Sommersemester 2018

Seminar IT-Sicherheit

When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals

–

Ermitteln eines Passworts mittels des WindTalker-Frameworks

Eingereicht von:
Vitus Jonassen Wittke
winf101936@fh-wedel.de

Betreut von:
Prof. Dr. Gerd Beuster

Eingereicht am:
31.05.2018

INHALTSVERZEICHNIS

EINLEITUNG

Mobilgeräte werden in zunehmendem Maße für Transaktionen mit sensiblen Daten, wie etwa Online-Banking oder Online-Shopping, eingesetzt. Daher existieren diverse direkte und indirekte Verfahren die auf fremden Mobilgeräten eingegebenen sensiblen Informationen zu ermitteln. Während direkte Verfahren darauf abzielen die Eingabe selbst wahrzunehmen, bedienen sich indirekte Verfahren sogenannter Side-Channels um Rückschlüsse auf die eingegebenen Informationen zu ziehen.

Viele dieser indirekten Verfahren erfordern es das Zielgerät mit Spyware zu kompromittieren oder spezielle Sensoren in unmittelbarer Nähe des Zielgeräts zu platzieren. Weiterhin sind viele dieser Verfahren auch nicht in der Lage zu erkennen wann die Eingabe sensibler Daten erfolgt und daher auch nicht in der Lage gezielt nur diese Daten auslesen. Trotz teilweise sehr guter Erkennungsraten, stellen diese Voraussetzungen und Einschränkungen eine Hürde dar diese Verfahren erfolgreich in der Praxis einzusetzen.

Das von einer Gruppe aus chinesischen und amerikanischen Wissenschaftlern in 2016 vorgestellte Framework „WindTalker“ unterliegt vielen dieser Einschränkungen nicht. Das Thema dieser Seminararbeit ist der von Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu und Na Ruan verfasste Artikel „When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals“ [LML16] in dem dieses Framework vorgestellt wird.

Diese Seminararbeit geht zunächst auf die Begriffe „Side-Channel Attacks“ und „Channel State Information“ ein und gibt anschließend einen Überblick über die allgemeine Funktionsweise von „WindTalker“. Diese Funktionsweise wird daraufhin mit anderen indirekten Verfahren verglichen. Im Anschluss wird der vierteilige Prozess der Passwortermittlung detailliert erläutert. Dem schließt sich eine Evaluation der Leistungsfähigkeit von „WindTalker“ in kontrollierter und realitätsnaher Umgebung an. Den Abschluss bildet eine Zusammenfassung.

CCS'16, October 24-28, 2016, Vienna, Austria.
© 2016 ACM. ISBN 978-1-4503-4139-4/16/10. . . $15.00
DOI: http://dx.doi.org/10.1145/2976749.2978397

MobiCom'15, September 7–11, 2015, Paris, France.
© 2015 ACM. ISBN 978-1-4503-3619-2/15/09 ...$15.00.
DOI: http://dx.doi.org/10.1145/2789168.2790109

GRUNDLAGEN

Side-Channel Attacks

Side-Channel Attacks stellen kryptoanalytische Methoden dar, deren Ziel es ist mittels an kryptologischen Geräten beobachtbaren Daten verwendete Schlüssel oder verarbeitete Daten zu ermitteln [OHW16]. Die Kanäle auf denen die Daten beobachtet werden können nennen sich dabei „Side-Channels“. Das Konzept erlangte durch den amerikanischen Kryptologen Paul C. Kocher und seiner 1996 veröffentlichte Arbeit „Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems“ [Koc96] Bekanntheit.

Die von Kocher veröffentlichte Arbeit beschäftigt sich dabei mit sogenannten „Timing Attacks“, die es durch den Einfluss von verwendeten Schlüsseln und Eingabedaten auf die Verarbeitungszeit eines kryptologischen Geräts ermöglichen den verwendeten Schlüssel zu rekonstruieren. Neben „Timing Attacks“ existieren noch diverse andere Angriffe auf diverse andere „Side-Channels“. So können unter anderem über den vom kryptologischen Gerät während der Verarbeitung verbrauchten Strom, die ausgesandten akustischen oder optischen Signale und dem genutzten Speicher Rückschlüsse auf Schlüssel und Eingabedaten gezogen werden. Die von „WindTalker“ genutzten „Channel State Information“ sind auch Ziel einiger Verfahren.

Channel State Information

Channel State Information stellen die Informationen zum Zustand eines Kommunikationskanals dar. Im Falle von WiFi-Signalen werden die „Channel State Information“ für jeden Unterträger gemessen. Durch die im WiFi Standard IEEE 802.11n [IEEE802] definierten Verfahren wie „Multiple-Input Multiple-Output“ (MIMO) und „Orthogonal Frequency Division Multiplexing“ (OFDM) erhöht sich die Anzahl der Unterträger stark, da sie sich aus dem Produkt aus der im Netzwerk vorhandenen Sendeantennen, Empfangsantennen und OFDM-Unterträgern ergibt.

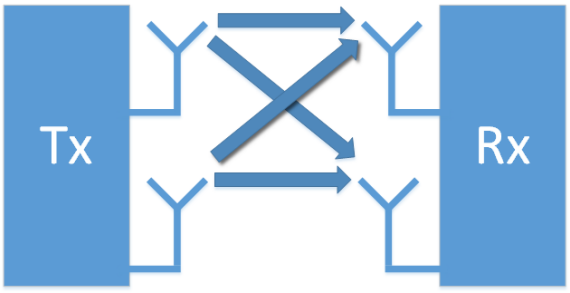

Abbildung 1: MIMO Funktionsweise

„Multiple-Input Multiple-Output“ ist dabei ein Verfahren bei dem zur drahtlosen Kommunikation mehrere Sende- und Empfangsantennen eingesetzt werden, wie in Abbildung 1 zu sehen ist. Der Einsatz mehrerer Antennen ermöglicht es neben der Erhöhung der Kanalkapazität durch gleichzeitiges Senden verschiedener Informationen auch durch Mehrwegausbreitung verursachte Signalauslöschung zu vermeiden, da es statistisch unwahrscheinlich ist, dass alle verwendeten Antennen von diesem Effekt betroffen sind. Tatsächlich können die klassischerweise negativen Effekte der Mehrwegausbreitung mit mehreren Sende- und Empfangsantennen genutzt werden, um die Kanalkapazität nochmals zu steigern [GSS03].

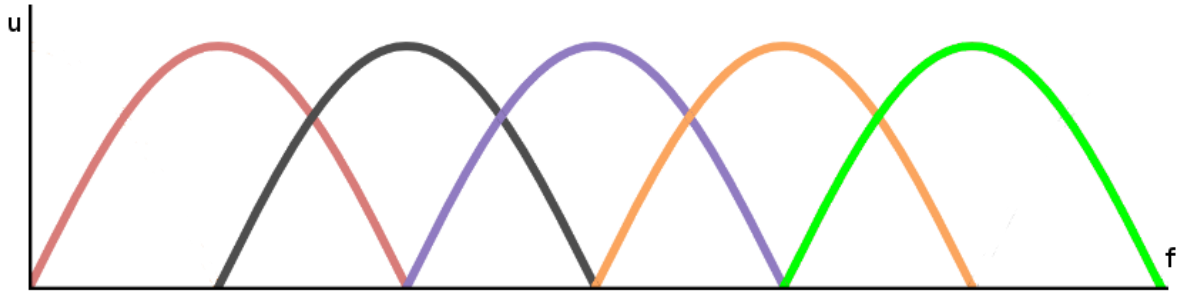

Abbildung 2: Orthogonale Frequenzen der Unterträger

„Orthogonal Frequency Division Multiplexing“ ist ein Verfahren bei dem die zu übertragenden Informationen auf Teildatenströme mit niedrigerer Datenrate aufgeteilt werden. Diese Teildatenströme werden anschließend über einzelne Unterträger gesendet. Damit die übertragenen Datenströme vom Empfänger unterschieden werden können, müssen die Träger, wie auf Abbildung 2 zu erkennen ist, orthogonal zueinander im Funktionenraum stehen. Das heißt, dass ihre Mittenfrequenz im Nulldurchgang der benachbarten Unterträger liegen muss. Der Einsatz dieses Verfahrens lässt Übertragungssysteme relativ unempfindlich gegenüber schmalbandigen Störungen werden, da die Informationen weiter über die nicht beeinflussten Unterträger gesendet werden können. Ein solcher Ausfall eines Unterträgers führt zwar zu einer geringeren Kanalkapazität, schränkt die Übertragung aber in keiner anderen Weise ein [LAB95].

Die „Channel State Information“ werden aus dem Frequenzgang für jeden Unterträger gewonnen. Der Frequenzgang ist hierbei der Quotient aus dem diskret fouriertransformierten gesendeten und empfangenen Signal und beschreibt den Zusammenhang zwischen diesen beiden Signalen. Bei der diskreten Fouriertransformation wird ein zeitdiskretes endliches Signal auf ein Frequenzspektrum abgebildet [Liz11]. Dieses Frequenzspektrum lässt sich als Gruppe von Sinusoiden veranschaulichen (Abbildung 3 und 4).

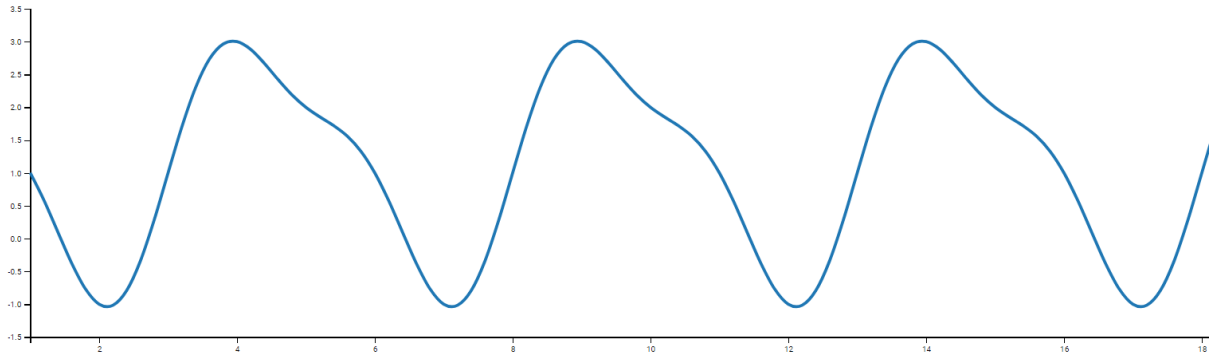

Abbildung 3: Ursprüngliches Signal *X*

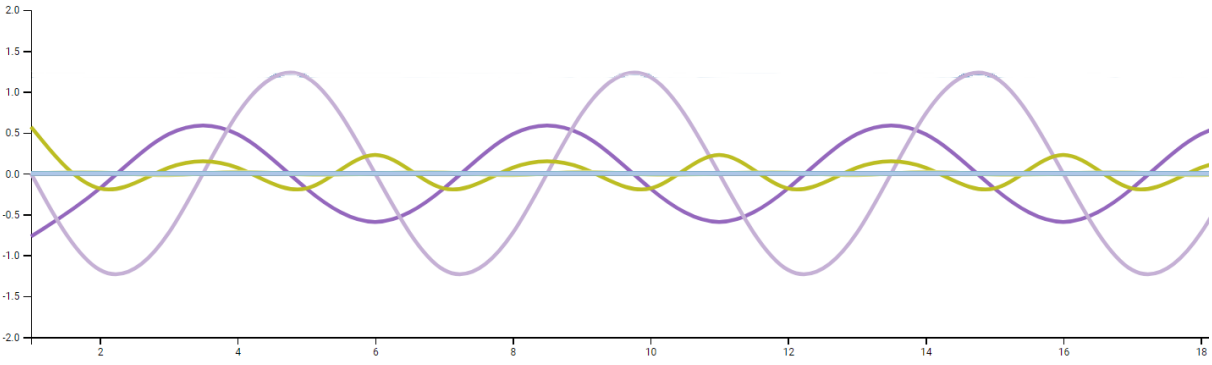

Abbildung 4: In Sinusoide zerlegtes Signal *X*

Wenn $X(f,t)$ und $Y(f,t)$ die fouriertransformierten gesendeten bzw. empfangenen Signale für den Unterträger f über die Zeit t darstellen, ergeben sich die CSI $H(f,t)$ folgendermaßen:

$$H(f,t) = \frac{Y(f,t)}{X(f,t)}$$

WindTalker verwendet hiervon lediglich den Amplitudengang, also das Verhältnis der Amplituden von gesendetem und empfangenem Signal. Der hierdurch ebenfalls bestimmbare Phasengang, also das Verhältnis der Phasen von gesendetem und empfangenem Signal, wird nicht zur Ermittlung der Eingaben verwendet.

WINDTALKER IN DER THEORIE

Allgemeine Funktionsweise

WindTalker läuft auf einem Laptop, der ein öffentliches WiFi-Signal zur Verfügung stellt mit dem sich die potenziellen Zielgeräte verbinden können. Während die Verbindung zum Ziel besteht, werden mithilfe eines speziellen Tools und dem im Laptop installierten NIC kontinuierlich CSI gesammelt, da die Fingerbewegungen bei Eingaben auf verbundenen Geräten einen deutlichen Einfluss auf diese haben. Nebenbei läuft außerdem ein Packet-Sniffer, der anhand der Ziel-IPs der einzelnen Packets feststellen kann, ob zurzeit mit einer sensiblen IP-Adresse kommuniziert wird.

Alle in diesem sensiblen Zeitfenster gesammelten CSI werden vorverarbeitet und anschließend von einem Klassifikator zur Ermittlung der getätigten Eingaben verwendet. Der Klassifikator vergleicht dabei die CSI-Kurvenverläufe der einzelnen, durch die Vorverarbeitung identifizierten, Eingabezeitfenster mit den Kurvenverläufen der von der Zielperson erlangten Trainingsdaten und ordnet diese mit gewissen Wahrscheinlichkeiten bestimmten Eingaben zu. Diese Trainingsdaten müssen in möglichst großer Anzahl vom Ziel des Angriffs erlangt werden, da eine größere Menge Trainingsdaten einen positiven Einfluss auf die Erkennungsrate hat.

Vergleichbare Verfahren

Es existieren diverse andere Verfahren, die sich ebenfalls gewisser Side-Channels bedienen, um Rückschlüsse auf getätigte sensible Eingaben ziehen zu können. So gibt es Verfahren, die sich akustischer [LWK15] oder optischer [YLF14] Signale bedienen. Auch die von den Bewegungssensoren eines Mobilgeräts aufgezeichneten Daten können zur Ermittlung getätigter sensibler Eingaben verwendet werden [OHD12].

Ein Nachteil vieler dieser Verfahren ist die Notwendigkeit das Zielgerät mit entsprechender Spyware zu kompromittieren oder entsprechende Sensoren in unmittelbarer Nähe des Zielgeräts anzubringen. Diese Voraussetzungen in einer Weise, die die Zielperson nicht bemerkt, herzustellen ist mit relativ großem Aufwand verbunden und macht viele dieser Verfahren somit praxisuntauglich.

Neben WindTalker gibt es noch zwei sehr ähnliche Verfahren zur Ermittlung getätigter sensibler Eingaben, die sich CSI bedienen. Bei diesen beiden Verfahren handelt es sich allerdings, im Gegensatz zu WindTalker, um Out-of-band keystroke inference (OKI) Verfahren bei denen das Zielgerät nicht mit einem vom Angreifer gestellten WiFi-Signal verbunden ist. Bei WindTalker handelt es sich demnach um ein In-band keystroke inference (IKI) Verfahren, da das Zielgerät hierbei mit einem solchen WiFi-Signal verbunden.

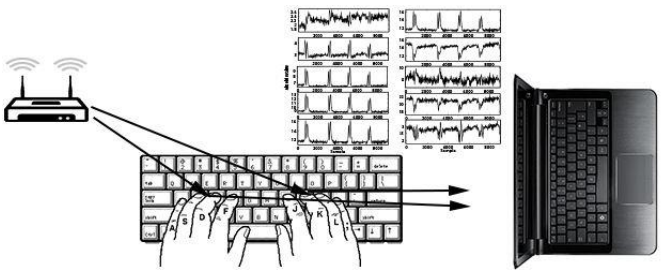

Abbildung 5: Funktionsweise von "WiKey" aus [ALW15]

Das erste dieser Verfahren nennt sich „WiKey“ und basiert wie WindTalker auf der Ermittlung der getätigten sensiblen Eingaben anhand der durch Fingerbewegungen entstandenen Einflüsse auf die CSI [ALW15]. Da das Zielgerät hierbei nicht selbst mit dem WiFi-Signal verbunden ist und somit selbst keine CSI liefern kann, muss das Ziel zwischen einem WiFi-Router und einem WiFi-Empfänger platziert werden (Abbildung 5). Die vom Empfänger gesammelten CSI sind dadurch, dass sie durch die Position von Sender und Empfänger das Zielgerät passieren müssen, in entsprechender Weise durch die Eingaben auf dem Zielgerät beeinflusst. Zur Ermittlung der sensiblen Eingaben ist es notwendig die CSI des gesamten Aufzeichnungszeitraums zu verwenden, da mangels Packet-Sniffing nicht ermittelt werden kann, in welchem Zeitraum die sensiblen Eingaben getätigt wurden. Die schlussendliche Ermittlung der Eingaben verläuft wie bei WindTalker über einen Klassifikator, der anhand der Ähnlichkeit zu den Trainingsdaten die Eingaben ermittelt.

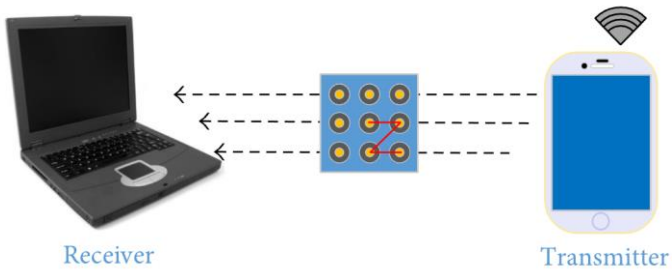

Abbildung 6: Funktionsweise von "WiPass" aus [ZZT16]

Das zweite Verfahren heißt „WiPass“ und ist „WiKey“ sehr ähnlich, da es auf dem gleichen Prinzip basiert [ZZT16]. Es bietet durch die Verwendung eines durch ein Mobilgerät erzeugten Hotspots (Abbildung 6) statt eines WiFi-Routers größere Flexibilität in der Platzierung des Senders, unterscheidet sich aber ansonsten kaum von „WiKey“. Beide Verfahren sind in der Lage unter guten Bedingungen sehr hohe Erkennungsraten zu erzielen.

ABLAUF EINES ANGRIFFS

Erkennen des sensiblen Zeitfensters

Wenn das Zielgerät mit dem, zu WindTalker gehörigen, WiFi-Signal verbunden ist, ist es möglich die vom Zielgerät gesendeten Packets zu untersuchen. Sensible Daten lassen sich aufgrund der für diese meist verwendete HTTPS-Verschlüsselung nicht auslesen. Da die Packets weitergeleitet werden müssen, sind die Ziel-IP-Adressen jedoch frei sichtbar. Anhand dieser Ziel-IP-Adressen kann WindTalker per Packet-Sniffing feststellen, ob das Packet an eine IP-Adresse, die im verwalteten Pool sensibler IP-Adressen ist, versendet wird.

Sobald vom Zielgerät Packets an eine sensible IP-Adresse geschickt werden, zeichnet WindTalker den Start- und Endzeitpunkt dieser Kommunikation auf. Für die nachfolgende Analyse der CSI müssen somit nur die in diesem Zeitraum gesammelten CSI berücksichtigt werden.

Erlangen der CSI per ICMP

Während die Verbindung zum, zu WindTalker gehörigen, WiFi-Signal besteht, werden mittels ICMP Echo Requests [Bra89] CSI vom Zielgerät gesammelt. In Versuchen hat sich eine Frequenz von 800 ICMP Echo Requests pro Sekunde als optimal erwiesen. Diese Frequenz mag relativ hoch erscheinen, wirkt sich aufgrund der sehr geringen Packetsize nur minimal auf die verfügbare Bandbreite aus. Ein 98 Byte großes ICMP Packet 800-mal pro Sekunde zu verschicken, braucht lediglich 78,4 kB/s, was bei den Übertragungsraten aktueller WiFi Standards, wie 802.11n oder 802.11ac, nur einen Bruchteil der maximalen Übertragungsleistung ausmacht.

Um möglichst viele Interferenzen beim Sammeln der CSI zu vermeiden, wird eine der üblichen Rundstrahlantennen durch eine auf das Ziel gerichtete Richtantenne ausgetauscht. Diese schränkt den Zielbereich zwar ein, sorgt aber für deutlich rauschfreiere CSI.

Vorverarbeitung der Daten

Gewöhnliche Netzwerkhardware sorgt für ein hochfrequentes Rauschen in den CSI. Da WindTalker auf gewöhnlicher Netzwerkhardware läuft ist es notwendig dieses hochfrequente Rauschen zu reduzieren. Dies lässt sich mit einem Tiefpassfilter erreichen, da dieser die, im niedrigen Frequenzspektrum befindlichen, Einflüsse der Fingerbewegungen auf die CSI kaum beeinflusst, das im hohen Frequenzspektrum befindliche Rauschen aber deutlich reduziert. Hierzu wird ein Butterworth-Tiefpassfilter eingesetzt [But30].

Nach Reduktion des Rauschens verbleibt das Problem der unüberschaubaren Menge der Daten, da CSI für jeden OFDM-Unterträger pro Antennenpaar mit 800 Samples pro Sekunde aufgezeichnet werden. Diese große Datenmenge weiterzuverarbeiten, wäre äußerst rechenaufwändig, ineffizient und würde durch den großen Anteil an insignifikanten Daten zu schlechten Ergebnissen führen.

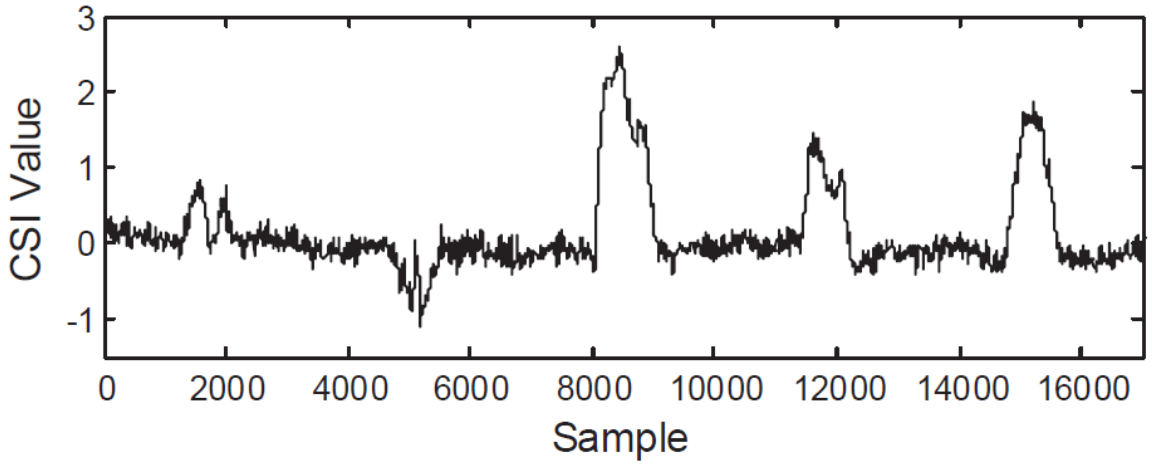

Abbildung 7: CSI-Zeitreihe nach Hauptkomponentenanalyse aus [LML16]

Per Hauptkomponentenanalyse lässt sich die Dimensionalität der Daten deutlich reduzieren, da am Ende nur noch wenige Komponenten mit einer starken Korrelation zwischen CSI-Kurvenverlauf und den getätigten Fingerbewegungen übrigbleiben [Smi02]. Die größte Korrelation findet sich bei vier ausgewählten Eigenwerten bei den ersten Komponenten, während der Rest meist nur Rauschen ist. Von diesen vier Komponenten wird die erste Komponente ausgewählt, da sie meist die größten Veränderungen in den CSI aufweist, ohne dabei ein starkes Rauschen aufzuweisen. Sollte die ausgewählte Komponente jedoch, wider Erwarten, sehr starkes Rauschen aufweisen, wird die jeweils nächste Komponente zur weiteren Analyse ausgewählt. Das Ergebnis der Hauptkomponentenanalyse ist in Abbildung 7 zu sehen.

Ermitteln des Tastendrucks

Nach der Vorverarbeitung der CSI lässt sich feststellen, dass der Kurvenverlauf zwar eine gut sichtbare Korrelation zu den einzelnen Tastendrücken aufweist, die für den Klassifikator entscheidende Identifikation des Anfangs- und Endpunkts des Tastendrucks jedoch aufgrund der starken Veränderungen in der Wahrscheinlichkeitsverteilung im Eingabezeitfenster nicht mit herkömmlichen Burst-Erkennungsverfahren möglich ist. Daher wird zur Ermittlung der Start- und Endpunkte der Tastendrücke ein, eigens dafür konzipiertes, dreistufiges Verfahren eingesetzt.

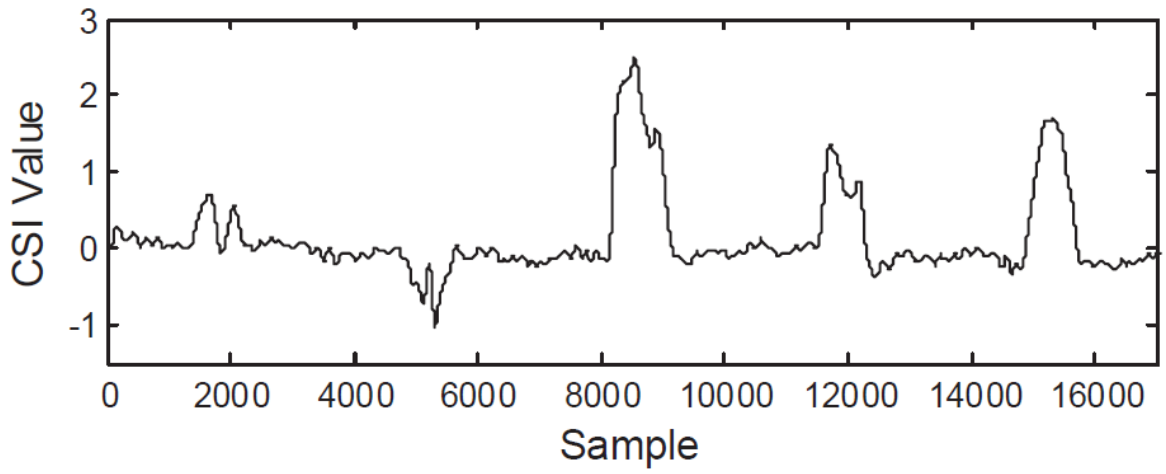

Abbildung 8: Ergebnis der Anwendung des "Waveform Profile Building" aus [LML16]

Der erste Schritt nennt sich „Waveform Profile Building“ und hat zum Ziel das Rauschen in den CSI weiter zu reduzieren, da dieses, trotz der vorhergehenden Schritte, immer noch klar vorhanden ist. Zur Reduktion des Rauschens wird, wie schon zuvor, ein Butterworth-Tiefpassfilter eingesetzt, da dieser die niedrigfrequenten durch Fingerbewegungen verursachten Veränderungen wenig beeinflusst (Abbildung 8).

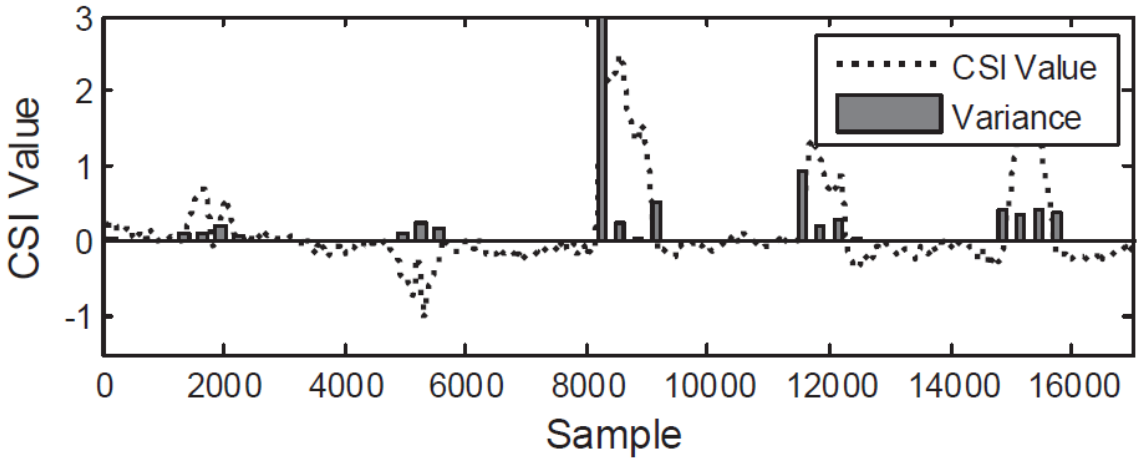

Abbildung 9: Untersuchung der Varianz der einzelnen Segmente aus [LML16]

Im zweiten „CSI Time Series Segmentation and Feature Segment Selection“ genannten Schritt werden die CSI in Segmente aufgeteilt. Wenn τ die gewünschte zeitliche Länge der Segmente ist, *S* die Sampling-Frequenz und *T* die zeitliche Länge der vorliegenden CSI darstellt, ergibt sich die Anzahl der Segmente *N* folgendermaßen:

$$N = \left[\frac{T * S}{\tau * S}\right]$$

Da die Segmente, die während eines Tastendrucks aufgezeichnet wurden, eine wesentlich höhere Varianz als Segmente, auf die das nicht zutrifft, aufweisen (Abbildung 9), werden nur Segmente ausgewählt deren Varianz über einem vorher festgelegten Schwellenwert liegt. Diese ausgewählten Segmente werden basierend auf ihrem zeitlichen Abstand zueinander gruppiert und stellen als Gruppe die CSI-Zeitreihe eines einzelnen Tastendrucks dar. Die Mittelpunkte dieser Gruppen dienen als Feature Segment des Tastendrucks, den sie repräsentieren.

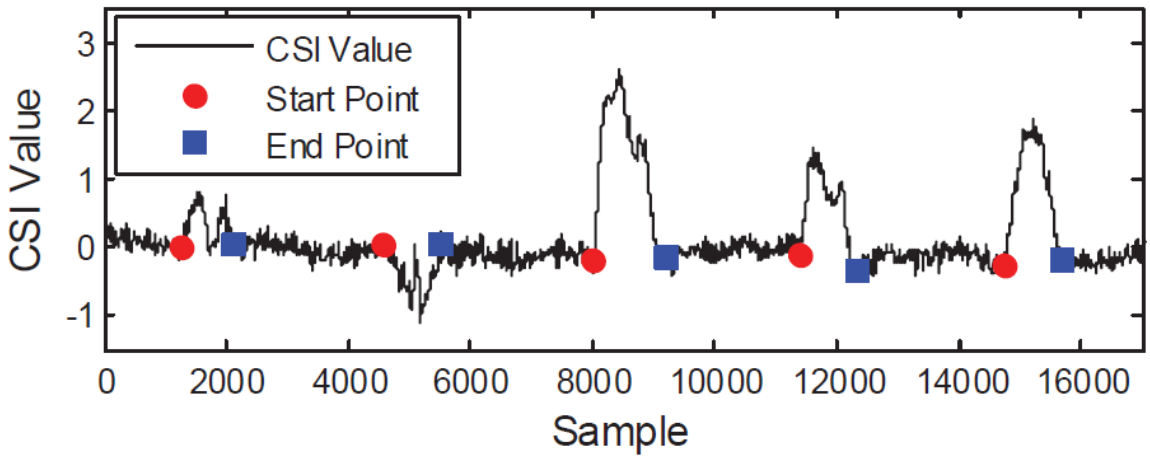

Abbildung 10: Identifikation der Start- und Endpunkte aus [LML16]

Im dritten und letzten Schritt, der „Keystroke Waveforms Extraction“ genannt wird, werden in den einzelnen Gruppen die Start- und Endpunkte des tatsächlichen Tastendrucks bestimmt. Diese Punkte sollten so gewählt sein, dass der durch sie beschränkte Bereich einen möglichst großen Teil des Kurvenverlaufs des einzelnen Tastendrucks abdeckt ohne dabei zu viel vom nicht durch den Tastendruck beeinflussten Kurvenverlauf zu beinhalten. Dies wird erreicht indem der Durchschnittswert der Samples *J* in der betreffenden Gruppe gebildet wird und die Punkte in denen sich die CSI-Zeitreihe mit diesem Wert überschneidet als Ankerpunkte festgehalten werden. Von diesen Ankerpunkten aus werden die nächstgelegenen lokalen Extrema gesucht deren Wert unter *J* liegt und als Start- bzw. Endpunkt des Tastendrucks bestimmt (Abbildung 10). Der Bereich zwischen Start- und Endpunkt wird extrahiert und weiterverarbeitet.

Die für die einzelnen Tastendrücke extrahierten Kurvenverläufe weisen aufgrund der hohen Sampling-Rate beim Sammeln der CSI eine hohe Dichte an Datenpunkten auf, die für den Klassifikator beim Bestimmen des Tastendrucks einen hohen Rechenaufwand bedeutet.

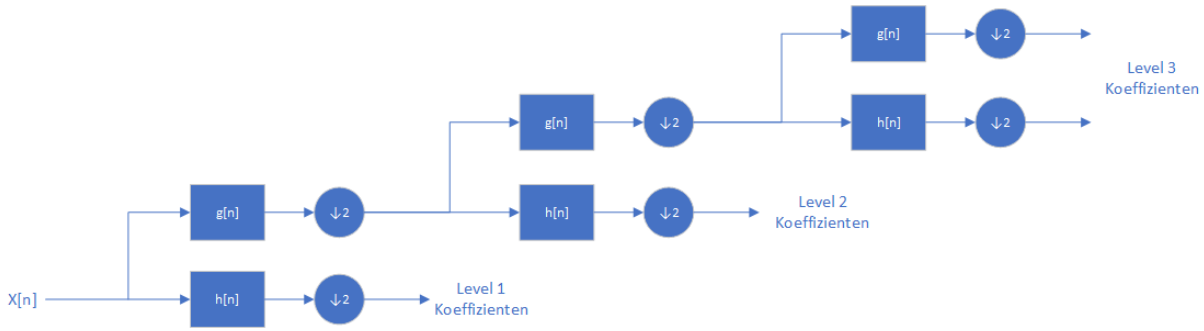

Abbildung 11: Dreifache DWT-Kompression

Aus diesem Grund wird die CSI-Zeitreihe per „Discrete Wavelet Transform“ (DWT) komprimiert [ASS10]. Diese Kompression wird erreicht indem das Eingangssignal, welches in diesem Fall die CSI-Zeitreihe eines Tastendrucks ist, sowohl durch einen Tiefpassfilter *g* als auch einen Bandpassfilter *h* auf Basis eines Wavelets gefiltert wird. Die Ergebnisse dieses Filterns sind die Approximationskoeffizienten und Detailkoeffizienten. Da durch die Filter die Anzahl der Frequenzen in den Koeffizienten halbiert wurde, kann nach dem Nyquist-Shannon-Abtasttheorem [Nyq28] die Anzahl der Samples ebenfalls halbiert werden.

Als geeignete Kompression hat sich eine dreifache DWT Kompression (Abbildung 11) mit dem Daubechies D4 Wavelet als Basis erwiesen. Hierbei werden die sich ergebenden Level-3- Approximationskoeffizienten als Basis zur Klassifikation verwendet.

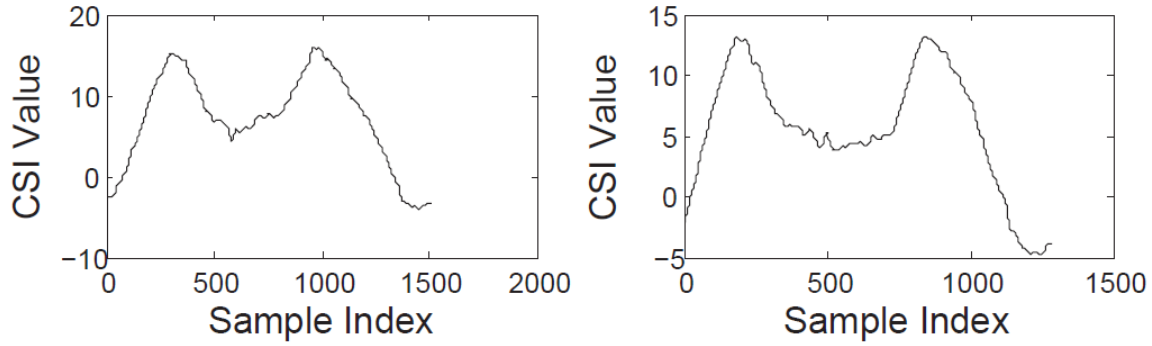

Abbildung 12: Zwei CSI-Zeitreihen bei Eingabe der Zahl 2 aus [LML16]

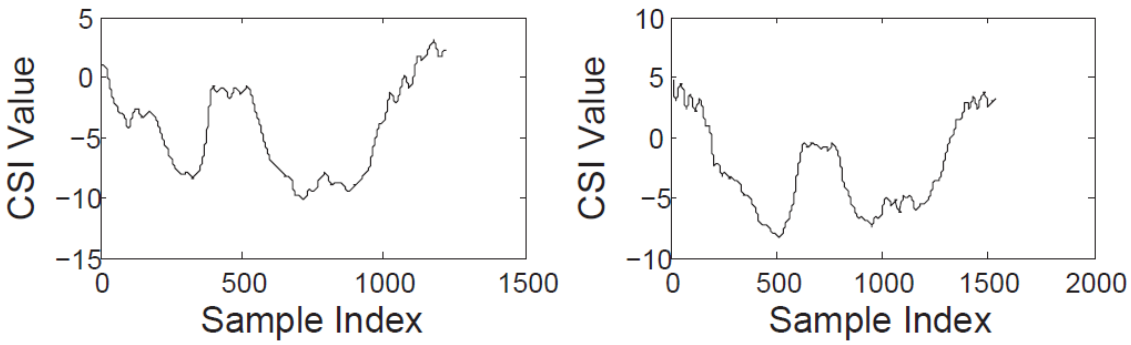

Abbildung 13: Zwei CSI-Zeitreihen bei der Eingabe der Zahl 4 aus [LML16]

Der Klassifikator vergleicht die zu untersuchende CSI-Zeitreihe mittels „Dynamic Time Warping“ mit den Trainingsdaten. „Dynamic Time Warping“ stellt ein Verfahren dar, das zwei Zeitreihen nichtlinear in der Zeit verformt um den Abstand zwischen diesen festzustellen [Cul99]. Für alle Zahlen werden alle pro Zahl gesammelten Trainingsdaten per „Dynamic Time Warping“ mit den zu untersuchenden CSI-Zeitreihen verglichen und die jeweilige ermittelte Distanz diesem Trainingsdatensatz als Punktzahl zugeordnet. Pro Zahl werden aus den gewonnenen Punktzahlen die Mittelwerte gebildet, die als Punktzahl für die entsprechende Zahl dienen. Da die Zahl mit der niedrigsten Punktzahl somit die Zahl mit der höchsten Wahrscheinlichkeit der tatsächlich eingegebenen Zahl zu entsprechen ist, wird diese vom Klassifikator ausgewählt. Wie sich in den Abbildungen 12 und 13 erkennen lässt, weisen die Eingaben bestimmter Zahlen klar voneinander unterscheidbare charakteristische Kurvenverläufe auf.

Auch nach Auswahl der wahrscheinlichsten Zahl werden die Punktzahlen der einzelnen Zahlen gespeichert, um jeweils den nächstwahrscheinlicheren Kandidaten angeben zu können. Die Möglichkeit nächstwahrscheinlichere Kandidaten zu bestimmen kann die Wahrscheinlichkeit die korrekte Zahl anzugeben in Abhängigkeit von der Anzahl der Kandidaten stark steigern.

WINDTALKER IN DER PRAXIS

Kontrollierte Umgebung

Um die Leistungsfähigkeit und Anwendbarkeit von WindTalker zu testen, wurde eine Reihe kontrollierter Versuche mit Freiwilligen durchgeführt und die Ergebnisse ausgewertet.

Als Access Point diente in diesen Versuchen ein herkömmlicher nicht spezifizierter Laptop, der mit einem Intel 5300 NIC mit zwei Rundstrahlantennen und einer Richtantenne ausgestattet war. Auf dem Laptop lief Ubuntu 14.04 LTS mit einem modifizierten Intel-Treiber, der das Auslesen der CSI ermöglichte. Die Sampling-Rate lag bei den bereits erwähnten 800 Samples pro Sekunde und der Access Point wurde an der linken Seite des Zielgeräts in 75cm Abstand platziert. Bei den Zielgeräten, die für diesen Versuch verwendet werden, handelte es sich um ein Samsung Note 5, ein Xiaomi Redmi Note 3 und ein Nexus 5, die auf den Android Versionen 6.0.1, 5.0.2 und 6.0.1 liefen.

An dem Versuch nahmen 10 Freiwillige teil, die sich aus 7 Männern und 3 Frauen zusammensetzten, alle Rechtshänder waren und in der von ihnen gewohnten Weise tippten. Während des Versuchs nahmen die Freiwilligen an einer Trainingsphase teil in der Sie Zahlen in einer vom System angegebenen Weise eingeben sollten, um Trainingsdaten für den Klassifikator zu erzeugen. An diese Trainingsphase schloss sich die Testphase an in der die Freiwilligen ebenfalls Zahlen in einer vom System angegebenen Weise eingeben sollten. Anhand der in dieser Phase gesammelten Daten sollte WindTalker ermitteln welche Eingaben von den Freiwilligen getätigt wurden. Dieser Ablauf durfte nicht länger als 30 Minuten dauern, da sich die CSI mit Veränderungen in der Umgebung ebenfalls stark verändern können.

Im ersten Teil des Versuchs haben die Freiwilligen 10 Reihen von Trainingsdaten eingegeben, die jeweils aus einer Folge der Zahlen von 0 bis 9 bestanden. Eine dieser Zahlenreihen wurde als Testdatensatz ausgewählt, während die verbleidenden 9 Reihen als Trainingsdatensatz für den Klassifikator dienten.

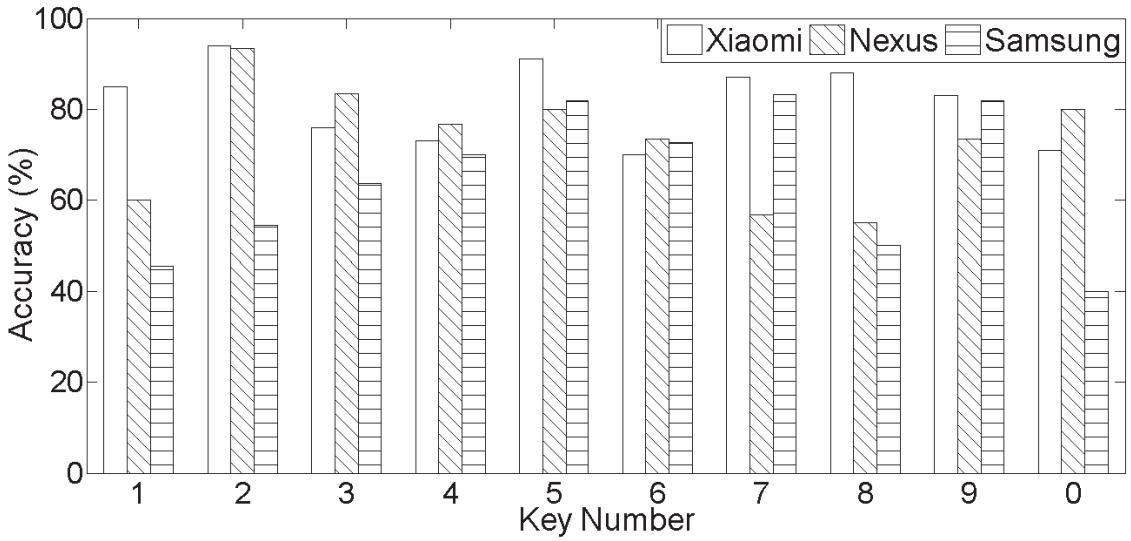

Abbildung 14: Klassifikationsgenauigkeit im ersten Teil des Versuchs aus [LML16]

Im Durchschnitt erreichte WindTalker in diesem Versuch eine Klassifikationsgenauigkeit von 81,8% mit dem Xiaomi-Gerät, 73,2% mit dem Nexus-Gerät und 64% mit dem Samsung-Gerät bei der Bestimmung einer einzelnen Zahl. Wie anhand dieser Daten und Abbildung 14 zu sehen ist, schwankt die Klassifikationsgenauigkeit je nach Zielgerät sehr stark.

Da es in der Praxis unwahrscheinlich ist 10 Reihen von Trainingsdaten von einer Zielperson zu sammeln, wurden im zweiten Teil des Versuchs nur noch 3 dieser Reihen als Trainingsdaten für den Klassifikator verwendet. Statt einer der von den Freiwilligen eingegebenen Reihen als Testdatensatz zu verwenden, wurden in dieser Phase des Versuchs 10 zufällig generierte 6-stellige Passwörter, die von den Freiwilligen eingegeben wurden, als Testdatensatz verwendet.

Tabelle 1: Genauigkeiten unter Berücksichtigung verschiedener Kandidaten nach [LML16]

Mobiltelefon	1 Kandidat	2 Kandidaten	3 Kandidaten
Samsung	0,63	0,83	0,89
Xiaomi	0,79	0,88	0,95

Wie in Tabelle 1 zu sehen ist, ist die durchschnittliche Erkennungsrate pro Zahl mit 79% mit dem Xiaomi-Gerät und 63% mit dem Samsung-Gerät kaum geringer als im ersten Teil des Versuchs. Da die meisten Dienste, die Passwörter verwenden, mehrmalige Falscheingaben von Passwörtern erlauben, kann die Passworteingabe mehrmals mit den vom Klassifikator bestimmten nächstwahrscheinlichen Kandidaten wiederholt werden. Wie sich in Tabelle X zeigt, kann die Erkennungsrate schon durch Wiederholung mit dem zweit- oder drittwahrscheinlichsten Kandidaten merklich gesteigert werden.

Dieser Effekt lässt sich auch beobachten, wenn die Erkennungsrate 6-stelliger Passwörter untersucht wird. Die Wahrscheinlichkeit für ein 6-stelliges vom Klassifikator ermitteltes Passwort das korrekte Passwort zu sein ergibt sich aus dem Produkt der Wahrscheinlichkeiten der einzelnen Zahlen des ermittelten Passworts die korrekte Zahl an dieser Position im Passwort zu sein. Für ein 6-stelliges Passwort gibt es 10^6 mögliche Kombinationen, die nach absteigender Wahrscheinlichkeit geordnet werden.

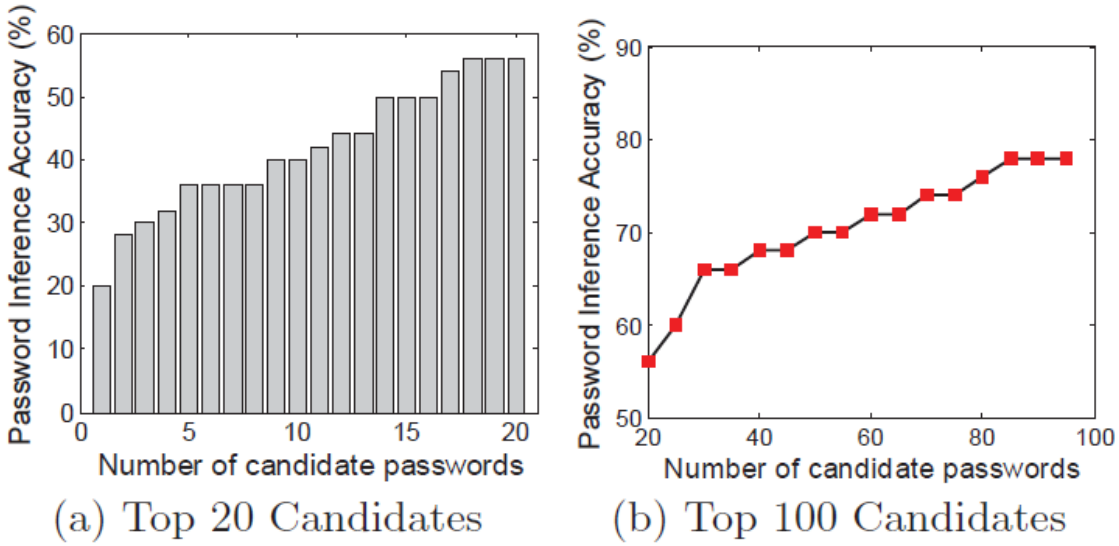

Abbildung 15: Erkennungsrate nach berücksichtigten Kandidaten aus [LML16]

Wie sich in Abbildung 15(a) zeigt, liegt die Erkennungsrate für ein 6-stelliges Passwort, bei ausschließlicher Berücksichtigung des wahrscheinlichsten Passworts, bei nur 20%. Mit den fünf oder zehn wahrscheinlichsten Kandidaten lässt sich die Erkennungsrate schon auf 38% bzw. 42% steigern. In Abbildung 15(b) ist zu sehen, dass die Erkennungsrate bei annähernd 100 berücksichtigten Kandidaten bei knapp unter 80% liegt.

Realitätsnahe Umgebung

Um neben der Leistungsfähigkeit auch die Praxistauglichkeit von WindTalker zu testen, wurde ein Versuch in realitätsnaher Umgebung durchgeführt.

Bei diesem Versuch wurde der Access Point in einer Cafeteria-ähnlichen Umgebung in 1m Abstand zum Zielgerät hinter einem Tresen versteckt. Ziel dieses Versuchs war es ein auf dem Zielgerät eingegebenes 6-stelliges Passwort für den Online-Bezahldienst AliPay zu ermitteln.

Die Freiwilligen durchliefen in diesem Versuch drei verschiedene Phasen. Die erste Phase war, wie schon im Versuch zuvor, eine Trainingsphase bei der die Freiwilligen vorgegebene Zahlen auf dem Zielgerät eingeben sollten. Die Abfrage dieser Zahlen erfolgte jedoch, im Gegensatz zum ersten Versuch, mit zufallsgenerierten Zahlen, die in einer ähnlichen Weise wie Text-Captchas abgefragt wurden. In der zweiten Phase sollten die Freiwilligen ihren Gewohnheiten gemäß im Internet surfen. Die letzte Phase verlangte von den Freiwilligen bei einer Online-Shopping-Plattform den Bezahlvorgang mit AliPay abzuschließen und somit auch ihr AliPay Passwort einzugeben.

Wie im vorherigen Versuch wurden auch hier beständig CSI mit 800 ICMP Echo Replies pro Sekunde gesammelt. Sobald Packets an den AliPay zugeordneten IP-Adressraum 110.75.xx.xx versendet werden, erkennt WindTalker dass das sensible Zeitfenster begonnen hat. Der Zeitpunkt des Versands des letzten an diesen Adressraum versandten Packets gibt Aufschluss über den Endzeitpunkt des sensiblen Zeitfensters. In diesem Versuch hat sich gezeigt, dass der Bezahlprozess von AliPay wesentlich mehr Eingaben als das die Eingabe des Passworts selbst erfordert und es somit notwendig ist das Passwort von den anderen Eingaben unterscheiden zu können. Aus diesem Grund wurden nur durchgängige 6-stellige Eingaben berücksichtigt.

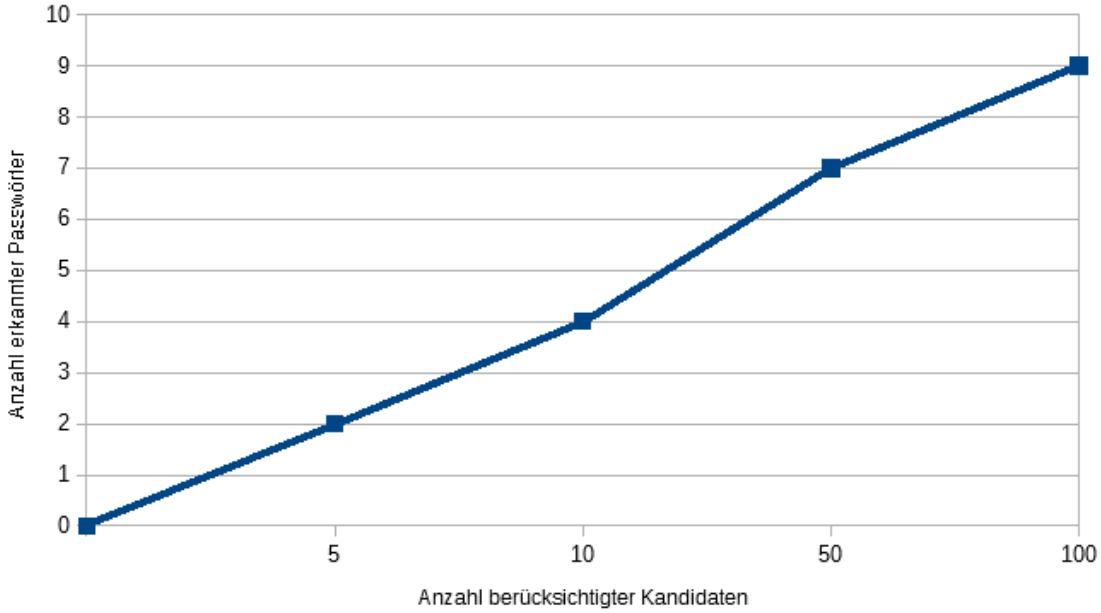

Abbildung 16: Ergebnis des zweiten Versuchs nach [LML16]

Der Versuch wurde mit 10 verschiedenen Passwörtern durchgeführt und hatte das in Abbildung 16 zu sehende Ergebnis. Wie im vorherigen Versuch, zeigt sich auch hier, dass der Anteil der erkannten Passwörter mit Anzahl der berücksichtigten Kandidaten steigt. Die hieraus errechnete Erkennungsrate ist allerdings unter diesen realitätsnahen Bedingungen geringer als im vorherigen Versuch. Es ist nicht auszuschließen, dass es sich hierbei um eine Anomalie handelt, da die Anzahl der getesteten Passwörter gering ist.

Einschränkungen

Trotz der guten Ergebnisse in den Versuchen unterliegt WindTalker gewissen Einschränkungen, die einen negativen Einfluss auf die Praxistauglichkeit haben.

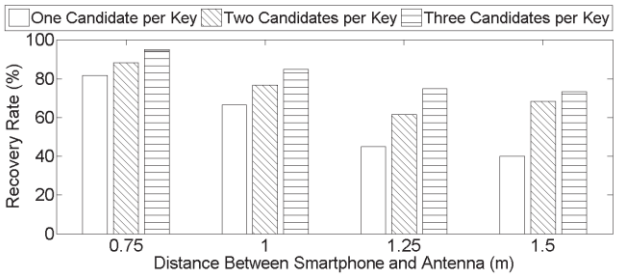

Abbildung 17: Einfluss der Distanz auf die Erkennungsrate aus [LML16]

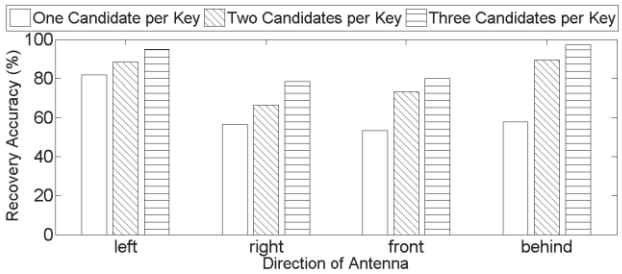

Abbildung 18: Einfluss der relativen Position auf die Erkennungsrate aus [LML16]

Sowohl eine erhöhte Distanz zum Zielgerät als auch eine andere Position als links vom Zielgerät haben, wie in den Abbildungen X und Y zu sehen ist, einen negativen Einfluss auf die Erkennungsrate. Verschlechtert wird diese Situation durch den Umstand, dass sich je nach Abstand und Richtung zum Zielgerät die CSI und der Einfluss, den die Fingerbewegung bei der Eingabe sensibler Daten auf die CSI haben, stark verändern. Hierdurch ist es notwendig den Bewegungsspielraum der Zielperson stark einzuschränken, da ansonsten die an einer Position erlangten Trainingsdaten für die Ermittlung des an einer anderen Position eingegebenen Passworts untauglich sind.

Weiterhin gibt es gegen diese Art der Ermittlung sensibler Daten diverse effektive Gegenmaßnahmen. So können die Zielpersonen es vermeiden sich mit öffentlichen kostenlosen WiFi-Netzwerken zu verbinden, um ein sammeln der CSI gänzlich zu verhindern, oder den CSI über Software absichtlich starkes Rauschen hinzufügen, um die Ermittlung der sensiblen Daten unmöglich zu machen. Weiterhin können auch randomisierte Keypad-Layouts für die Passworteingabe verhindern, dass WindTalker die korrekten eingegeben Zahlen ermitteln kann. Die Hersteller der Zielgeräte können ihre Geräte außerdem so konfigurieren, dass hochfrequente ICMP Echo Requests nicht beantwortet werden und ein Sammeln der CSI verhindert wird. Sollte sich die Zielperson doch mit dem öffentlichen kostenlosen WiFi-Netzwerk verbinden auf dem WindTalker läuft und keine der anderen Gegenmaßnahmen verwenden, reicht es, wenn sie sich während der Eingaben viel bewegt oder absichtlich die eigene Tippweise variiert, um einer Passwortermittlung zu entgehen.

Eine weitere Hürde stellt die Notwendigkeit dar von der Zielperson möglichst viele Trainingsdaten zu gewinnen ohne dass diese den Verdacht hat Ziel eines Angriffs zu sein. Hinzu kommen die technischen Probleme der Software, die zum Auslesen der CSI verwendet wird. Bei dieser Software kommt es beim Sammeln der CSI von gewissen NICs, wie dem des iPhones, zu regelmäßigen Abstürzen.

ZUSAMMENFASSUNG

WindTalker ist, wie die Versuche zeigen, in der Lage hohe Erkennungsraten zu erzielen, wenn mehrere nächstwahrscheinliche Passwortkandidaten mitberücksichtigt werden und die Umgebung gewisse Anforderungen erfüllt. Weiterhin kann es durch die Verwendung eines einzelnen gewöhnlichen Laptops als Access Point und CSI-Aufzeichnungsgerät sehr flexibel platziert werden und erfordert keinerlei Kompromittierung des Zielgeräts. Auch die Möglichkeit das sensible Zeitfenster per Packet-Sniffing zu bestimmen, steigert die Praxistauglichkeit WindTalkers im Vergleich zu ähnlichen Verfahren enorm.

Probleme ergeben sich allerdings, wie bei vielen ähnlichen Verfahren, aus der Notwendigkeit sehr bestimmte Bedingungen herstellen und diese auch während des Angriffs konstant halten zu müssen, um WindTalker erfolgreich einsetzen zu können. Auch die technische Limitation, dass WindTalker bei bestimmten Zielgeräten aufgrund der verwendeten Software nicht eingesetzt werden kann, schränkt die Praxistauglichkeit merklich ein. Da die beteiligten Forscher die Elimination dieser Limitation und eine Steigerung der Erkennungsrate unter anderen Bedingungen zum Ziel zukünftiger Arbeiten erklärt haben, bleibt abzuwarten, ob diese Einschränkungen in der nächsten Version von WindTalker noch vorhanden sind.

LITERATURVERZEICHNIS

[ASS10] A.N. Akansu, W.A. Serdijn, und I.W. Selesnick: Wavelet Transforms in Signal Processing: A Review of Emerging Applications, Physical Communication, Elsevier, vol. 3, issue 1, März 2010, S. 1–18

[ALW15] Ali, K., Liu, A. X., Wang, W., und Shahzad, M.: Keystroke recognition using wifi signals. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (2015), ACM, S. 90–102.

[But30] Stephen Butterworth: On the Theory of Filter Amplifiers In: Wireless Engineer, vol. 7, 1930, S. 536–541

[Bra89] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, Oktober 1989.

[Cul99] Damir Culjat: DTW oder dynamic time warping (1999). http://www.inf.fu-berlin.de/lehre/WS98/SprachSem/culjat/node4.html (abgerufen am 30. April 2018)

[GSS03] D. Gesbert, M. Shafi, D. Shiu, P. Smith und A. Naguib: From Theory to Practice: An Overview of MIMO Space-Time Coded Wireless Systems. In: IEEE Journal on Selected Areas in Communications. Vol. 21, No. 3, 2003, S.281–302

[IEEE802] IEEE Std. 802.11n-2009: Enhancements for higher throughput. http://www.ieee802.org, 2009.

[Koc96] Paul C. Kocher: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proc Int Cryptol Conf, Volume 1109 of Lecture Notes in Computer Science, Springer 1996, S. 104–113

[LAB95] B. LeFloch, M. Alard, C. Berrou: "Coded Orthogonal Frequency Division Multiplex", Proc. IEEE, vol. 83, Juni 1995, S. 982-996

[LWK15] Liu, J., Wang, Y., Kar, G., Chen, Y., Yang, J., und Gruteser, M.: Snooping keystrokes with mm-level audio ranging on a single phone. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (2015), ACM, S. 142–154.

[Liz11] Fourier transform. P.I. Lizorkin (originator), Encyclopedia of Mathematics (2011). URL: http://www.encyclopediaofmath.org/index.php?title=Fourier_transform&oldid=12659 (abgerufen am 30. April 2018)

[LML16] Mengyuan Li, Yan Meng , Junyi Liu , Haojin Zhu , Xiaohui Liang , Yao Liu , Na Ruan: When CSI Meets Public WiFi: Inferring Your Mobile Phone Password via WiFi Signals, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 24. –28. Oktober, 2016, ACM, S. 1068–1079

[Nyq28] Harry Nyquist: Certain Topics in Telegraph Transmission Theory. In: Transactions of the American Institute of Electrical Engineers. Vol. 47, 1928, S. 617–644

[OHW16] Nicole Opiela, Petra Hoepner, Mike Weber: DAS ÖFIT-TRENDSONAR DER IT-SICHERHEIT, Kompetenzzentrum Öffentliche IT Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Mai 2016, S.31

[OHD12] Owusu, E., Han, J., Das, S., Perrig, A., and Zhang, J.: Accessory: password inference using accelerometers on smartphones. In Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (2012), S. 1–6

[Smi02] Lindsay I Smith: A tutorial on Principal Components Analysis (2002) http://www.cs.otago.ac.nz/cosc453/student_tutorials/principal_components.pdf (abgerufen am 4. Mai 2018)

[YLF14] Yue, Q., Ling, Z., Fu, X., Liu, B., Ren, K., und Zhao, W.: Blind recognition of touched keys on mobile devices. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (2014), ACM, S. 1403–1414.

[ZZT16] Zhang, J., Zheng, X., Tang, Z., Xing, T., Chen, X., Fang, D., Li, R., Gong, X., und Chen, F.: Privacy leakage in mobile sensing: your unlock passwords can be leaked through wireless hotspot functionality (2016) https://www.hindawi.com/journals/misy/2016/8793025/ (abgerufen am 14. Mai 2018)