Fremde Hand am Handy erkennen

27.11.2015 | 19:05 | Von Veronika Schmidt (Die Presse)

Sicherheit.Niederösterreichische Forscher entwickeln Diebstahlsicherungen für Smartphones: Am Verhalten des Nutzers wird erkannt, ob man der Besitzer ist oder nicht. Auch Viren können über ihr Verhalten ausfindig gemacht werden.

Damenabend bei einer Freundin. Ihr Smartphone läutet im Wohnzimmer, während sie in der Küche ist. Man geht ans Handy, weil man sieht, dass die dritte Freundin anruft, die sich verspätet. Doch kurz nachdem man abgehoben hat, ertönt ein Alarm, und das Gerät schaltet sich ab. So könnte eine Diebstahlsicherung der Zukunft funktionieren. In diesem Fall wäre es eine unerwünschte Nebenwirkung, da die fremde Benutzerin nichts Böses wollte. Doch meist hat, wer ein fremdes Handy in die Hand nimmt, nichts Gutes im Sinn. IT-Forscher nennen dies „Authentifizierung anhand verhaltensbasierter Charakteristika". Anders gesagt: Kann ein Handy erkennen, wer es in die Hand nimmt? Ist die Art des Wischens, Abhebens, Tippens bei jedem Nutzer unterschiedlich?

An der FH St. Pölten wurde soeben ein großes Projekt über Smartphone Security – u. a. finanziert vom Technologieministerium – abgeschlossen, das sich dem Thema widmete. „Da Smartphones noch nicht so lang auf dem Markt sind, war die Zahl an Publikationen anderer Forscher zu verhaltensbasierter Authentifizierung überschaubar", sagt Ernst Piller, Leiter des Instituts für IT-Sicherheitsforschung. Für Computertastaturen gibt es einige Forschungsergebnisse, wie man anhand der Tastaturbenutzung erkennt, wer sie betätigt. Das individuelle Tippverhalten unterscheidet sich nicht nur bei so groben Dingen wie Zweifinger-Suchmodus im Vergleich zum Zehnfingersystem. Auch erfahrene Sekretäre unterscheiden sich im Verhalten an den Tasten.

Welche Sensoren liefern Info?

Pillers Team wollte nun wissen: Welche Daten können auf dem Smartphone belegen, dass der Benutzer der Besitzer ist? „Solche Geräte besitzen neben dem Touchscreen so viele Sensoren: Kompass, Beschleunigungssensor, Näherungssensor, Umgebungslichtsensor, Barometer, GPS und Magnetometer", sagt Piller. „Wir untersuchten, welche Sensoren viel relevante Information hergeben und welche wenig." Noch wichtiger war: Auf welche Daten kann man für eine ständige Kontrolle leicht zugreifen?

„An viele Daten kommt man nicht heran, indem man einfach eine Software oder App installiert. Man müsste dazu die Geräte rooten, das bedeutet, dass man die komplette Kontrolle über das Gerät erhält", sagt Piller. Da aber eine Anwendung für die breite Masse entwickelt werden sollte, hat man sich nur auf Sensoren und Daten konzentriert, die ohne Eingriff in das Betriebssystem zugänglich sind.

Das sind erstens die Touchbewegungen, also das Berühren des Bildschirms: Wo drückt man hin, wie wischt man über den Screen? Zweitens unterscheidet sich bei jedem Nutzer das Tippen in die virtuelle Tastatur.

„Bei der Smartphone-Tastatur, die man meist mit nur ein oder zwei Fingern bedient, sind andere Dinge ausschlaggebend als bei herkömmlichen, die mit der ganzen rechten und linken Hand bedient werden", so Piller. Am signifikantesten war jedem Nutzer zuordenbar, wie stark er beim Tippen aufdrückte.

Drittens kann ein Smartphone anhand der Geräteführung erkennen, wer es in die Hand nimmt. Bewegungs- und Beschleunigungssensoren messen, wie schnell das Handy vom Tisch gehoben wird, ob mit der linken oder rechten Hand, wie man es an das Ohr führt und vieles mehr.

„Diese Art der Authentifizierung hat den Vorteil, dass die Kontrolle den ganzen Tag laufen kann: Bei anderen biometrischen Sicherungen gibt man nur zum Start des Geräts oder beim Start einer App seinen Fingerabdruck ab oder macht einen Gesichtsscan", sagt Piller. Doch verhaltensbasierte Kontrolle greift auch dann, wenn der Besitzer kurz aus dem Raum geht. Beim Zurückkommen sieht er, ob jemand sein Handy benutzt hat. „Der Nachteil ist, dass die Erkennung nicht sofort in der ersten Sekunde klar ist." Denn das Gerät kann zwar den Besitzer und sein Verhalten gut identifizieren. Aber wenn das Verhalten nicht dem Schema entspricht, muss erst abgeglichen werden: Ist da jemand Fremder dran oder hat der Besitzer nur einen schlechten Tag, ist müde, nimmt er es mit der falschen Hand oder sitzt gerade im Auto? Dieser Abgleich dauert einige Zeit. „Wir wollen zudem alle Daten im Gerät behalten und nicht zentral bearbeiten, damit zukünftige Anbieter den Nutzer nicht überwachen können", betont Piller. Sonst könnte etwa eine Bank, die ihr Telebanking durch verhaltensbasierte Authentifizierung sichert, überprüfen, ob der Kunde das Handy betrunken bedient, ob er krank oder gesund ist etc.

Doch nicht nur Personen können anhand ihres Verhaltens kontrolliert werden: Auch Software hat ein typisches Verhalten, das man nutzen kann, um Handys vor Viren zu schützen. Im Josef-Ressel-Zentrum an der FH St. Pölten wurde gezeigt, dass es möglich ist, auch auf dem Smartphone Schadsoftware durch Verhaltensanalyse zu erkennen. „Ein herkömmlicher Virenscanner vergleicht Millionen von Signaturen von bekannten Viren mit jenen auf Ihrem Smartphone."

Viren einer Familie ähneln sich

Doch täglich gibt es fast 90.000 neue Viren. „Manche Spionagesoftware läuft bereits seit Jahren auf einem Gerät, bevor sie als Schadsoftware erkannt wird", sagt Piller. Die verhaltensbasierte Erkennung durchleuchtet jedoch die Prozesse hinter den Anwendungen: Familien von Schadsoftware verhalten sich ähnlich. Kennt man die Arbeitsweise der Familie, wird man neue, zuvor unerkannte Viren schneller finden, weil sie sich so verhalten wie ihre Vorgänger. Eine clevere Lösung, doch „auch Viren werden immer intelligenter", sagt Piller, dem die Forschungsfragen in diesem Gebiet nicht ausgehen.