idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Ruhr-Universität Bochum
Dr. Julia Weiler

25.02.2019
http://idw-online.de/de/news711063

Forschungsergebnisse
Informationstechnik
überregional

Bochumer Forscher umgehen digitale Signaturen von PDF-Dokumenten

Forschern der Ruhr-Universität Bochum ist es gelungen, die Inhalte von signierten PDF-Dokumenten zu ändern, ohne die Signatur dabei ungültig werden zu lassen. Fast alle getesteten PDF-Anwendungen bemerkten die Manipulation nicht. Signierte PDF-Dateien werden von vielen Firmen für Rechnungen verwendet; manche Staaten wie Österreich oder die USA schützen damit auch Regierungsdokumente. Die Forscher vom Bochumer Horst-Görtz-Institut für IT-Sicherheit veröffentlichten ihre Ergebnisse am 25. Februar 2019 online (https://pdf-insecurity.org).

Da sie fast alle gängigen PDF-Anwendungen und Online-Services betraf, wandten sich die Forscher im Oktober 2018 an das Computer Emergency Response Team des Bundesamtes für Sicherheit in der Informationstechnik, um die Schwachstelle zu melden. Mit dessen Unterstützung halfen die Bochumer Forscher Dr. Vladislav Mladenov, Dr. Christian Mainka, Martin Grothe und Prof. Dr. Jörg Schwenk den Entwicklern der PDF-Anwendungen gemeinsam mit Karsten Meyer zu Selhausen von der Firma Hackmanit, die Sicherheitslücken zu schließen.

PDF-Signaturen weit verbreitet

„Digitale Signaturen in PDF-Dokumenten gewährleisten ähnlich wie das kleine grüne Schloss im Webbrowser, dass das Dokument wirklich von dem angegebenen Absender stammt“, erklärt Jörg Schwenk. „Viele Deutsche bezahlen ihre Rechnungen täglich per Überweisung auf Basis solcher signierten Dokumente.“

Seit in der Europäischen Union 2014 die Regulierung zu „Electronic Identification, Authentication and Trust Services“ (eIDAS) in Kraft getreten ist, sind digitale Signaturen weit verbreitet. Viele große Unternehmen nutzen sie für Rechnungen, alle Verträge bei EU-Projekten werden digital signiert, und in Österreich geschieht das auch bei allen Gesetzen. „Das Unternehmen Adobe bietet einen digitalen Signierdienst an, der nach eigenen Aussagen allein 2017 acht Milliarden Signaturen ausstellte“, veranschaulicht Jörg Schwenk.

Desktop-Anwendungen und Online-Services getestet

Um PDF-Dateien zu öffnen, existieren zahlreiche Tools. Die Forscher überprüften 22 gängige Desktop-Applikationen für Windows, Linux und MacOS sowie weitere sieben Online-Services. Bei Letzteren handelt es sich um Webseiten, deren Aufgabe es ist, die Signatur eines hochgeladenen PDF-Dokuments zu überprüfen. Sie werden zum Beispiel von Behörden und Unternehmen verwendet.

Die Forscher probierten für jede Anwendung und jeden Service drei verschiedene Angriffsklassen aus: Universal Signature Forgery (USF), Incremental Saving Attack (ISA) und Signature Wrapping Attack (SWA). Sie versuchten, den Inhalt eines Dokuments zu ändern, ohne dass die PDF-Tools das merkten.

Eine Billion US-Dollar Rückzahlung

Das Ergebnis: 21 der getesteten Desktop-Anwendungen und fünf Online-Services waren durch mindestens einen der drei Angriffe verwundbar. Die IT-Experten konnten jeden beliebigen Inhalt der PDF-Dokumente verändern. So verwandelten sie beispielsweise einen zu zahlenden Rechnungsbetrag in eine Kostenrückerstattung von einer Billion US-Dollar, ohne die Signatur der PDF-Rechnung zu kompromittieren.

Aktuellste Version installieren

Listen aller analysierten PDF-Anwendungen (https://www.pdf-insecurity.org/signature/viewer.html) und Online-Services (https://www.pdf-insecurity.org/signature/services.html) finden sich auf der Webseite zum Angriff.

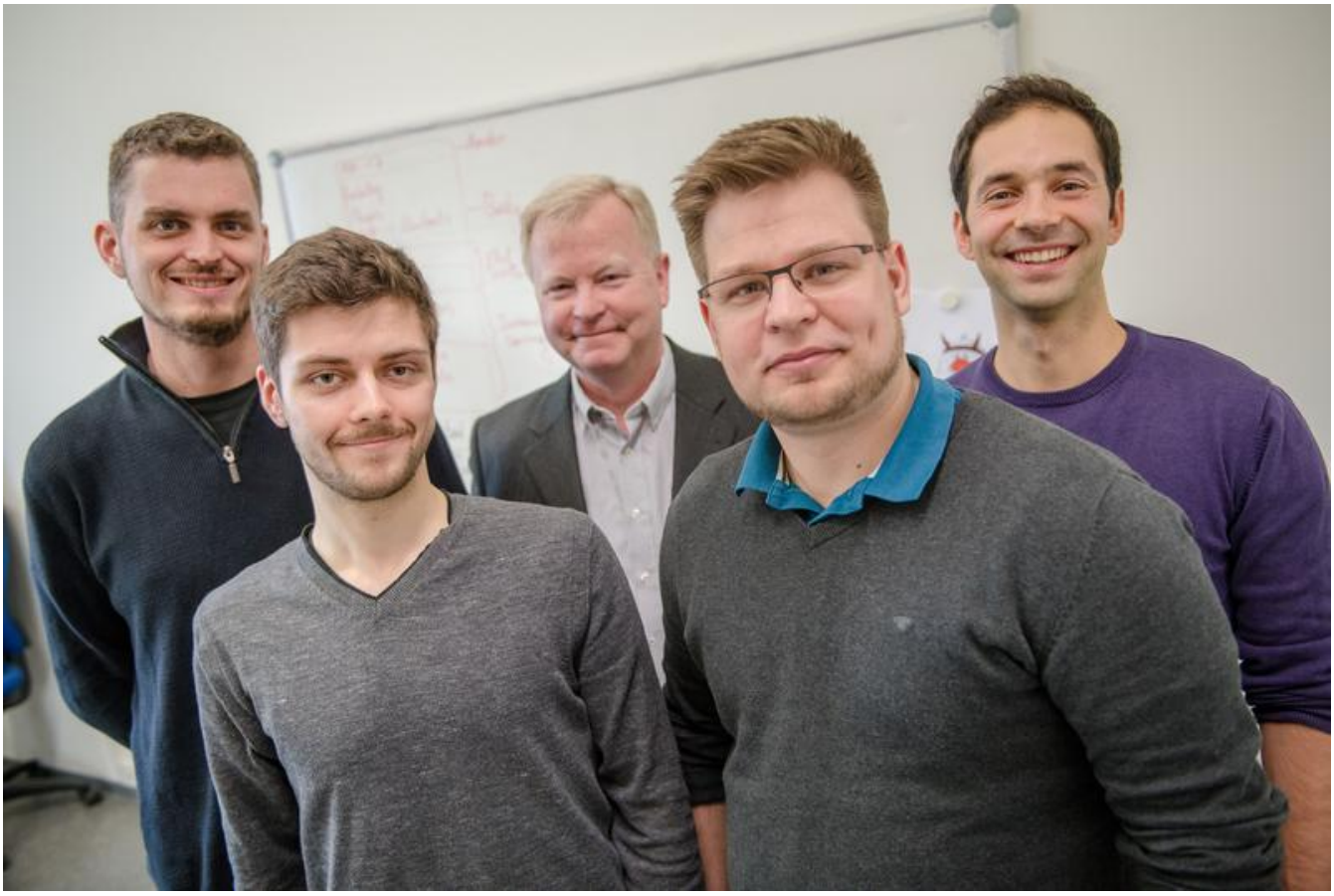
„Nutzerinnen und Nutzer von PDF-Readern können nachschauen, welche Version sie derzeit installiert haben, und diese mit unserer Liste im Internet vergleichen“, sagt Jörg Schwenk. Falls ein Nutzer die von der Sicherheitslücke betroffene Version (oder eine ältere Version) installiert hat, sollte er sich bei dem jeweiligen Software-Hersteller erkundigen, ob ein Update für die Software verfügbar ist, raten die Forscher.

wissenschaftliche Ansprechpartner:

Dr. Vladislav Mladenov
Lehrstuhl für Netz- und Datensicherheit
Horst-Görtz-Institut für IT-Sicherheit
Ruhr-Universität Bochum
Tel.: 0234 32 26742
E-Mail: vladislav.mladenov@rub.de

Dr. Christian Mainka
Lehrstuhl für Netz- und Datensicherheit
Horst-Görtz-Institut für IT-Sicherheit
Ruhr-Universität Bochum
Tel.: 0234 32 26796
E-Mail: christian.mainka@rub.de

Allgemeine Anfragen können auch über die E-Mail-Adresse team@pdf-insecurity.org gestellt werden.



Christian Mainka, Karsten Meyer zu Selhausen, Jörg Schwenk, Martin Grothe und Vladislav Mladenov (von links) deckten die Sicherheitslücke auf.