Manipulierte PDF-Verträge

Wie sich PDF-Zertifikate aushebeln lassen und wie Sie sich schützen können

Mit zertifizierten Signaturen sollen sich PDF-Dokumente manipulationssicher gestalten lassen. Forscher der Ruhr-Universität Bochum (RUB) haben aber Schwachsellen in der Spezifikation sowie den Implementierungen dieser Dokument-Zertifikate entdeckt.

Von Andrea Trinkwalder

Mit dem Portable Document Format (PDF) lassen sich Verträge papierlos abwickeln und sogar rechtssicher unterschreiben, wenn man ein geeignetes Zertifikat für die qualifizierte elektronische Signatur besitzt. Dokumentnormen und Signatur-Verordnungen wie eIDAS sollen Rechtssicherheit bei digital abgewickelten Geschäfte garantieren. Doch die ISO-Spezifikation des standardisierten Dokumentenformats lässt zu viel Spielraum und die meisten gängigen Anzeigeprogramme unterstützen Nutzer nur unzureichend dabei, Manipulationen zu erkennen, bemängeln Forscher der Ruhr-Universität Bochum. Als Hilfe zur Selbsthilfe haben die Sicherheitsexperten um Simon Rohlmann auch einen Online-Service entwickelt, mit dem Nutzerinnen und Nutzer ihre Dokumente und bevorzugte PDF-Software auf die Schwachstellen hin abklopfen können.

Die PDF-Spezifikation bietet umfangreiche Mechanismen, um die etablierten Unterschriften-Workflows aus der analogen in die digitale Welt zu übertragen: Mehrere Vertragspartner können ein PDF nicht nur digital unterschreiben, sondern auch – wie auf Papier – Passagen markieren und Bemerkungen dazu ergänzen. Ob und welche Änderungen erlaubt sind, legt der Urheber fest, indem er als erster ein Dokumentzertifikat anbringt und die entsprechenden Befugnisse für die anderen Beteiligten auswählt. Ab diesem Zeitpunkt soll das Zertifikat den Dokumentinhalt vor Manipulationen schützen: Versucht etwa eine Partei, heimlich den Vertragstext zu ändern, ist das Zertifikat ungültig. Ein verlässlicher PDF-Betrachter muss dies unmissverständlich und deutlich sichtbar anzeigen.

Simon Rohlmann und sein Team haben nun gezielt nach Lücken sowohl in der PDF-Spezifikation als auch in der Implementierung gängiger Betrachter gesucht, um diese Sicherheitsmechanismen auszuhebeln – und sind fündig geworden. Es gelang ihnen, zwei grundlegende Angriffsszenarien zu entwickeln und PDF-Dokumente mithilfe der vom Urheber genehmigten Aktionen so geschickt zu manipulieren, dass die meisten gängigen Betrachter und Editoren das Zertifikat weiterhin als gültig einstuften. Durch Manipulationen am PDF-Code konnten die Forscher die entsprechenden Objekte darüber hinaus so tarnen, dass auch eine manuelle Überprüfung durch misstrauische Zeitgenossen ins Leere läuft.

Betroffen waren 24 PDF-Editoren und -Betrachter, darunter Adobe Acrobat (und Acrobat Reader), Foxit Reader sowie Foxit Phantom, LibreOffice Draw sowie PDF-XChange Editor. Adobe hat bereits alle Versionen gefixt, LibreOffice ist ab Version 7.0.4 abgesichert und Foxit Reader sowie PhantomPDF ab Version 10.1.1 (Windows) beziehungsweise 4.1.1 (macOS).

Camouflage

Der wunde Punkt liegt in zwei der Permission Levels, die der Urheber beim Zertifizieren festlegen kann:

1. Er kann Änderungen komplett verbieten.
2. Er kann das Signieren sowie Ausfüllen von Formularfeldern erlauben.
3. Er kann zusätzlich das Hinzufügen von Anmerkungen gestatten.

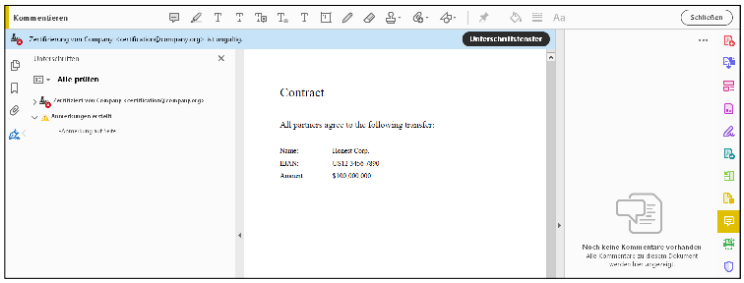
Das Ändern des Inhalts, also etwa von Bildern, Texten und Grafiken, erlaubt keiner dieser Level. Und: Die Forscher haben auch keinen Ansatz gefunden, diesen starken Schutz eingebetteter Inhalte zu umgehen. Die in Stufe 2 und 3 erlaubten Aktionen öffnen aber eine andere Tür für Angreifer, weil sie als inkrementelles Update ans Ende des PDFs angehängt werden – also außerhalb des per Prüfsumme abgesicherten Bereichs. Simon Rohlmann und sein Team schafften es, echt wirkenden Content mittels zweckentfremdeter Unterschriftsfelder (Stufe 2) und Anmerkungen (Stufe 3) zu ergänzen und verräterische Spuren durch direkte Manipulation am PDF-Code so geschickt zu verwischen, dass diese auf den Benutzer wie Originaldokumentinhalt wirken. So ließ sich beispielsweise ein Textannotationsfeld einfach über dem vereinbarten Rechnungsbetrag platzieren – mit einem Betrag von hundert Millionen statt 100 US-Dollar.

Bedingt abwehrbereit

Grundsätzlich gibt es in PDF-Viewern drei Mechanismen, die den Nutzer auf Manipulationen hinweisen sollten: Beim Öffnen erscheint oberhalb des signierten Dokuments normalerweise eine schmale Leiste, die die Signatur als gültig, ungültig oder auch als nicht überprüfbar einstuft. In der Regel enthält die Leiste eine Schaltfläche, über die sich ein Panel mit detaillierten Informationen einblenden lässt. Unter anderem gibt es dort Auskunft über den Permission Level, die Eigenschaften des Zertifikats sowie am Dokument durchgeführte Änderungen. Eine dritte Informationsquelle wäre die Kommentarleiste, die normalerweise sämtliche Anmerkungen übersichtlich auflistet – was Rohlmann und seine Mitstreiter aber durch relativ einfache Änderungen am Code des PDF-Dokuments erfolgreich verhinderten.

Bild: Simon Rohlmann, Ruhr-Universität Bochum

Eine simple Textfeld-Überlagerung (Mitte) enttarnen misstrauische Nutzer, indem sie die Kommentarleiste öffnen. Doch eine Manipulation am /subtype-Objekt im PDF-Code verhindert, dass das Textfeld dort erscheint.



100 Millionen statt 100 US-Dollar: Acrobat und Acrobat Reader stufen das Zertifikat des per Text-Anmerkung manipulierten Vertrags mittlerweile als ungültig ein; die getarnte Anmerkung erscheint aber nach wie vor nicht in der dafür vorgesehenen Leiste.

Die Forscher bemängeln darüber hinaus, dass meist weder die Kommentarleiste noch die detaillierten Signaturinformationen automatisch eingeblendet werden, sondern nur die schmale Infoleiste. Wenn Acrobat (Reader) und Konsorten das Zertifikat aber als gültig einstufen – schließlich handelte es sich um erlaubte Änderungen –, schöpfen technisch weniger versierte Anwender keinen Verdacht und werden von der Software auch nicht zum Nachforschen ermuntert.

Hilfe zur Selbsthilfe

Ob nun ein solches Dokument vor Gericht Bestand hat oder nicht, Manipulationsmöglichkeiten verringern auch das Vertrauen in digitale Workflows. Die Forscher der RUB decken nicht nur Lücken auf, sondern engagieren sich aktiv in der Verbesserung der Dokumentsicherheit. Zum einen haben sie ein Online-Tool entwickelt, mit dem jeder Anwender seine eigenen Untersuchungen durchführen kann: „PDF Detector“ inspiziert Dokumente hinsichtlich der beschriebenen Attacken, siehe ct.de/yugq. Darüber hinaus arbeiten sie mittlerweile aktiv zusammen mit dem ISO-Komitee an einer sicheren PDF-Spezifikation. Last, but not least geht es ihnen auch darum, die noch allzu technischen Signatur-Workflows praxistauglich zu machen, damit Anwender auch ohne Kenntnis der knapp tausendseitigen Spezifikation in der Lage sind, die Vertrauenswürdigkeit eines PDFs einzuschätzen. Die Viewer überfordern ihre Nutzer noch mit teils kryptischen Statusreports oder verbergen manch hilfreiche Prüffunktion hinter unscheinbaren Schaltflächen.

Annotation	Capabilities				Allowed in			Danger Level
	Text		Image		P1	P2	P3	
	Add	Hide	Add	Hide				
FreeText	✓	✓	✗	✓	−	−	+	High
Redact	✓	✓	✗	✗	−	−	+	High
Stamp	✗	✓	✓	✓	−	−	+	High
Caret	✗	✓	✗	✓	−	−	+	Medium
Circle	✗	✓	✗	✓	−	−	+	Medium
Highlight	✗	✓	✗	✓	−	−	+	Medium
Ink	✗	✓	✗	✓	−	−	+	Medium
Line	✗	✓	✗	✓	−	−	+	Medium
Polygon	✗	✓	✗	✓	−	−	+	Medium
PolyLine	✗	✓	✗	✓	−	−	+	Medium
Square	✗	✓	✗	✓	−	−	+	Medium
Squiggly	✗	✓	✗	✓	−	−	+	Medium
StrikeOut	✗	✓	✗	✓	−	−	+	Medium
Underline	✗	✓	✗	✓	−	−	+	Medium
FileAttachment	✗	✓	✗	✓	−	−	+	Low
Sound	✗	✓	✗	✓	−	−	+	Low
Text(Sticky Note)	✗	✓	✗	✓	−	−	+	Low
3D	✗	✓	✗	✓	−	−	−	None
Link	✗	✓	✗	✓	−	−	−	None

Bild: Simon Rohlmann, Ruhr-Universität Bochum

Der Permission Level 3 erlaubt Anmerkungen. Für Manipulationen eignen sich vor allem Freitext-, Redigieren- und Stempelfunktionen, weil man diese Objekte so geschickt gestalten und tarnen kann, dass sie wie Originalinhalte wirken.

Acrobat (Reader) und LibreOffice Draw stufen die manipulierten Dokumente der RUB-Forscher mittlerweile als ungültig ein. Mit PDF-XChange und Foxit Reader lassen sich die Manipulationen immerhin aufspüren, wenn man die entsprechenden Funktionen kennt: Foxit Reader blieb vage, wies in unseren Tests in der detaillierten Signatur-Info aber darauf hin, dass Anmerkungen hinzugefügt wurden. Sogar die getarnten Inhalte, die nicht in der Kommentarleiste auftauchen, kann man darüber anklicken und leicht lokalisieren. In PDF-XChange lässt sich das nicht manipulierte Original über den unscheinbaren Link „Signierte Version: zur Anzeige klicken“ einblenden, was immerhin einen visuellen Vergleich erlaubt, aber bei umfangreichen Verträgen nicht ideal ist. Ob Ihr bevorzugter Betrachter vergleichbare Funktionen bietet und die Änderungen zuverlässig anzeigt, können Sie mit den Exploits der Bochumer Forscher herausfinden. Hilfreich ist auch eine Inhaltsvergleichsfunktion, die Unterschiede in zwei Dokumentversionen aufspürt und farbig markiert. *(atr@ct.de)* c't

***Wissenschaftliche Veröffentlichung, Exploits, Online-Testservice:* ct.de/yugq**