KIRAS Erfolgsgeschichten

Projekt : Smartphone Security

Neue Verfahren zur Benutzer- und Datenauthentifizierung und zum Zugriffs- und Malwareschutz für Smartphones, Tablets und BYOD

Fact-Box:

Unternehmen:	**Fachhochschule St. Pölten, Institut für IT Sicherheitsforschung, Matthias Corvinus Strasse 15, 3100 St. Pölten**
Produkt:	**Im Rahmen des Projektes entstanden vier Hauptergebnisse:** **a) BenutzerInnen-Authentifizierung mit Hilfe des Reisepasses** **b) Kontinuierliche biometrische BenutzerInnen-Authentifizierung durch Überprüfung des personenspezifischen Bewegungsmusters bei der Gerätebedienung** **c) Datenverschlüsselung für Cloud-Speicher** **d) Verhaltensbasierte Malwareerkennung**
Impact:	**Zu a.) Im Projekt entstanden eine App für Smartphones und eine Software für eine Zentrale, die eine hochsichere Benutzer-Authentifizierung über das Internet mit Hilfe des Reisepasses auf einfache Weise ermöglicht. Dabei muss die BenutzerIn nach dem Start der App nur den Reisepass zum Smartphone halten und die Zentrale kann eine sichere BenutzerInnen-Authentifizierung durchführen.** **Zu b.) Es konnte im Projekt gezeigt werden, dass es möglich ist Smartphone BenutzerInnen durch Überprüfung des personenspezifischen Bewegungsmusters (Touchbewegungen, Geräteführung, Tippverhalten) bei der Gerätebedienung zu erkennen. Das Verfahren wurde mit einer selbst entwickelten Banking-App (angelehnt an George der ERSTE Bank) getestet. Die Forschungsergebnisse können direkt in eine Lösung (z.B. Telebanking) integriert werden – mehrere Unternehmen evaluieren derzeit einen Einsatz.** **Zu c.) Im Projekt entstand ein neues Verschlüsselungssystem für Daten in Cloud Speichern, das speziell die Anforderungen und Leistungsfähigkeit von Smartphones berücksichtigt. Dabei liegt die Hoheit der in der Cloud gespeicherten Daten ausschließlich bei den BesitzerInnen. Das System wurde für die Android Plattform in Form einer App entwickelt. Sie wird nach Verbesserungen in der Benutzerführung als Open Source Lösung veröffentlicht.** **Zu d.) Im Projekt konnte an Hand einer Proof-of-Concept Implementierung gezeigt werden, dass der Einbau verhaltensbasierter Verfahren zur Erkennung von Schadsoftware in die Sandboxing-Techniken von Smartphones und Tablets möglich ist und funktioniert. Die Firma IKARUS hat die Forschungsergebnisse übernommen, um sie in ein konkretes Produkt des Marktes zu integrieren.**

Beschreibung:

Ziele des Projektes sind die Erforschung und Entwicklung einer:

a) weltweiten BenutzerInnen-Authentifizierung mit Hilfe des Reisepasses

b) kontinuierlichen biometrischen BenutzerInnen-Authentifizierung durch Überprüfung des personenspezifischen Bewegungsmusters bei der Gerätebedienung

c) Datenverschlüsselung für Cloud-Speicher

d) verhaltensbasierten Malwareerkennung

Technologische Auswirkungen

Die steigende Verfügbarkeit von Smartphones und Tablet-PCs (über 3 Milliarden im Jahr 2016) stellt die Cyber Security vor weitreichende große Herausforderungen. Da einige wichtige Sicherheitsprobleme von Smartphones und Tablet-PCs noch kaum oder unzureichend gelöst sind, beschäftigte sich das Projekt Smartphone Security genau mit einigen derartigen, bislang weitgehend vernachlässigten Bereichen.

Zu a.) BenutzerInnen-Authentifizierung mit Hilfe des Reisepasses: Es konnte gezeigt werden, dass der Reisepass für eine hochsichere weltweite BenutzerInnen-Authentifizierung über das Internet geeignet ist und in Verbindung mit Smartphones verwendet werden kann.

Zu b.) Kontinuierliche biometrische BenutzerInnen-Authentifizierung durch Überprüfung des personenspezifischen Bewegungsmusters bei der Gerätebedienung: Es konnte im Projekt gezeigt werden, dass es möglich ist Smartphone BenutzerInnen anhand unterschiedlicher verhaltensbasierter Charakteristika zu erkennen. Diese Charakteristika wurden im Projekt herangezogen, um ein eindeutiges Nutzerprofil zu erstellen und dieses am mobilen Endgerät zu hinterlegen. Moderne mobile Geräte liefern dafür das notwendige Werkzeug. Sie besitzen neben einem Touchscreen unter anderem einen digitalen Kompass, Beschleunigungssensor, Näherungssensor, Umgebungslichtsensor, Gyroskop, Barometer, GPS oder Magnetometer. Das Hauptergebnis ist ein kontinuierliches Authentifizierungsverfahren, das auf Fuzzy Set Theorie und einem Scoring Modell basiert und Touchbewegungen, Geräteführung und das Tippverhalten der Smartphone Benutzung heranzieht, um zu entscheiden, ob es sich um die legitime BenutzerIn handelt oder nicht.

Zu c.) Datenverschlüsselung für Cloud-Speicher: Im Projekt entstand ein neues Verschlüsselungssystem für Daten in Cloud Speichern, das speziell die Anforderungen und Leistungsfähigkeit von Smartphones berücksichtigt und auch eine sichere externe Schlüsselsicherung enthält. Dabei liegt die Hoheit der in der Cloud gespeicherten Daten ausschließlich bei den BesitzerInnen. Damit kann die Datensicherheit von extern gespeicherten Daten wesentlich verbessert werden. Die externe Speicherung von Daten hat einen sehr hohen Stellenwert im Bereich der mobilen Geräte, insbesondere im Online-/Cloud-Kontext, da diese Geräte zumeist nur über begrenzte Möglichkeiten zur Speicherung verfügen. Des Weiteren ist die Synchronisation von Anwender-/Nutzdaten über mehrere Geräte durch die Cloud Services sicherheitstechnisch problematisch. In üblichen heutigen Lösungen müssen dabei die BenutzerInnen die Kontrolle über ihre Daten auch dem Anbieter direkt oder indirekt gewähren, eine oftmals inakzeptable Situation.

Zu d.) Verhaltensbasierte Malwareerkennung: Da Malware (Schadsoftware) ein zunehmen-

des Problem bei mobilen Geräten darstellt und klassische Virenscanner zur Lösung in Zukunft relativ ineffizient sind, wurde im Projekt eine für dieses Umfeld optimierte und spezifische verhaltensbasierte Erkennung erforscht und entwickelt. Diese basiert auf den Ergebnissen des KIRAS-Projektes MalwareDef und wurde speziell für die Hardware-anforderungen von Smartphones optimiert. Die Grundidee von MalwareDef ist es, typische Aktionen von Malware auf einem relativ hohen Abstraktionsniveau formal zu definieren und über diese Definitionen Malware dynamisch zu entdecken. Der Einsatz verhaltensbasierter Verfahren eignet sich besonders für mobile Geräte, weil dort die Technik des Sandboxings zunehmend zum Einsatz kommt. Dies ermöglicht die Kontrolle des Verhaltens zur Laufzeit. Außerdem hat sie bei mobilen Geräten zwei Vorteile: Erstens muss keine Signaturdatenbank gespeichert werden, da das Verhalten der Malware in Form generischer Beschreibungen als formale Grammatik vorliegt (was bei der geringeren Speichergröße bei mobilen Geräten von großer Bedeutung ist); und zweitens kann mit verhaltensbasierter Malware-Erkennung auch neuartige Malware erkannt werden, die bislang noch nicht aufgetreten ist.

Des Weiteren wurden die wichtigsten Projektergebnisse sechs Mal international publiziert.

Wirtschaftliche Auswirkungen

Zu a.) Es entstanden während des Forschungsprojektes und danach in Entwicklungs-tätigkeiten (Diplomarbeiten etc.) am Institut eine App und eine Software für eine Zentrale, die eine weltweite hochsichere BenutzerInnen-Authentifizierung mit Hilfe des Reisepasses auf einfache Weise ermöglicht. Dabei muss die BenutzerIn nach dem Start der App nur den Reisepass zum Smartphone halten und die Zentrale kann eine sichere BenutzerInnen-Authentifizierung durchführen. Voraussetzungen dafür sind, dass das Smartphone NFC-fähig ist, auf der Android Plattform basiert und online ist.

Zu b.) Das Verfahren wurde mit einer selbst entwickelten Banking-App (angelehnt an George der ERSTE Bank) getestet, um seine Einsetzbarkeit zu zeigen. Die Forschungsergebnisse können direkt in eine Lösung (z.B. Telebanking) integriert werden – mehrere Unternehmen evaluieren derzeit einen Einsatz.

Zu c.) Das neue Verschlüsselungssystem wurde für die Android Plattform in Form einer App entwickelt und umfangreich getestet. Die App zeigte dabei eine hohe Effizienz in Bezug auf Verarbeitungsgeschwindigkeit und Speicherbedarf. Sie wird nach Verbesserungen in der Benutzerführung als Open Source Lösung veröffentlicht. Für Unternehmen, die für den Markt eine noch professionellere Lösung entwickeln möchten, steht das Institut zur Verfügung.

Zu d.) Im Projekt konnte gezeigt werden, dass der Einbau verhaltensbasierter Verfahren zur Erkennung von Malware in die Sandboxing-Techniken von Smartphones und Tablets möglich ist und funktioniert. Die Firma IKARUS hat die Projektergebnisse übernommen, um sie in ein konkretes Produkt des Marktes zu integrieren.

PartnerInnen im Projekt waren: A1 Telekom Austria AG, Austria Card Plastikkarten und Ausweissysteme GmbH, BeeOne GmbH (Tochterunternehmen der ERSTE Group), Bundesministerium für Inneres (BM.I), Bundesministerium für Landesverteidigung und Sport (BMLVS) und Cryptas IT-Security GmbH.