Tobias Höller (JKU Linz)
Verknüpfung von physischen Aktivitäten mit einer privaten dezentralen digitalen Identität durch die Digidow Architektur
01.10.19 13:40

Das Digidow Projekt möchte die physischen Aktionen einer Person anhand deren biometrischer Daten durch ein dezentrales Netzwerk mit einer digitalen Identität verknüpfen. Eine wesentliche Komponente einer Digidow Transaktion ist die initiale Suche nach den relevanten Kommunikationspartnern innerhalb der verteilten Infrastruktur.

Dieser Vortrag betrachtet die Anforderungen an diese initiale Phase und analysiert die Vorteile und Nachteile der verschiedenen möglichen Ausgangspunkte, von denen die Suche gestartet werden kann.

Sabrina Buchegger (FH Campus Wien)
Benutzerfreundliche Authentifizierung - Eine prototypische Implementierung und Evaluierung eines neuartigen Authentifizierungsmechanismus für mobile Geräte
01.10.19 15:25

Übliche Methoden zum Schutz mobiler Geräte sind PIN, Muster und Fingerabdrücke. Obwohl solche Methoden weitgehend verwendet werden, gibt es bereits eine Anzahl an erfolgreichen Angriffen, um sie zu brechen. Deswegen wurden in der Vergangenheit bereits mehrere Authentifizierungsmethoden entwickelt, die bestimmten Angriffen standhalten können. Im Besonderen wurden bildbasierte Authentifizierungsmethoden vorgestellt, die der Verwendung schwacher Passwörter gegenwirken sollen und einen Fokus auf Benutzerfreundlichkeit legen.

In dieser Arbeit wird eine weitere bildbasierte Authentifizierungsmethode vorgestellt, die Schutz gegen typische Angriffe auf mobile Geräte bieten und eine besonders leichte Bedienung für den Benutzer ermöglichen soll. Es wird dabei angenommen, dass nur der Besitzer eines Gerätes alle Bilder, die sich auf diesem Gerät befinden, erkennen kann. Dabei werden bei der Authentifizierung teilweise Bilder aus dem Internet und Bilder aus dem Gerät selbst angezeigt, die der Benutzer als solche erkennen muss. Für diese Anwendung muss der Benutzer keine neuen Informationen lernen, wie es bei üblichen Authentifizierungsmethoden wie Passwörtern, oder bei anderen bildbasierten Methoden der Fall ist. Die Methode wurde prototypisch implementiert und wird verwendet, um eine Umfrage zur Benutzerfreundlichkeit und Sicherheit, besonders gegenüber nahestehender Personen des Benutzers, durchzuführen.

Die Arbeit zeigt, dass es möglich ist, eine Authentifizierungsmethode zu implementieren, die zufällige Bilder aus dem Internet und dem mobilen Gerät anzeigt. Die meisten Testsubjekte zeigten Interesse an der Anwendung mit der Voraussetzung einer schnelleren Bedienung. Die Analyse der Anwendung und der Vergleich mit anderen Authentifizierungsmethoden zeigt, dass die Sicherheit der Methode stark von der Konfiguration der Anwendung und von dem Inhalt der Bilder, die sich auf dem Gerät befinden, abhängt.

Florian Nuding (TU Wien)
Angriffe auf maschinelles Lernen - Eine Untersuchung auf Risiken und Gegenmaßnahmen
01.10.19 17:00

Die auf der Welt produzierte Menge an Daten hat sich über die letzten Jahre hinweg drastisch erhöht und wird sich Prognosen zufolge innerhalb der nächsten drei Jahre verdoppeln. Maschinelles Lernen versucht daraus einen Nutzen zu ziehen, indem große Datenmengen automatisiert verarbeitet und Modelle darauf trainiert werden, um beispielsweise so Prognosen über die Zukunft zu ermöglichen. Die Daten müssen dafür, bei konventionellem maschinellem Lernen, an einem Ort zusammengeführt

und dort verarbeitet werden. Dies kann aber hinsichtlich datenschutzrechtlicher Aspekte Probleme bereiten, vor allem wenn es sich um persönliche oder vertrauliche Daten aus sensiblen Quellen handelt.

Abhilfe könnte hier verteiltes maschinelles Lernen schaffen. Dabei werden Modelle einzeln und lokal trainiert und erst im Anschluss gesichert in ein großes, globales Modell zusammengeführt. Auch existieren zahlreiche Angriffe, um maschinelles Lernen zu unterwandern und dessen Resultate zu beeinflussen. In der Vergangenheit wurden im Speziellen "Adversarial Machine Learning" sowie "Backdoor Attacken" als besonders vielversprechend eingestuft.

Ein Bedrohungsszenario zeigt sich beispielsweise in Gebäuden mit Gesichtserkennung als Zutrittsbeschränkung. Sollte es einem Angreifer gelingen, in den Trainingsprozess des Erkennungsmodells einzugreifen, so könnte dieser eine "Backdoor" einpflanzen, beispielsweise das Tragen einer bestimmten Brille. Jeder, der diese Brille trägt, unabhängig von dessen eigentlicher Berechtigung, könnte im Anschluss die Gesichtserkennung bestehen, da durch eine erfolgreiche "Backdoor Attacke" das Tragen der Brille ausreicht, um Zutritt zu erhalten.

Im Zuge meiner Diplomarbeit führe ich eine Evaluierung der Machbarkeit dieser Angriffe durch. Auch erarbeite ich die Unterschiede der Effektivität dieser Attacken bei konventionellem und verteiltem maschinellem Lernen und analysiere etwaige Möglichkeiten diesen entgegenzusteuern.

Tobias Dam (FH St. Pölten)
Web-Security-Scanner: Fortlaufende Analysen von Bedrohungsentwicklungen
02.10.19 13:40

Bedrohungen im Internet verändern und entwickeln sich ständig weiter, einmalige Analysen der angewandten Techniken verlieren sehr schnell ihre praktische Relevanz.

Der Web-Security-Scanner des Instituts für IT Sicherheitsforschung scannt automatisiert regelmäßig 1 Million der meistbesuchten Webseiten und analysiert die gesammelten Daten, um Veränderungen und Trends im Internet zu erkennen. Der Web-Security-Scanner wurde als Docker Swarm konzipiert und instrumentalisiert Headless Chrome-Browser, welche mithilfe des Chrome Developer Tools (DevTools) Protocol gesteuert werden. Diese einzelnen Scanner übermitteln die Daten anschließend an den zentralen Server, welcher die Daten zur weiteren Analyse in einer NoSQL Datenbank persistiert. Aufgrund des modularen Designs kann das Framework laufend um weitere Analysen erweitert werden.

Mithilfe des Web-Security-Scanners konnten wir die Funktionsweisen von Cryptomining auf Webseiten analysieren und nutzen die regelmäßigen Resultate um Blocklisten für unsere Browser-Erweiterung CoinEater (https://coineater.io) zu erstellen. Weiters haben wir die aktuellen Anwendungen von Popups auf typosquatting Domains anhand der Scanergebnisse untersucht.

Katharina Pfeffer (SBA Research)
Usable Security
02.10.2019 15:25

Menschliche Aspekte werden im Design von IT-Systemen oft nicht bedacht, wodurch es in der Praxis zu Sicherheits- und Privatsphärenverletzungen kommen kann, obwohl die darunterliegenden Systeme in der Theorie sicher sind. Diese Diskrepanz betrifft EndnutzerInnen und EntwicklerInnnen, die diese Systeme bedienen und entwickeln, und schafft außerdem Spielraum für potenzielle AngreiferInnen. In diesem Kontext kommt das Forschungsgebiet „Usable Security“ zum Einsatz. Dieses setzt sich mit der Gestaltung von IT Systemen auseinander, um die Anwendbarkeit dieser für EndnutzerInnen und EntwicklerInnen zu erhöhen und gleichzeitig die Angriffsfläche für potenzielle Attacken zu minimieren.

Matthias Wenzl (FH Technikum Wien)
Implantierung von Sicherheitsfeatures in ressourcenbeschränkte eingebettete Systeme
02.10.19 17:00

Innerhalb der letzten zehn Jahre wurden Computersysteme durch neu entstandene Anwendungsfälle wie ''Ambient Assistive Technologies'', ''Car2X'' Kommunikation, ''Smart Homes'', ''Smart Cities'' und Industrie 4.0 zu allgegenwärtigen Begleitern in unserem täglichen Leben. Die unausweichliche Vernetzung dieser Geräte wird heute auch häufig als das Internet der Dinge (Internet of Things, IoT) bezeichnet. Dieses besteht zu einem überragenden Teil aus speziell für Ihren Anwendungsfall optimierten vernetzten Computern, sogenannten eingebetteten Geräten (Embedded Systems). Aufgrund ihrer Spezialisierung und den damit verbundenen Randbedingungen wie zum Beispiel Energieverbrauch, sowie der deterministischen Einhaltung zeitlicher Vorgaben (Echtzeitbedingungen), ist es in vielen Embedded Systems nicht möglich ein Standardbetriebssystem für eingebettete Systeme wie zum Beispiel Windows IoT Core, oder Linux zu verwenden. Daraus resultierend verfügen eine Vielzahl der Computer im Internet der Dinge nicht über ausreichend Sicherheitsfeatures, welche in Standardbetriebssystemen bereits flächendeckend integriert sind. Die quelltextseitige Nachrüstung sämtlicher Software für eingebettete Systeme ist jedoch unter anderem Aufgrund des hohen Grades an Software- (Systeme mit speziellen Betriebssystemen, komplett ohne Betriebssystem) und Hardwarediversität (unterschiedlichen Prozessorarchitekturen, Speichergrößen und Zusatzhardware) illusorisch.

Innerhalb dieses Vortrages wird ein neuer Ansatz vorgestellt, welcher es erlaubt, Sicherheitsfeatures in vernetzte eingebettete Systeme, unter Berücksichtigung ihrer Randbedingungen, zu implantieren, um neue und bestehende Systeme im IoT immuner gegen Angriffe Unbefugter zu machen.