Ruhr-Universität Bochum

Lehrstuhl für Netz- und Datensicherheit

Exposé für die Anmeldung der Masterarbeit

Simon Rohlmann
7. April 2019

Thema der Masterarbeit

Sicherheit von Transformationsmethoden in PDF Signaturen

Motivation

Im Juni 1993 veröffentliche Adobe Systems das Referenzhandbuch zum Portable Document Format (PDF). Das Format baut auf der PostScript-Sprache auf und soll Texte, sowie Grafiken in Form von digitalen Dokumenten plattformunabhängig für Benutzer verfügbar machen [8, S. 5].
Seit dem Jahr 2008 wird das Portable Document Format in der Norm ISO-32000-1 der International Organization for Standardization spezifiziert [3].
Mit der Veröffentlichung des Referenzhandbuchs zu PDF 1.3 werden offiziell Signaturen unterstützt [2, S. 4]. Adobe unterscheidet zwischen digitalen Signaturen auf Basis asymmetrischer Kryptographie, welche zur Berechnung Schlüsselpaare bestehend aus öffentlichen und privaten Teil heranziehen, sowie elektronischen Signaturen, die z.B. mit handschriftlichen Unterschriften gleichzusetzen sind [2, S. 451]. Eine digitale Signatur soll die drei Schutzziele: Integrität, Authentizität und Nichtzurückweisbarkeit erfüllen [7, S. 328]. So kann der Empfänger eines PDF Dokuments mit digitaler Signatur feststellen wer das Dokument digital unterschrieben hat und ob es nachträglich verändert wurde. Der Unterzeichner wiederrum kann wegen der digitalen Signatur, welche unter Verwendung seines privaten Schlüssels erstellt wurde, nicht abstreiten das Dokument unterschrieben zu haben.
Verwendung finden digitale Signaturen unteranderem im E-Government, E-Justice oder im Onlinehandel. So führen beispielsweise die sächsischen Finanzämter PDF Signaturen explizit als zugelassenes Signaturaustauschformat auf [1]. Die gesetzliche Grundlage für rechtsgültige digitale Signaturen bietet in der EU die eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste [6]. Ergänzend dazu findet in Deutschland das Vertrauensdienstegesetz [VDG] Anwendung.
Für digitale Signaturen im Allgemeinen und PDF Signaturen im Speziellen gibt es somit ein weitgefächertes Einsatzgebiet. Da diese digitalen Signaturen rechtsgültigen Charakter besitzen, ist die Sicherheit und Unfälschbarkeit von entscheidender bedeutet. Das Erforschen von Möglichkeiten, um nachträglich den Inhalt eines digital signierten PDF Dokuments zu ändern, ohne dabei die Signatur zu invalidieren, stellt somit eine wichtige Forschungsaufgabe dar.

Problemstellung

In der Masterarbeit “Security of PDF Signatures“ von Karsten Meyer zu Selhausen [10], sowie im Paper “1 Trillion Dollar Refund - How To Spoof PDF Signatures“ von Mladenov et al. [9], wurden verschiedene Techniken vorgestellt die zu einer gültigen Signaturprüfung führen, obwohl der Quelltext eines PDF Dokuments verändert wurde. Auf diesen Forschungsergebnissen aufbauend möchte ich in meiner Masterarbeit weiter die Sicherheit von PDF Signaturen erforschen.
Adobe unterscheidet bei digitalen Signaturen zwischen den zwei Signaturtypen Approval und Certification. Während es vom Typ Approval mehrere Signaturen geben kann, darf eine Certification Signatur nur einmal im Dokument vorkommen und muss gleichzeitig die erste Signatur sein [4, S. 6-7]. Die in den oben genannten Arbeiten ermittelten Angriffe auf PDF Signaturen, Universal Signature Forgery, Incremental Saving Attack und Signature Wrapping Attack, sind auf beide Signaturtypen anwendbar.
Im Verlauf meiner Masterarbeit möchte ich mich detailliert mit den für die Signatur wichtigen Transformationmethoden / -parametern auseinandersetzen und mögliche Schwachstellen im Validierungsprozess aufdecken. Hierzu zählen die Transformationmethoden FieldMDP, DocMDP[1] und UR3 [4, S. 2].
Im Zusammenhang mit Signaturen spielen Formularfelder innerhalb eines PDF Dokuments eine besondere Rolle. So ist es bspw. möglich das Ausfüllen von Formularfelder zu erlauben, ohne dabei die Signatur zu invalidieren. Darüber hinaus kann aber ein Formularfeld durch eine Signatur auch besonders geschützt werden und ein nachträgliches Ändern des Formularinhalts zu einer ungültigen Signatur führen. Um entsprechende Änderungen während des Validierungsprozesses zu erkennen, wird der FieldMDP Parameter verwendet. MDP steht hierbei für Modification Detection and Prevention [4, S. 9].
Über die DocMDP Methode lässt sich steuern, welche Aktionen nach einer Signierung erlaubt bleiben, ohne die Signatur zu invalidieren. Die Festlegung erfolgt über den “P“-Parameter der die Werte 1-3 akzeptiert. Mit 1 wird festgelegt, dass keine Änderungen erlaubt sind. 2 erlaubt das Ausfüllen von Formularen, sowie das Anfügen von Approval Signaturen. Mit 3 besteht zusätzlich zu den Berechtigungen aus 2 die Möglichkeit Kommentare über Annotation-Objekte hinzuzufügen. DocMDP bezieht sich immer auf das gesamte Dokument, daher kann dieser Parameter nur in Verbindung mit einer Certification Signatur verwendet werden [4, S. 9-10].
Der UR3 Parameter, welcher für Usage Rights steht, erlaubt es zusätzliche Rechte zu aktivieren, falls der Validierungsprozess eine gültige Signatur ermitteln konnte. Bei einer ungültigen Signatur werden die vorher definierten

[1] Nur bei Cerification Signaturen verfügbar

Rechte nicht gewährt [4, S. 10].
Modifikationen an diesen Methoden bzw. deren Parametern könnten dazu führen, dass Quelltextveränderungen möglich sind ohne die Signatur zu invalidieren.

Optionalbereich

Optional könnten folgende Themen zusätzlich behandelt werden:

- Filter und Subfilter: Diese regeln die Verwendung von kryptographischen Funktionen für die Erstellung und Validierung einer digitalen Signatur [3, S. 467].
- Content Masking: Das grafische Vortäuschen einer gültigen Signatur gegenüber dem Benutzer.

Vorgehen

Zu Beginn wird der aktuelle Versionstand der Systeme protokolliert und eine Sicherungskopie der Testumgebung angelegt, welche die aktuellste Version der ausgewählten PDF Systeme beinhaltet. Darüber hinaus werden die dazugehörigen Installationsdateien archiviert. Dieses Vorgehen soll verhindern, dass automatische Programmaktualisierungen die Auswertung der Ergebnisse behindern. Im nächsten Schritt wird ein PDF Dokument mit Certification Signatur erstellt, welches als Referenzdokument für weitere Schritte dienen soll. Hierfür wird die in der ISO 32000-1 spezifizierte PDF Version 1.7 verwendet. Die bereits bekannten Angriffe auf PDF Signaturen, Universal Signature Forgery, Incremental Saving Attack und Signature Wrapping Attack werden unter Verwendung des erstellen Dokuments getestet. Diese Tests zeigen auf, ob alle PDF Betrachtungsprogramme den Umgang mit Certification Signaturen beherrschen. Programme, die die zu untersuchenden Transformationen nicht unterstützen, können so zu Beginn ausgemustert werden.
Da der Umgang der einzelnen Programme mit den in der Problemstellung beschriebenen Methoden und Parametern noch nicht absehbar ist, werden die Programme unter Verwendung eines nicht manipulierten Dokuments getestet. So soll festgestellt werden, ob beispielsweise die Parameter 1-3 der DocMDP korrekt vom Betrachtungsprogramm interpretiert wird.
Auf Basis der bisherigen Ergebnisse werde ich verschiedene Manipulationsoptionen entwickeln, die wiederum im nächsten Schritt mit allen Programmen getestet werden. Das jeweilige Verhalten der Programme wird dokumentiert und ein Screenshot des Validerungsfensters gespeichert. Die so gewonnen Kenntnisse können für weitere Manipulationsschritte hilfreich sein.
Am Ende der Masterarbeit sollte sich somit zeigen, ob Manipulationen an

den Transformationsmethoden / -parametern zu validen Signaturen, trotz einer Veränderung am Quelltext des PDF Dokuments, führen können.

Testumgebung

Aktuell[2] liegt der Anteil von Windows Betriebssystemen im Desktop-Bereich bei 74,4 % [5]. Aus diesem Grund soll vorrangig Windows 10 als Basisbetriebssystem für die Testumgebung verwendet werden. Um bei Bedarf die gesamte Testumgebung den Betreuern verfügbar zu machen, wird diese in einer virtuellen Maschine installiert. Auf dem Markt sind verschiedene Programme zum Betrachten von PDF Dokumenten verfügbar. Im bereits erwähnten Paper "1 Trillion Dollar Refund - How To Spoof PDF Signatures" werden einige dieser Programme betrachtet [9, S. 8]. Diese Auswahl soll ebenfalls als Basis für diese Masterarbeit genutzt werden und kann bei Bedarf um weitere PDF Betrachtungsprogramme erweitern werden.

Zeitplanung

Zunächst sollen die offiziellen Referenzhandbücher zu PDFs und die Dokumente zu digitalen Signaturen von Adobe studiert werden. Ziel hierbei ist es den genauen Validierungsprozess zu verstehen. Dabei steht vor allem das Mitwirken der Transformationsmethoden und deren Parameter im Vordergrund. Während dieser Sichtung der zur Verfügung stehenden Dokumente werden bereits die dazu passenden Grundlagenabschnitte der Masterarbeit entstehen. Hierfür sind vier bis fünf Wochen einzuplanen, wobei der vorzeitige Übergang in die nächste Phase möglich wäre.
Im nächsten Schritt beginnt der Aufbau der Testumgebung. Nach der Installation des Betriebssystems, der Betrachtungsprogramme und dem Anlegen eines Sicherungspunktes, soll mit der Evaluation der bekannten Angriffe auf PDF Signaturen unter Verwendung von Certification Signaturen begonnen werden. Parallel dazu sollen ebenfalls im Grundlagenkapitel die Methodik der Angriffe beschrieben werden. Hierfür sind vier bis fünf Wochen einzuplanen. Der Abschluss der Arbeitspakete "Sichtung der Unterlagen", "Aufbau der Testumgebung" und "Evaluation bekannter Angriffe" bildet den ersten Meilenstein.
Darauffolgend soll mit der Entwicklung geeigneter Manipulationen der Transformationsmethoden / -parameter begonnen werden. Diese Manipulationsvarianten werden anschließend mit allen PDF Betrachtungsprogrammen getestet. Die Ergebnisse der Tests werden anschließend auf mögliche Hinweise analysiert, die zu weiteren Manipulationsmöglichkeiten führen könnten. Parallel dazu werden die Ergebnisse analysiert und dienen als Basis für den

[2] Stand: Februar 2019

schriftlichen Durchführungsteil der Arbeit. Hierfür sind sechs bis acht Wochen einzuplanen. Dieser Teilschritt bildet den zweiten Meilenstein.
Im letzten Schritt werden die Ergebnisse der Arbeiten zusammengefasst, ein Résumé verfasst und ein Ausblick auf mögliche Folgethemen gegeben. Hierfür sind vier bis sechs Wochen einzuplanen.

Meilenstein	**Arbeitspaket**	**Zeitraum**
1	Sichtung der Unterlagen Aufbau der Testumgebung Evaluation bekannter Angriffe	8 - 10 Wochen
2	Entwicklung der Manipulationsvarianten Anwenden der Manipulationsvarianten	6 - 8 Wochen
	Abschlussarbeiten	4 - 6 Wochen

Tabelle 1: Übersicht der Zeitplanung

Literaturverzeichnis

[1] Freistaat Sachsen: Landesamt für Steuern und Finanzen. Qualifizierte Elektronische Signatur. http://www.finanzamt.sachsen.de/eSignatur.html, abgerufen am 25. März 2019.

[2] Adobe Systems Incorporated. Adobe Portable Document Format Version 1.3. In *PDF Reference second edition*, 1999.

[3] Adobe Systems Incorporated. PDF 32000-1:2008. In *Document management - Portable document format - Part 1: PDF 1.7*, 2008.

[4] Ben Rogers. Digital Signatures in a PDF. https://www.adobe.com/devnet-docs/etk_deprecated/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf, abgerufen am 27. März 2019.

[5] StatCounter. Desktop Operating System Market Share Worldwide - February 2019. http://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-201802-201902, abgerufen am 28. März 2019.

[6] Das Europäische Parlament und der Rat der Europäischen Union. Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910, abgerufen am 25. März 2019.

[7] Christof Paar und Jan Pelzl. Digitale Signaturen. In *Kryptografie verständlich*, 2016.

[8] Tim Bienz und Richard Cohn. In *Portable Document Format Reference Manual*, 1993.

[9] Vladislav Mladenov, Christian Mainka, Karsten Meyer zu Selhausen, Martin Grothe und Jörg Schwenk. 1 Trillion Dollar Refund - How To Spoof PDF Signatures. 2018. https://pdf-insecurity.org/download/paper.pdf.

[10] Karsten Meyer zu Selhausen. Security of PDF Signatures. 2018. https://pdf-insecurity.org/download/DIGITALVERSION_KMeyerZuSelhausen_SecurityOfPDFSignatures_2018-11-25.pdf.