Richtlinie zum „Software-Sprint“ StalkerBuster - Identifizierung von Stalking-Software

Schlussbericht

Zuwendungsempfänger:

StalkerBuster - Petra Hagemann und Ulrich Fouquet GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS18S26 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Kurze Darstellung der Aufgabenstellung und Motivation

Digitales Stalking verbreitet sich immer mehr. Dabei werden z.B. Smartphones von Partner.innen oder anderen vertrauten Personen präpariert, ausgelesen oder anderweitig missbraucht, um diese sozial zu kontrollieren. Taucht ein solcher Verdacht auf, ist er technisch meist nur aufwändig zu überprüfen und zu belegen. Dies betrifft nicht nur die Betroffenen selbst, sondern auch Berater.innen in spezialisierten Frauenzentren etc. Der StalkerBuster soll rasche und begründbare Einschätzungen ermöglichen, aufgrund derer Betroffene und Berater.innen besser informierte Entscheidungen in einer sozial heiklen Situation treffen können. So hilft der StalkerBuster dabei, Kontrolle und Vertrauen in die eigenen Kommunikationsgeräte zurückzugewinnen.

Der StalkerBuster ist eine auf einem RaspberryPi laufende Software, mit der sich das auf Stalkingprogramme zu untersuchende Gerät verbinden muss. Anders als viele andere Vorgehensweisen oder Programme, wie z.B. Virenscanner, untersucht der StalkerBuster nicht das Gerät selbst auf Stalkingsoftware, sondern protokolliert den ein- und ausgehenden Internetverkehr. Auf diese Weise können nicht nur spezielle Stalkingapps, sondern auch das Verhalten anderer Programme auf dem Gerät sichtbar gemacht werden.

Das Protokoll des Netzverkehrs wird auf eine Weise aufbereitet, die eine rasche Einordnung der Situation erlaubt und Material für tiefergehende Untersuchungen sichert. Filterung und Analyse des Netzwerktraffics geht dabei auf öffentlich einsehbare Regeln zurück. Auch wird das Verhalten bekannter und verbreiteter Stalkingapps und -technologien analysiert, so dass diese mit großer Wahrscheinlichkeit erkannt werden können. Liegen Hinweise auf Stalking vor, kann gezielt auf dem Gerät nach der entsprechenden Stalking-Technologie gesucht werden.

Als Meilensteine für die Entwicklung des StalkerBusters wurden festgelgt:

- Festlegung Anfangs-Requirement und zu verwendende Libraries

- Einrichtung der Filter- und Alarm-Datenbank - read-only

- Lauffähigkeit Basis-Software

- (optional) Erstellung Reproduzierbarer Build für RaspberryPi3-Image

- Feedback aus konsolidierter Testaktion der Testgruppe einarbeiten

- Webinterface

Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

Die Zielgruppe des StalkerBusters sind Berater.innen in Frauenzentren etc., die bei Verdacht von Cyberstalking entweder nicht das technische Know-How oder die Zeit haben, die Geräte ihrer Klient.innen eingehend zu untersuchen. Der StalkerBuster unterstützt sie hierbei und gibt schnelle Hinweise, ob tatsächlich Geräte ausspioniert werden. Falls dies der Fall ist können die vom StalkerBuster gesicherten Informationen weitergehend untersucht werden. Gleichzeitig können die Berater.innen den Betroffenen gezielte psychologische Unterstützung anbieten.

Der StalkerBuster kann ganz im Sinne des Themas der 4. Runde des Softwaresprints ¨Power to the User¨ mit Hilfe der Berater.innen den Klient.innen der Beratungszentren die Kontrolle über ihre Kommunikationsgeräte zurückgeben. Die Klient.innen können nach der Analyse ihres Netzwerkverkehrs nicht nur ungewollte Stalkerware entfernen, sondern auch selbstbestimmt bei anderen Apps entscheiden, ob eine festgestellte Kommunikation nach Außen gewünscht ist und diese bei Bedarf unterbinden. So kann Vertrauen in die eigenen Kommunikationsgeräte zurückgewonnen werden.

Ausführliche Darstellung der Ergebnisse

Da der StalkerBuster leider nicht auf einem bereits vorhandenen Tool aufsetzen konnte, sondern komplett neu konzipiert und erstellt werden musste, hat die Entwicklung einzelner Module mehr Zeit als erwartet in Anspruch genommen. Obwohl Prototypen der einzelnen Module und entsprechende Tests zu diesen fertig gestellt sind, konnten sie noch nicht zusammengeführt werden. Somit konnte noch keine lauffähige Version des StalkerBusters mit Berater.innen getestet werden. Ein einsatzfähiger Prototyp soll jedoch bis zum Sommer 2019 fertiggestellt und im Anschluss in Frauenberatungszentren getestet werden.

Da während der Förderphase das Thema Cyberstalking auf verschiedenen Veranstaltungen diskutiert und der StalkerBuster vorgestellt wurde, konnte eine Online-Gruppe von Interessierten gegründet werden, die sich zum Thema aus-

tauscht und mit der gemeinsam Lösungen gegen Cyberstalking gefunden werden sollen. Auch haben verschiedene Softwareentwickler Interesse angekündigt, an einer möglichen Weiterentwicklung mitzuarbeiten.

Die von der Open Knowledge Foundation unterstützte Vernetzung und wöchentlichen Onlinetreffen waren sehr hilfreich zur Selbstmotivation, aber auch, um bestimmte Probleme mit den anderen Geförderten zu besprechen und gemeinsam Lösungen zu finden. Insbesondere bei der Erstellung des Webinterfaces des StalkerBusters konnte das UI/UX-Mentoring gezielte Hilfestellungen bei der Verbesserung des Layouts geben.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Für die Zielgruppe des StalkerBusters, den Betreuer.innen von Frauenzentren etc., wird ein leicht bedienbares Gerät bereitgestellt, das sie bei ihrer Arbeit unterstützt. Da meist nicht die Zeit oder Expertise vorhanden ist, um eingehende Geräte-Analysen bei Cyberstalkingverdacht vorzunehmen, kann der StalkerBuster eine erste Übersicht hierzu geben. Die Ergebnisse können mit den Klient.innen besprochen werden und bei Stalkingverdacht genauer untersucht werden.

Da der StalkerBuster als Open Source Software entwickelt wurde, können der komplette Code oder einzelne Teile heruntergeladen, genutzt oder auch weiterentwickelt werden. Insbesondere der Netzwerkscanner hat Interesse bei verschiedenen anderen Open-Source-Projekten geweckt und es wird geprüft, ob dieser so oder in angepasster Form eingesetzt werden kann. Weiterhin ist geplant, die Software auch für breitere Einsatzmöglichkeiten zu erweitern, um Netzwerkverkehr von Mobil- oder IoT-Geräten für die Nutzer.in sichtbar zu machen. Ziel ist es, der Nutzer.in die Möglichkeit zu geben, einen Überblick über die Netzwerkkommunikation ihrer Geräte zu geben und nicht erwünschte Kommunikation zu unterbinden. So kann die Nutzer.in Kontrolle über ihre Geräte zurückgewinnen.

Durch das Projekt konnte das Team sich fachlich im Bereich der Netzwerkanalyse spezialisieren. Die dafür notwendigen Erfahrungen, das teils unvermeidliche Trial-and-Error, wäre ohne die Unterstützung des Software-Sprints schlicht nicht möglich gewesen.
Für Petra Hagemann konnte das Projekt darüber hinaus einen wesentlichen Beitrag zum Schritt in die Selbständigkeit leisten.
Das Team konnte im fachlichen Bereich des Cyberstalkings Gleichgesinnte und Interessierte kennenlernen, die das Projekt auch mit ihrer teils erheblichen Expertise in Zukunft begleiten und helfen werden, die Weiterentwicklung zu verstetigen.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Einen wichtigen Punkt, den wir vorläufig zurückgestellt haben, ist das Mitschneiden und Aufbrechen verschlüsselter Kommunikation. Dies hat sich als technisch immer schwieriger umsetzbar erwiesen, da neuere Versionen von Android (ab Version 7) genauere Prüfungen von Zertifikaten verlangen, respektive die Installation eigener Zertifikate erheblich erschweren. Durch die Einführung von TLS 1.3 wird unser Ansatz noch einmal deutlich erschwert.

Unter dem Gesichtspunkt der Datensicherheit haben wir uns daher entschlossen, bei verschlüsselten Verbindungen auf ein Aufbrechen der Kommunikation zu verzichten. Wir möchten kein Gerät anbieten, das Laien das einfache Aufbrechen verschlüsselter Kommunikation ermöglicht. TLS 1.3 und andere Techniken zum Schutz vertraulicher Kommunikation sollten aus unserer Sicht unterstützt und nicht umgangen werden.

Im Ergebnis bedeutet dies, dass wir uns bei der Analyse der Datenströme mit Metadaten und unverschlüsselten Daten begnügen.

Für ältere Geräte (Android Version < 7) werden wir ggf. noch eine Möglichkeit zum Mitschneiden verschlüsselter Kommunikation anbieten, das wird aber nicht mehr Teil unseres grundsätzlichen Lösungsansatzes sein.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Eine Webseite zum Thema Stalking ist unter https://stalkerbuster.de verfügbar. Hier sind umfangreiche Literaturhinweise zum Thema Stalkerware, Tipps zum Absichern der eigenen Kommunikationsgeräte sowie Links zu Beratungs- und Betreuungsstellen zu finden, die Betroffene unterstützen können.

Der komplette Open Source Code ist unter https://github.com/stalkerbuster veröffentlicht.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Aufgrund des Mehraufwands für einzelne Komponenten konnte im Förderungszeitraum noch keine integrierte Vollversion mit allen geplanten Komponenten erstellt werden. Die Fertigstellung soll bis Sommer 2019 erfolgen.

Eine Änderung der Planung erfolgte vor allem hinsichtlich zweier Umstände: Erstens erwies sich das Aufbrechen der Verschlüsselung als technisch und sozial schwieriger/fragwürdiger, als wir uns das im Vorfeld vorgestellt hatten.

Zweitens machte die Erstellung eines einfachen Interfaces für den Stalkerbuster mehr Arbeit als geplant, da sich die basalen Netzwerktools (vor allem für WLAN-Management) auf verschiedenen Betriebssystemen viel grundsätzlicher unterscheiden, als wir das vorhergesehen hatten. Selbst im eingeschränkten Kreis der Debian-basierten Systeme (auf den wir uns anfänglich einschränkend kapriziert hatten) gibt es mindestens drei weit verbreitete und gleichzeitig sehr unterschiedliche Toolsets für das Management kabelloser Netzwerk-Verbindungen.

Da unser Projekt aber wesentlich davon lebt, auch für unbedarfte Anwender.innen handhabbar zu sein, war die Unterstützung wenigstens dieser wenigen Toolsets unabdingbar - bedeutete aber gleichzeitig auch dreifache Arbeit. Diese Ausweitung der Arbeit war womöglich ein Produkt schlechter Planung: Wir hatten mit solch einer Komplikation an so einer basalen Stelle nicht gerechnet.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Das Thema Cyberstalking findet erfreulicherweise mehr Beachtung in den Medien. So berichtet das Online-Magazine *Motherboard* von *Vice* in seiner thematischen Serie *When Spies Come Home* regelmäßig über Stalking und Spysoftware.

Konkrete Hilfestellungen zum Auffinden von Spyapps wurden im Computermagazin c‘t, von der vom BMJV geförderten Informationsseite mobilsicher.de oder auch vom Bundesverband der Frauenberatungsstellen und Frauennotrufe in Deutschland veröffentlicht. Seit Kurzem hat auch das auf Sicherheitssoftware spezialisierte russische Unternehmen Kaspersky Lab eine deutliche Kennzeichnung von Stalkerware in seine Antivirenprogramme aufgenommen.

Anders als der StalkerBuster untersuchen all diese Ansätze das Mobilgerät selbst. Dies bedeutet, dass nur bereits bekannte und genauer untersuchte Stalkerware gefunden wird, dies allerdings zuverlässiger als der StalkerBuster dies kann. Der breitere Ansatz des StalkerBusters, in dem sämtlicher Netzwerkverkehr mitgesnifft wird, verspricht ein umfassenderes Bild darüber, welche Programme welche Daten wohin senden. So können auch weniger bekannte Stalkingsapps aufgespürt werden und darüberhinaus eine Übersicht des Internetverkehr sämtlicher auf dem untersuchten Gerät installierten Programme gegeben werden.