sofort mit dem akustischen Spoofing begonnen wird. Eine Veröffentlichung als „beta“-Testversion bzw. anschließend als öffentliche und für jede verfügbare App stehen kurz bevor.

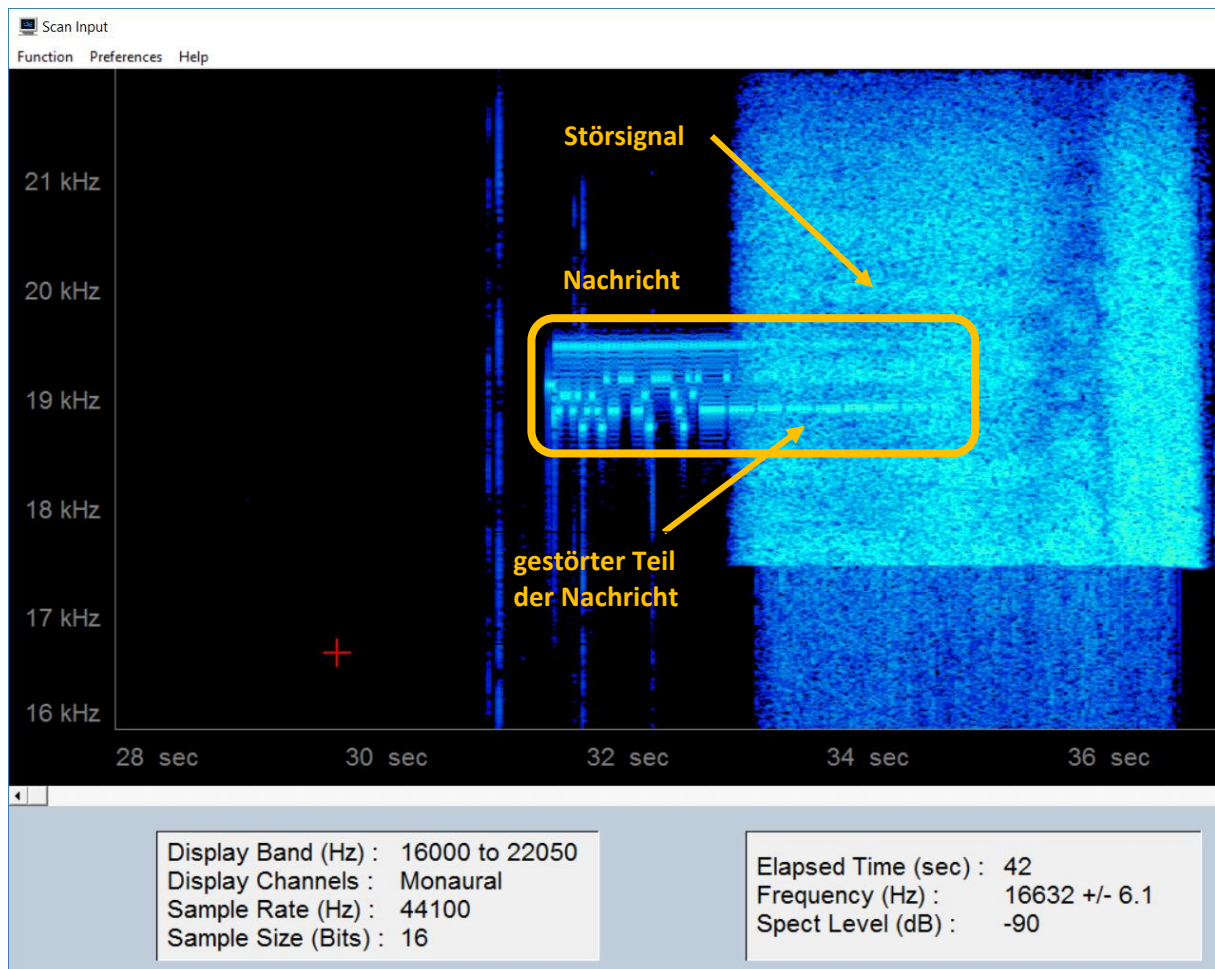


Abbildung 6: Echtzeiterkennung und automatische Blockierung einer Ultraschallnachricht. Nach etwa 1s (Erkennungsperiode) startet der Spoofer mit der automatischen Blockierung mittels Störsignal („preventive spoofing“ Einstellung aktiviert). Die Nachricht kann nicht mehr dekodiert werden, da der restliche Teil zu stark verrauscht ist.

Der Sourcecode der aktuellen „Alpha“-Testversion ist bereits unter GNU Lizenz öffentlich auf unserem GitLab Server verfügbar: <https://git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl>

Inhalt des letzten Arbeitspakets war ebenfalls die Bereitstellung aller noch nicht veröffentlichten Projektergebnisse (z.B. User Dokumentation, Developer Dokumentation, Prototypen, etc.). Alle Ergebnisse inklusive deren Veröffentlichungsort und Lizenz sind in Tabelle 1 aufgelistet.

Projektergebnisse

No.	Beschreibung	Lizenz	Ort
1	Project One-Pager (Projektkurzbeschreibung)	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/wp-content/uploads/2017/07/ProjectOnePager.pdf
2	Literaturüberblick über Ultraschallkommunikation	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/soniwiki
3	Audiodatensatz inkl. Visualisierungen und Dokumentation	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/wp-content/uploads/2017/04/audio_resources.zip
4	Projektwebseite	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at
5	Developer Dokumentation	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/documentation/
6	User Dokumentation	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/documentation/
7	Software Prototypen für die Ultraschallerkennung	GNU Lizenz	https://git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl
8	SoniControl Applikation (Sourcecode, kompilierte Version)	GNU Lizenz	https://git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl , https://play.google.com
9	Projektendbericht	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at

Tabelle 1: Ergebnisse des SoniControl Projekts sowie deren Lizenz und Veröffentlichungsort

Weitere Verwertung und Planung

Die SoniControl Firewall soll demnächst als Beta-Testversion und anschließend als finale App im Google PlayStore angeboten werden und dann von einer größeren Anzahl an UserInnen getestet werden. Die Ergebnisse dieses ersten breiten Tests sollen in die Weiterentwicklung der Firewall einfließen. Die weitere Entwicklung sieht mehrere Richtungen vor. Auf der einen Seite sollen Paketerkennungsfilter in die Firewall eingebaut werden, welche aktuelle und gängige Ultraschalltechnologien erkennen, um so zwischen unterschiedlichen Technologien differenzieren zu können. Auf der anderen Seite planen wir eine Web-Plattform „SoniCloud“ zu etablieren, über welche SoniControl AnwenderInnen ihre Ultraschallerkennungen angereichert mit Geoinformation miteinander teilen können. So soll auf breiter Ebene ein Bewusstsein und Sichtbarkeit für Ultraschallkommunikation geschaffen werden. Eine Diplomarbeit, welche sich mit der Erweiterung der SoniControl Firewall beschäftigt, ist bereits konkret in Planung. Die weitere Entwicklung soll darüber hinaus in Kooperation mit der Open Source Community erfolgen. Interessierte Entwickler können sich direkt an die Projektverantwortlichen unter sonicontrol@fhstp.ac.at wenden. Weitere Verwertungsmöglichkeiten werden in den kommenden Monaten evaluiert. Geplant ist weiters eine Integration von SoniControl in das derzeit parallel laufende Projekt SoniTalk (<http://sonitalk.fhstp.ac.at>).

Veröffentlichungen

Das Projekt SoniControl wurde im Zuge einer **Keynote** auf der Fachkonferenz „The Mobile Enterprise“ im Novomatic Forum in Wien am 8. Juni 2017 von Matthias Zeppelzauer vorgestellt und stieß dort auf großes Interesse. Im September 2017 wurde das Projekt auf dem **Ars Electronica Festival** ausgestellt und dort einer breiten Öffentlichkeit mit einer Livedemonstration präsentiert. Weiters wurde zu

Projektbeginn eine **Presseaussendung** über die APA getätigt, welche zu einem großen Medienecho in Radio, Fernsehen und Zeitungen geführt hat. Im Folgenden sind alle Projektveröffentlichungen zusammengefasst:

Vorträge

- All Around Audio Symposium, St. Pölten University of Applied Sciences, November 29, 2017, Vortragender: Matthias Zeppelzauer
- Netzpolitischer Abend, 11.1.2018, Metalab Wien, Vortragender: Matthias Zeppelzauer

Ausstellungen

- ARS Electronica Festival 7.9.2018-11.9.2018, Linz
- Tag der offenen Tür, Bundesministerium für Wissenschaft, Forschung und Wirtschaft (BMFWF), 26.11.2017, Wien

Radioberichte

- [Netidee prämiiert 23 Internet-Projekte](#), Campus Radio FH St.Pölten, 23.11.2017
- [Smartphones am Lauschen hindern: Campus Talk mit Matthias Zeppelzauer zum Projekt SoniControl.](#), Campus Radio FH St.Pölten, 21.08.2017
- [Wie Ultraschallmaskierung Audiotracking verhindert](#), Deutschlandradio, 17.12.2016
- [Handy-Tracking-Abwehr der FH St. Pölten](#), Ö1 Morgenjournal II, 16.12.2016
- [Neues Projekt der FH St. Pölten: "SoniControl"](#), Radio Niederösterreich Mittagsmagazin, 16.12.2016
- [FH St. Pölten lässt mit interessanter Entwicklung aufhorchen](#), Radio Arabella Niederösterreich, 13.12.2016
- [Digital.Leben - Ideen für das Internet Netidee Gala 2016](#), Ö1, 21.11.2016

Fernsehberichte

- [Wenn das Handy heimlich zuhört](#), P3tv, 13.12.2016

Zeitungsberichte

- [Jung-Forscher zeigten Abhör-Schutz & Bio-Bildschirm](#), noen.at, 22.09.2017
- [Projekt SoniControl – Audiotracking durch Smartphones](#), land-der-erfinder.at, 31.08.2017
- [Lasst uns stören!](#), factorynet.at, 08.09.2017
- [FH St. Pölten beim Ars-Electronica-Festival](#), MeinBezirk.at, 17.08.2017
- [How smartphone apps spy on users by listening to inaudible signals](#), techworld.com, 14.08.2017
- [SoniControl: FH St. Pölten will heimliches Audiotracking stoppen](#), factorynet.at, 09.01.2017
- [Online-Helden: Initiativen für ein „besseres“ Internet](#), Der Brutkasten, 22.12.2016
- [Damit das Handy nicht mehr mithört](#), Die Presse, 16.12.2017
- [FH St. Pölten - Wenn das Handy heimlich zuhört](#), noen.at, 15.12.2016
- [Unser Handy hört heimlich zu](#), scinexx.de, 8.12.2016
- [App soll Audiotracking auf dem Smartphone verhindern](#), PC Welt, 8.12.2016
- [App soll Audiotracking auf dem Smartphone verhindern](#), Macwelt, 8.12.2016
- [App soll „Spion Handy“ zur Strecke bringen](#), Computerwoche, 8.12.2016

- [Gläserne User durch Audio-Cookies: App der FH St. Pölten schafft Abhilfe](#), Der neue Mann, 8.12.2016
- [Dem Handy die Ohren zuhalten](#), business-panorama.de, 7.12.2016
- [Wenn das Handy heimlich zuhört: Abwehr ungewollten Audiotrackings durch akustische Cookies](#), innovations-report.de, 7.12.2016
- [Fachhochschule St. Pölten entwickelt Handy-App gegen heimliches Audiotracking](#), derStandard.at, 7.12.2016
- [Gläserne User durch Audio-Cookies: App der FH St. Pölten schafft Abhilfe](#), Horizont, 7.12.2016
- [Wenn das Handy heimlich zuhört: Abwehr ungewollten Audiotrackings durch akustische Cookies](#), Extrem News, 7.12.2016
- [Wenn das Handy heimlich zuhört](#), orf.at, 7.12.2016
- [Platz 1 für SoniControl bei Wettbewerb der netidee](#), FH St.Pölten, 22.11.2016

Partnerschaften

Im Zuge des Projekts konnten bereits mehrere Partnerschaften aufgebaut werden:

- Wir haben eine Kooperation mit Forschern der TU Braunschweig (tu-braunschweig.de) etabliert, welche im Mai 2017 eine umfangreiche Studie zum Thema Ultraschallkommunikation veröffentlicht haben [3]. Die Forscher haben zahlreiche Mobile Apps auf deren Fähigkeiten hin untersucht über Ultraschall zu kommunizieren und haben eine starke Verbreitung von Ultraschalltracking in heutigen Apps festgestellt. Die Forscher haben uns ihre Forschungsergebnisse zur Verfügung gestellt. Gemeinsam besteht ein Interesse an einer zukünftigen Kooperation.
- Wir haben im Zuge des Projekts eine Kooperation mit dem Verein für Konsumenteninformation (www.vki.at) aufgebaut und diese zu Produkten beraten, welche Ultraschall zur Datenübertragung einsetzen.

Zusammenfassung

Das Projekt SoniControl war sowohl inhaltlich als auch vom Echo der Medien und der BesucherInnen bei unseren Livedemonstrationen ein großer Erfolg. Die Implementierung der Firewall stellte sich als anspruchsvoller heraus als ursprünglich angenommen. Dennoch konnte der Zeitplan eingehalten werden. Alle im Projektantrag definierten Erfolgsmesskriterien konnten erfüllt werden und somit eine erste lauffähige Ultraschallfirewall realisiert werden. Besonders angenehm stellte sich die Kooperation mit dem Fördergeber netidee.at bzw. IPA dar, welcher beispielsweise durch die Ermöglichung der Ausstellung auf der ARS Electronica signifikant zur Dissemination des Projekts beigetragen hat und wofür an dieser Stelle explizit gedankt werden soll.

Lizenz

Der Inhalt dieses Dokuments steht unter [Creative Commons Attribution-NonCommercial 4.0 License](#).

Referenzen

- [1] Carrara, B. C., & Adams, C. (2015, June). On characterizing and measuring out-of-band covert channels. In Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security (pp. 43-54). ACM.
- [2] Urkowitz, H. (1967). Energy detection of unknown deterministic signals. Proceedings of the IEEE, 55(4), 523-531.
- [3] Arp, D., Quiring, E., Wressnegger, C., & Rieck, K. (2017, April). Privacy threats through ultrasonic side channels on mobile devices. In Security and Privacy (EuroS&P), 2017 IEEE European Symposium on (pp. 35-47). IEEE.

Einseitige Projektzusammenfassung



Novel technologies like Google Nearby and Silverpush build upon ultrasonic sounds to exchange information. More and more of our devices communicate via this inaudible communication channel. Ultrasonic communication enables to pair devices, exchange information but also to track users and their behavior across several devices similar to cookies in the web. Every device with a microphone and a speaker is able to send and receive ultrasonic information. The user is usually not aware of this inaudible and hidden data transfer. To overcome this gap, within the project SoniControl we research the current capabilities of ultrasonic communication and raise awareness for this unknown communication channel. To date there is no technology available that detects ultrasonic communication and that enables the user to protect his or her privacy. We develop a mobile application that detects ultrasonic activity, notifies the user and blocks the information on demand. Thereby, we want to raise the awareness for this novel technology and help users to protect their privacy.

All information about the SoniControl Project can be found on the project website: <http://sonicontrol.fhstp.ac.at>. The website provides general information as well as a number of resources (project deliverables) listed in the following:

No.	Description	License	Location
1	Project One-Pager (short description of the project, i.e. this document)	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at
2	Literature survey on ultrasonic communication technologies	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/soniwiki
3	Audio dataset of ultrasonic recordings with visualizations, including documentation	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/wp-content/uploads/2017/04/audio_resources.zip
4	Developer documentation	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/documentation/
5	User documentation	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at/documentation/
6	Software prototypes for detection of ultrasonic cookies	GNU License	https://git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl
7	SoniControl Application (complete source code, compiled application)	GNU License	https://git.nwt.fhstp.ac.at/m.zeppelzauer/SoniControl , https://play.google.com
8	Final Project Report	CC BY-SA 3.0	http://sonicontrol.fhstp.ac.at



Contact
 email: Matthias.zeppelzauer@fhstp.ac.at
 web: <http://mc.fhstp.ac.at/people/matthias-zeppelzauer>

