RUB

RUHR-UNIVERSITÄT BOCHUM

Sicherheitsanalyse von OpenDocument v1.2

Steve Martin

Exposé – 22. Oktober 2019.
Lehrstuhl für Netz- und Datensicherheit.

Betreuer: Prof. Dr. Jörg Schwenk
Berater: Dr.-Ing. Christian Mainka und Dr.-Ing. Vladislav Mladenov

hgi Lehrstuhl für Netz- und Datensicherheit

1 Einleitung

Das vom Technical Comitee of Organization for the Advancement of Structured Information Standards (OASIS) spezifizierte und im Jahr 2006 in der internationalen Norm ISO/IEC 26300 veröffentlichte Open Document Format for Office Applications (ODF) ist ein quelloffener Standard für Büroanwendungen. Ursprünglich wurde ODF von Sun Microsystems entwickelt.
ODF wird beispielsweise zur Erstellung von Präsentationen, Kalkulationstabellen, Textverarbeitungsdateien und Diagrammen, sowohl mit freien als auch proprietären Programmen in einem einheitlichem Format, genutzt.
In den folgenden Abschnitten wird ein kleiner Einblick in die Thematik ODF gegeben und näher betrachtet, welche IT-sicherheitstechnischen Aspekte zu beachten sind.

1.1 Motivation

Bei der Erstellung von Dokumenten nach dem ODF Standard wird die Auszeichnungssprache Extensible Markup Language (XML) verwendet. Eine OpenDocument Datei ist somit ein XML basiertes Dateiformat, welches eine einzelne XML Datei oder eine Sammlung dieser mit zusätzlich anderen Dateien, wie zum Beispiel Bildern, enthält, im ZIP-Format zusammengefasst und komprimiert ist.
Abhängig vom gewählten Verwendungszweck bietet ODF verschiedene Dateitypen. Im Folgenden werden einige Dateierweiterungen vorgestellt.

- .odt (OpenDocument Text) für Textdokumente
- .ods (OpenDocument Spreadsheet) für Tabellen
- .odp (OpenDocument Presentation) für Präsentationen
- .odg (OpenDocument Drawing) für Zeichnungen
- .odb (OpenDocument Database) für Datenbanken

Der eigentliche ODF Standard ist in drei Teile aufgeteilt.

Teil I: "OpenDocument Schema" definiert ein XML Schema für Office-Anwendungen und dessen Semantik [5]

Teil II: "Recalculated Formula (OpenFormula)Format" definiert eine formale Sprache, welche in OpenDocument Dokumenten verwendet wird [6]

Teil III: "Packages" definiert Paketformate, welche für OpenDocument Dokumente verwendet werden [7]

Um die Schutzziele Vertraulichkeit, Integrität und Nicht-Zurückweisbarkeit des Verfassers eines ODF Dokuments einzuhalten, nutzt der Standard zwei bereits in XML definierte Verfahren: XML Signature, um die Integrität und Nichtzurückweisbarkeit des Verfasser sicher zustellen und XML Encryption, um die Vertraulichkeit zu wahren.
Ein großer Vorteil von ODF im Gegensatz zu proprietären Dateiformaten ist, dass das Format in keiner Abhängigkeit zu einer bestimmten Software oder Versionen steht. Durch die Interoperabilität wird der Dokumentenaustausch enorm erleichtert, wovon vor allem Verwaltungsinstitutionen profitieren. Bereits in einem vom 28. November 2008 vorgestellten Beschluss des Rates der IT-Beauftragten wurde ein Vorschlag zur Einführung offener Dokumentenformate in der Bundesverwaltung eingereicht und am 02. Dezember 2008 beschlossen den ODF Standard schrittweise einzuführen [3]. Aus diesem Grund besteht daher ein besonderes Interesse die IT-sicherheitsrelevanten Features, welche ODF bietet, auf Schwachstellen hin zu untersuchen.

1.2 Forschungsstand

Da bereits einige Angriffe auf XML Signature und XML Encryption existieren, besteht das Interesse herauszufinden, ob diese Angriffe auch im ODF Kontext Anwendung finden könnte.
In der wissenschaftlichen Publikation "Analysis of Signature Wrapping Attacks and Countermeasures" [8] wurde bereits darauf aufmerksam gemacht, wie XML Signaturen umgangen werden können. Bei einer XML Signature Wrapping (XSW), auch bezeichnet als XML Rewriting, Attacke versucht der Angreifer den signierten Teil zu ändern ohne die eigentliche Signatur zu invalidieren.
In einer anderen wissenschaftlichen Publikation "Spoofing OpenPGP and S/MIME Signatures in Emails" [11] wurden Methoden aufgezeigt, wie Signaturen in E-Mails gefälscht werden können. Hierbei gilt es zu untersuchen, ob diese Methoden ebenfalls auf XML Signaturen im ODF Kontext eingesetzt werden können.

Aus der im Jahr 2018 veröffentlichten Publikation "Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels" [12] wurde darauf aufmerksam gemacht, dass ein Angreifer mit Hilfe eines bestimmten Binär Strings (bezeichnet als "Malleability Gadget") den Klartext einer mittels Advanced Encryption Standard (AES)-Cipher Block Chaining (CBC) verschlüsselten Nachricht manipulieren kann. Somit kann der Angreifer beliebige Klartexte erstellen, wodurch die modifizierten Chiffretexte, zum Beispiel im Email Kontext, zur Ausführung von Schadcode genutzt werden können. ODF nutzt zur Verschlüsselung ebenfalls XML Encryption im CBC-Modus. Es gilt zu untersuchen, ob dieser Angriff auch auf im ODF Format erstellte Dokumente anzuwenden ist.

2 Methodik

Das Ziel dieser Masterarbeit ist es, den Standard ODF auf Schwachstellen hin zu evaluieren, diese aufzuzeigen und nachzuweisen. In den folgenden Abschnitten werden die einzelnen Meilensteine, mögliche Probleme und Herausforderungen sowie die Zeit, die für die jeweiligen Arbeitspakete voraussichtlich benötigt wird, vorgestellt.

2.1 Überblick

Um die fachliche Expertise zu erlangen, ist es zunächst erforderlich, sich in den OASIS Standard für ODF [4] einzulesen. Hierbei liegt der Fokus vor allem auf Signatur und Verschlüsselung. Doch auch andere Punkte, wie zum Beispiel Formulareingaben, worüber eventuell Cross-Site-Scripting (XSS) Angriffe möglich sein könnten, müssen beachtet werden. Die erlangten Erkenntnisse, unter anderem auch welche weiteren Sicherheitsfeatures ODF bietet, werden dokumentiert und aufgezeigt.
Nach Sichtung der erforderlichen Unterlagen wird ein Testkatalog mit bereits bekannten Angriffsvektoren, in Bezug auf XML Signature, erstellt, welche später in erzeugten .odt, .ods, .odp und .odg Dateien getestet werden. Auch die während der Untersuchung aufgefallenen Angriffsmöglichkeiten werden in den Testkatalog aufgenommen, um sie in der Evaluierungsphase untersuchen zu können.
In der darauffolgenden Phase wird die Testumgebung entsprechend der zu testenden Angriffe aufgebaut. Hierbei werden in erster Linie mit den Open Source Programmen Apache OpenOffice und LibreOffice die erforderlichen Dateien unter Windows und Linux erzeugt und eventuell benötigte Drittanbieter Software installiert.
Nachdem alle Voraussetzungen für eine erfolgreiche Evaluierung erfüllt sind, werden die im Testkatalog aufgelisteten Angriffe auf die einzelnen Dateien ausgeführt und die Ergebnisse dokumentiert. Ein weiterer Teil der Evaluierung ist es, die im Standard angegebenen Sicherheitsfeatures zu testen. Etwaige Unterschiede in Bezug auf das Betriebssystem beziehungsweise der verwendeten Software werden ebenfalls dokumentiert.

2.2 Detaillierte Beschreibung

Das Ziel der ersten Phase "Einarbeitung in den ODF Standard" ist es, einen Überblick über das XML Schema, welches ODF verwendet, zu verschaffen. Der Fokus liegt hierbei vorrangig auf den Abschnitten Signatur und Verschlüsselung, welche im dritten Teil des Standards [7] näher beschrieben sind.
Die erste Phase umfasst folgende Arbeitspakete:

Nummer	Name	Obligatorisch/Fakultativ	Dauer
1	Dokumenttypen	Obligatorisch	1 Tag
2	Dokumentenstruktur	Obligatorisch	3 Tage
3	Metadaten (RDF und Non-RDF)	Fakultativ	3 Tage
4	Textinhalt	Fakultativ	3 Tage
5	Datenbank Front-End Dokumenteninhalt	Fakultativ	6 Tage
6	Formulareingabe und Event Listeners	Fakultativ	7 Tage
7	Signaturvorgang	Obligatorisch	9 Tage
8	Verschlüsselungsvorgang	Obligatorisch	9 Tage
9	Versionsunterschiede von XML Signature	Fakultativ	3 Tage
10	Versionsunterschiede von XML Encryption	Fakultativ	3 Tage

Die ersten sechs Arbeitspakete beziehen sich auf den ersten Teil des Standards [5]. Hierbei soll gezeigt werden, wie im ODF Standard Textinhalte und Benutzereingaben, wie zum Beispiel Datenbankeinträge oder Formulareingaben, verarbeitet werden.
Um die Arbeitspakete 7 und 8 zu bearbeiten, wird neben dem dritten Teil des Standards [7] auch die World Wide Web Consortium (W3C) Spezifikation für XML Signature [1] und XML Encryption [9], welche in ODF verwendet werden, benötigt. Erste Recherchen haben bereits ergeben, dass ODF v1.2 laut Spezifikation "XML Signature Syntax and Processing (Second Edition)" [1] nach W3C Empfehlung vom 10. Juni 2008 und "XML Encryption Syntax and Processing" [9] nach W3C Empfehlung vom 10. Dezember 2002 verwendet. Die jeweils aktuelle Version des Standards von XML Signature ist 2.0 (vom 23. Juli 2015) [2] und von XML Encryption 1.1 (vom 11. April 2013) [10]. In Arbeitspaket 9 und 10 soll optional untersucht werden, ob relevante Unterschiede zur aktuellen Version von XML Signature und XML Encryption existieren und ob sich daraus Schwachstellen ableiten lassen können.

Nachdem alle relevanten Erkenntnisse erarbeitet und dokumentiert wurden, besteht das Ziel in der zweiten Phase den Testkatalog für die Angriffe zu erstellen. Hierbei sollen ebenfalls die verschiedenen Angreifermodelle aufgezeigt werden.
Die zweite Phase umfasst folgende Arbeitspakete:

Nummer	Name	Obligatorisch/Fakultativ	Dauer
11	Erarbeiten der Angreifermodelle	Obligatorisch	3 Tage
12	Aufstellen der Angriffe gegen Signatur	Obligatorisch	5 Tage
13	Aufstellen der Angriffe gegen Verschlüsselung	Obligatorisch	5 Tage
14	Aufstellen der Angriffe gegen unsichere Features	Fakultativ	4 Tage
15	Erstellen der Ergebnistabelle	Obligatorisch	1 Tag

Arbeitspaket 11 besteht aus der Erstellung und Dokumentation der verschiedenen Angreifermodelle. Der Angreifer hat Erfolg, wenn der eigentliche Empfänger die vom Angreifer manipulierte Datei nicht von der originalen unterscheiden kann. Hierbei werden folgende Modelle betrachtet:

- Angreifer ist Ersteller des Dokuments und versucht Signatur zu fälschen
- Angreifer ist Ersteller des Dokuments und fügt Schadcode ein
- Angreifer versucht signiertes Dokument zu manipulieren
- Angreifer versucht signiertes und verschlüsseltes Dokument zu manipulieren
- Angreifer versucht verschlüsseltes Dokument zu lesen
- Angreifer versucht verschlüsseltes Dokument zu manipulieren

Nach der Erstellung der Angreifermodelle werden in den Arbeitspaketen 12 bis 14 die verschiedenen Angriffe kategorisiert, aufgelistet und deren geplante Folgen bestimmt. Hierbei gilt es sowohl bereits bekannte Angriffe als auch Angriffe aufzulisten, welche sich aus Phase 1, insbesondere eventuelle Angriffe die noch in älteren Versionen von XML Signature und XML Encryption möglich waren, herauskristallisiert haben.
Im letzten Arbeitspaket (15) aus Phase 2 werden die zu untersuchenden Merkmale festgelegt. Ebenfalls Bestandteil ist es, eine Tabelle vorzubereiten, welche die zu untersuchenden Merkmale und das Ergebnis auflistet.

In der dritten Phase werden die Voraussetzungen an die Testumgebung festgelegt und diese entsprechend eingerichtet. Da ebenfalls das Ziel darin besteht herauszufinden, ob es Unterschiede im Hinblick auf das gewählte Betriebssystem beziehungsweise die verwendete Software gibt, werden in dieser Phase auch die benötigten Dateien unter Verwendung des jeweiligen Betriebssystems generiert.
Die dritte Phase umfasst folgende Arbeitspakete:

Nummer	Name	Obligatorisch/Fakultativ	Dauer
16	Voraussetzungen der Testumgebung festlegen	Obligatorisch	2 Tage
17	Bereitstellung der Ressourcen	Obligatorisch	3 Tage
18	Einrichten der benötigten Software	Obligatorisch	2 Tage
19	Generierung der zu untersuchenden Dateien	Obligatorisch	1 Tag

In Phase 2 wurde festgelegt, welche Angreifermodelle betrachtet werden, welche Angriffe auf die Dateien ausgeübt werden und welche geplanten Folgen auftreten können. Aus diesen Aspekten ergeben sich die Voraussetzungen, welche die Testumgebung erfüllen muss, um Arbeitspaket 16 zu bearbeiten.
In Arbeitspaket 17 wird sowohl festgestellt, welche Hard- und Software benötigt wird, um die entsprechenden Voraussetzungen zu erfüllen, als auch die Beschaffung derer durchgeführt.
Sobald alle erforderlichen Ressourcen verfügbar sind, wird in Arbeitspaket 18 die Software installiert und eingerichtet.
Abschließend zu Phase 3 werden im Arbeitspaket 19 die erforderlichen Dateien erzeugt und einer Ordnerstruktur entsprechend zugeordnet.

Die Umsetzung der Angriffe wird in der vierten Phase durchgeführt und mittels Screenshots dargestellt. Hierbei wird jeder aufgelistete Angriff ausgeführt, das Systemverhalten dokumentiert und untersucht ob die geplanten Folgen auch der Wirklichkeit entsprechen.
Die vierte Phase umfasst folgende Arbeitspakete:

Nummer	Name	Obligatorisch/Fakultativ	Dauer
20	Angriff auf Signatur	Obligatorisch	10 Tage
21	Angriff auf Verschlüsselung	Obligatorisch	10 Tage
22	Angriff auf unsichere Features	Fakultativ	8 Tage
23	Angriff auf veraltete Version	Fakultativ	6 Tage

Das Arbeitspaket 20 umfasst alle Angriffe die gegen die Signatur gerichtet sind. Das Ziel ist es den Angriff so zu gestalten, dass die Signatur nicht invalidiert wird und somit das Opfer (der eigentliche Empfänger der Datei) keinen Unterschied zu einer nicht manipulierten Datei bemerkt.
Im Arbeitspaket 21 wird untersucht, welche Angriffe erfolgreich gegen die Verschlüsselung ausgeführt werden können.
Die von ODF bereitgestellten Sicherheitsfeatures werden im Arbeitspaket 22 angegriffen. Hierbei geht es insbesondere darum aufzuzeigen, welche Möglichkeiten ein Angreifer hat, auch auf andere Aspekte neben Signatur und Verschlüsselung, Einfluss zu nehmen, wie zum Beispiel mit einer Denial-of-Service (DoS) Attacke.
Im Arbeitspaket 23 werden die Angriffe getestet, welche sich aus den unterschiedlichen Versionen ergeben und ob diese Wirkung zeigen.

In der fünften und letzten Phase sollen die gesammelten Erkenntnisse zusammengefasst werden.
Die fünfte Phase umfasst folgende Arbeitspakete:

Nummer	Name	Obligatorisch/Fakultativ	Dauer
24	Fazit Angriff auf Signatur	Obligatorisch	3 Tage
25	Fazit Angriff auf Verschlüsselung	Obligatorisch	3 Tage
26	Fazit Angriff auf unsichere Features	Fakultativ	3 Tage
27	Fazit Angriff auf veraltete Version	Fakultativ	3 Tage
28	Gesamtwertung der Sicherheitstechnischen Aspekte von ODF	Obligatorisch	5 Tage

In den Arbeitspaketen 24 bis 27 sollen sowohl die Angriffe aus Phase 4 auf Verschlüsselung, Signatur und andere Aspekte als auch deren Folgen zusammengefasst werden.
Im Arbeitspaket 28 wird eine Gesamtwertung des Sicherheitskonzepts von ODF, im besonderem Maße bezogen auf Signatur und Verschlüsselung, vorgenommen. Hierbei geht es besonders darum erneut zu verdeutlichen, welche Ziele der Informationssicherheit (Vertraulichkeit, Integrität und Nicht-Zurückweisbarkeit des Verfassers) durch die im ODF Standard ergriffenen Maßnahmen erreicht wurden und wo eventuell noch Verbesserungsbedarf besteht.

Aus den 28 Arbeitspaketen ergeben sich 5 Phasen, welche ebenfalls die Meilensteine darstellen.
Die folgende Tabelle umfasst die fünf Phasen und dessen geplante Dauer:

Meilenstein	Phase	Dauer
1	Einarbeitung in den ODF Standard	47 Tage
2	Erstellung des Testkatalogs	18 Tage
3	Vorbereiten der Testumgebung	8 Tage
4	Angriffsdurchführung	34 Tage
5	Schlussfolgerungen aus den Angriffen	17 Tage

Die Dauer der Bearbeitung beträgt voraussichtlich 124 Tage.

3 Vorläufige Gliederung der Masterarbeit

Im Folgenden wird eine vorläufige Gliederung der Masterarbeit gegeben.

1. Einleitung
2. Einführung in den ODF Standard
   - 2.1 Dokumententypen und Verwendungszweck
   - 2.2 Allgemeine Dokumentenstruktur
   - 2.3 Verarbeitung von Text und Benutzereingaben
     - 2.3.1 Metadatenverarbeitung
     - 2.3.2 Textinhaltsverarbeitung
     - 2.3.3 Datenbankeingaben
     - 2.3.4 Formulareingaben
   - 2.4 XML Signature in ODF
     - 2.4.1 Signaturerzeugung
     - 2.4.2 Signaturvalidierung
   - 2.5 XML Encryption in ODF
     - 2.5.1 Verschlüsselungsvorgang
     - 2.5.2 Entschlüsselungsvorgang
   - 2.6 Versionsunterschiede zu XML Signature 2.0
   - 2.7 Versionsunterschiede zu XML Encryption 1.1
3. Angriffsplanung
   - 3.1 Definition der Angreifermodelle
     - 3.1.1 Angreifermodell I
     - 3.2.2 Angreifermodell II
     - 3.3.3 Angreifermodell III
     - 3.4.4 Angreifermodell IV
     - 3.5.5 Angreifermodell V
     - 3.6.6 Angreifermodell VI
   - 3.2 Angriffsvektoren gegen Signatur
   - 3.3 Angriffsvektoren gegen Verschlüsselung
   - 3.4 Angriffsvektoren gegen unsichere Features
   - 3.5 Definition der Untersuchungsmerkmale
4. Einrichten der Testumgebung
   - 4.1 Voraussetzungen
   - 4.2 Realisierung der Maßnahmen

5. Evaluierung
   5.1 Systemverhalten und Rückschlüsse gegen Signatur
   5.2 Systemverhalten und Rückschlüsse gegen Verschlüsselung
   5.3 Systemverhalten und Rückschlüsse gegen unsichere Features
6. Schlussbetrachtungen
   6.1 Zusammenfassung der Resultate
   6.2 Zukunftsausblick

4 Zeitlicher Ablauf

Es ist geplant, die Bearbeitung der Masterarbeit am 07.11.2019 zu beginnen. Der Bearbeitungszeitraum ergibt sich somit vom 07. November 2019 bis einschließlich zum 06. Mai 2020. In den folgenden Abschnitten werden die im Zeitraum befindlichen Wochenenden und gesetzlichen Feiertage, der Bearbeitungszeitraum der entsprechenden Arbeitspakete sowie eine zeitliche Abfolge der Arbeitspakete in Form eines Gantt-Diagramms vorgestellt.

4.1 Wochenenden und gesetzliche Feiertage

Die folgende Tabelle gibt Aufschluss über die im Bearbeitungszeitraum befindlichen Wochenenden und gesetzlichen Feiertage.

Art	Bezeichnung	Zeitpunkt/Zeitraum	Tagesanzahl
Wochenende	Samstag und Sonntag	09.11.2019 - 10.11.2019	2 Tage
Wochenende	Samstag und Sonntag	16.11.2019 - 17.11.2019	2 Tage
Wochenende	Samstag und Sonntag	23.11.2019 - 24.11.2019	2 Tage
Wochenende	Samstag und Sonntag	30.11.2019 - 01.12.2019	2 Tage
Wochenende	Samstag und Sonntag	07.12.2019 - 08.12.2019	2 Tage
Wochenende	Samstag und Sonntag	14.12.2019 - 15.12.2019	2 Tage
Wochenende	Samstag und Sonntag	21.12.2019 - 22.12.2019	2 Tage
Gesetzlicher Feiertag	1. Weihnachtstag	25.12.2019	1 Tag
Gesetzlicher Feiertag	2. Weihnachtstag	26.12.2019	1 Tag
Wochenende	Samstag und Sonntag	28.12.2019 - 29.12.2019	2 Tage
Gesetzlicher Feiertag	Neujahr	01.01.2020	1 Tag
Wochenende	Samstag und Sonntag	04.01.2020 - 05.01.2020	2 Tage
Wochenende	Samstag und Sonntag	11.01.2020 - 12.01.2020	2 Tage
Wochenende	Samstag und Sonntag	18.01.2020 - 19.01.2020	2 Tage
Wochenende	Samstag und Sonntag	25.01.2020 - 26.01.2020	2 Tage
Wochenende	Samstag und Sonntag	01.02.2020 - 02.02.2020	2 Tage
Wochenende	Samstag und Sonntag	08.02.2020 - 09.02.2020	2 Tage
Wochenende	Samstag und Sonntag	15.02.2020 - 16.02.2020	2 Tage
Wochenende	Samstag und Sonntag	22.02.2020 - 23.02.2020	2 Tage
Wochenende	Samstag und Sonntag	29.02.2020 - 01.03.2020	2 Tage
Wochenende	Samstag und Sonntag	07.03.2020 - 08.03.2020	2 Tage
Wochenende	Samstag und Sonntag	14.03.2020 - 15.03.2020	2 Tage
Wochenende	Samstag und Sonntag	21.03.2020 - 22.03.2020	2 Tage
Wochenende	Samstag und Sonntag	28.03.2020 - 29.03.2020	2 Tage
Wochenende	Samstag und Sonntag	04.04.2020 - 05.04.2020	2 Tage
Gesetzlicher Feiertag	Karfreitag	10.04.2020	1 Tag
Wochenende	Samstag und Sonntag	11.04.2020 - 12.04.2020	2 Tage
Gesetzlicher Feiertag	Ostermontag	13.04.2020	1 Tag
Wochenende	Samstag und Sonntag	18.04.2020 - 19.04.2020	2 Tage
Wochenende	Samstag und Sonntag	25.04.2020 - 26.04.2020	2 Tage
Gesetzlicher Feiertag	Tag der Arbeit	01.05.2020	1 Tag
Wochenende	Samstag und Sonntag	02.05.2020 - 03.05.2020	2 Tage

Es ergeben sich ein Gesamtanzahl von 26 Samstagen, 26 Sonntagen und 6 gesetzlichen Feiertagen. Somit stehen 124 Werktage zur Verfügung.

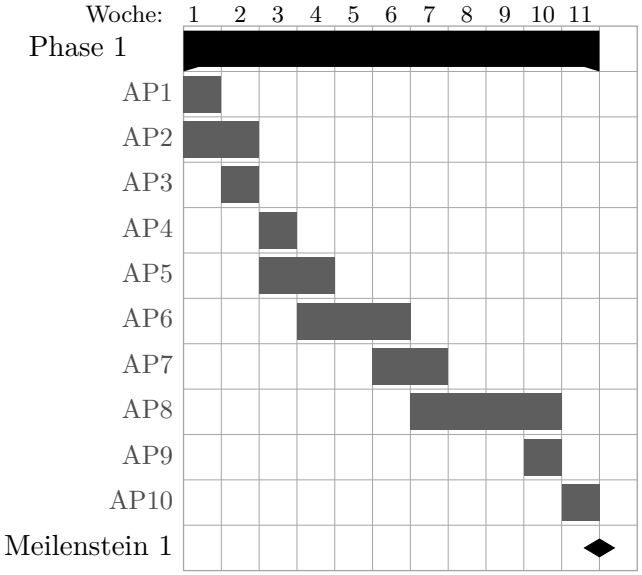
4.2 Bearbeitungszeitraum der Arbeitspakete

Die folgende Tabelle stellt den geplanten Bearbeitungszeitraum der Arbeitspakete dar.

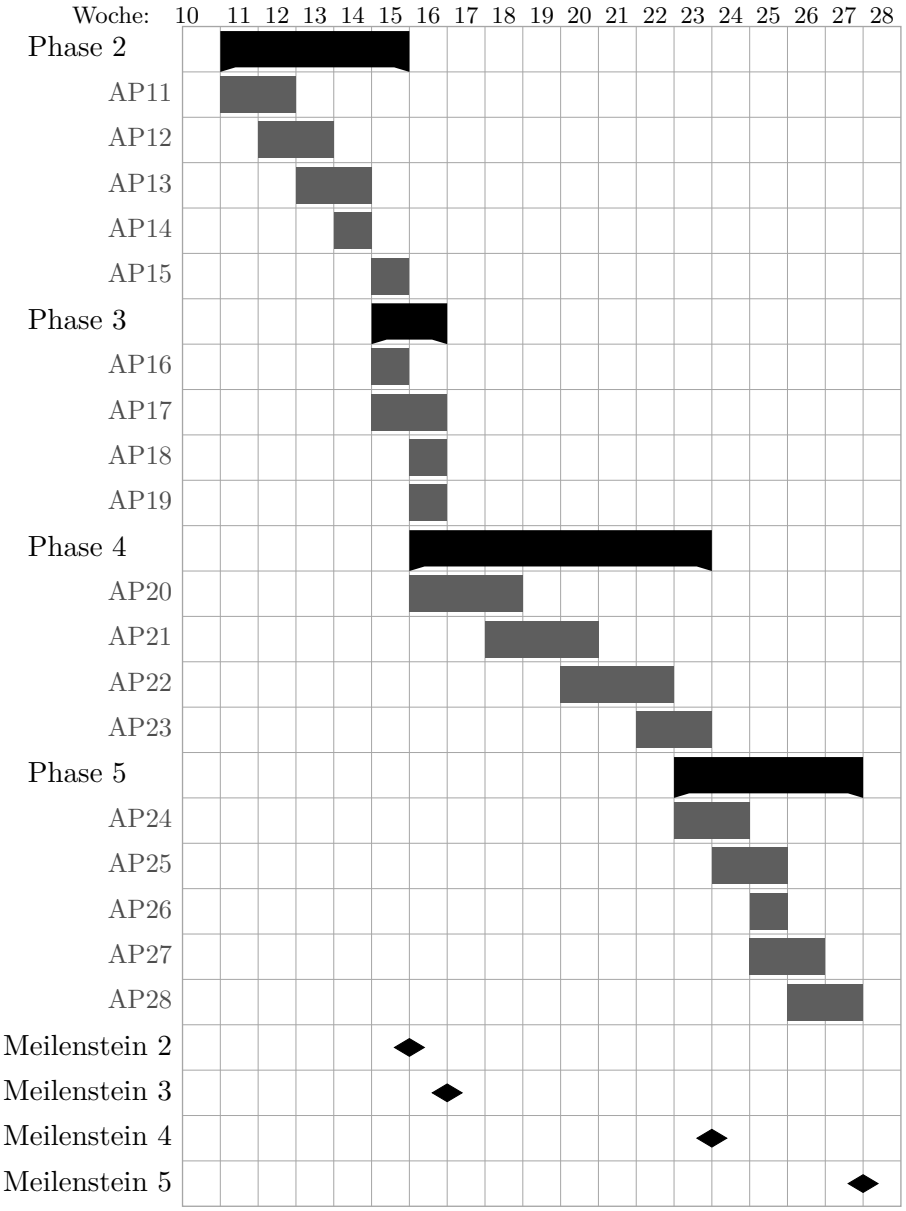
Nummer	Name	Bearbeitungszeitraum	Dauer
1	Dokumenttypen	07.11.2019	1 Tag
2	Dokumentenstruktur	08.11.2019 - 12.11.2019	3 Tage
3	Metadaten (RDF und Non-RDF)	13.11.2019 - 15.11.2019	3 Tage
4	Textinhalt	18.11.2019 - 20.11.2019	3 Tage
5	Datenbank Front-End Dokumenteninhalt	21.11.2019 - 28.11.2019	6 Tage
6	Formulareingabe und Event Listeners	29.11.2019 - 09.12.2019	7 Tage
7	Signaturvorgang	10.12.2019 - 20.12.2019	9 Tage
8	Verschlüsselungsvorgang	23.12.2019 - 07.01.2020	9 Tage
9	Versionsunterschiede von XML Signature	08.01.2020 - 10.01.2020	3 Tage
10	Versionsunterschiede von XML Encryption	13.01.2020 - 15.01.2020	3 Tage
11	Erarbeiten der Angreifermodelle	16.01.2020 - 20.01.2020	3 Tage
12	Aufstellen der Angriffe gegen Signatur	21.01.2020 - 27.01.2020	5 Tage
13	Aufstellen der Angriffe gegen Verschlüsselung	28.01.2020 - 03.02.2020	5 Tage
14	Aufstellen der Angriffe gegen unsichere Features	04.02.2020 - 07.02.2020	4 Tage
15	Erstellen der Ergebnistabelle	10.02.2020	1 Tag
16	Voraussetzungen der Testumgebung festlegen	11.02.2020 - 12.02.2020	2 Tage
17	Bereitstellung der Ressourcen	13.02.2020 - 17.02.2020	3 Tage
18	Einrichten der benötigten Software	18.02.2020 - 19.02.2020	2 Tage
19	Generierung der zu untersuchenden Dateien	20.02.2020	1 Tag
20	Angriff auf Signatur	21.02.2020 - 05.03.2020	10 Tage
21	Angriff auf Verschlüsselung	06.03.2020 - 19.03.2020	10 Tage
22	Angriff auf unsichere Features	20.03.2020 - 31.03.2020	8 Tage
23	Angriff auf veraltete Version	01.04.2020 - 08.04.2020	6 Tage
24	Fazit Angriff auf Signatur	09.04.2020 - 15.04.2020	3 Tage
25	Fazit Angriff auf Verschlüsselung	16.04.2020 - 20.04.2020	3 Tage
26	Fazit Angriff auf unsichere Features	21.04.2020 - 23.04.2020	3 Tage
27	Fazit Angriff auf veraltete Version	24.04.2020 - 27.04.2020	3 Tage
28	Gesamtwertung der Sicherheitstechnischen Aspekte von ODF	28.04.2020 - 05.05.2020	5 Tage

4.3 Gantt-Diagramm der Phase 1

Im aktuellen und folgenden Abschnitt wird der zeitliche Ablauf in Form eines Gantt-Diagramms vorgestellt. Die schwarzen Balken stellen die Wochen dar, in welchen die entsprechenden Arbeitspakete bearbeitet werden.



4.4 Gantt-Diagramm der Phase 2 bis 5



Literaturverzeichnis

[1] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, and Ed Simon. XML Signature Syntax and Processing (Second Edition). Standard, World Wide Web Consortium (W3C), Cambridge, Massachusetts, US, Juni 2008. URL `https://www.w3.org/TR/2008/REC-xmldsig-core-20080610/`. (Eingesehen am 11.09.2019).

[2] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, and Ed Simon. XML Signature Syntax and Processing Version 2.0. Standard, World Wide Web Consortium (W3C), Cambridge, Massachusetts, US, Juli 2015. URL `https://www.w3.org/TR/xmldsig-core2/`. (Eingesehen am 12.09.2019).

[3] Rat der IT-Beauftragten. Einführung offener Dokumentenformate in der Bundesverwaltung. Beschluss Nr. 11/2008, November 2008.

[4] Patrick Durusau, Michael Brauer, and Oracle Corporation. Open Document Format for OfficeApplications (OpenDocument) Version 1.2. Standard, Organization for the Advancement of Structured Information Standards (OASIS), Burlington, Massachusetts, US, September 2011. URL `http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2.html`. (Eingesehen am 11.09.2019).

[5] Patrick Durusau, Michael Brauer, and Oracle Corporation. Open Document Format for OfficeApplications (OpenDocument) Version 1.2. Standard, Organization for the Advancement of Structured Information Standards (OASIS), Burlington, Massachusetts, US, September 2011. URL `http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2-part1.html`. (Eingesehen am 11.09.2019).

[6] Patrick Durusau, Michael Brauer, and Oracle Corporation. Open Document Format for OfficeApplications (OpenDocument) Version 1.2. Standard, Organization for the Advancement of Structured Information Standards (OASIS), Burlington, Massachusetts, US, September 2011. URL `http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2-part2.html`. (Eingesehen am 11.09.2019).

[7] Patrick Durusau, Michael Brauer, and Oracle Corporation. Open Document Format for OfficeApplications (OpenDocument) Version 1.2. Standard, Organization for the Advancement of Structured Information Standards (OASIS), Burlington, Massachusetts, US, September 2011. URL `http://docs.`

oasis-open.org/office/v1.2/OpenDocument-v1.2-part3.html. (Eingesehen am 11.09.2019).

[8] S. Gajek, M. Jensen, L. Liao, and J. Schwenk. Analysis of signature wrapping attacks and countermeasures. In 2009 IEEE International Conference on Web Services, pages 575–582, Juli 2009. doi: 10.1109/ICWS.2009.12.

[9] Takeshi Imamura, Blair Dillaway, and Ed Simon. XML Encryption Syntax and Processing. Standard, World Wide Web Consortium (W3C), Cambridge, Massachusetts, US, Dezember 2002. URL https://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html. (Eingesehen am 11.09.2019).

[10] Takeshi Imamura, Blair Dillaway, Ed Simon, Kelvin Yiu, and Magnus Nyström. XML Encryption Syntax and Processing Version 1.1. Standard, World Wide Web Consortium (W3C), Cambridge, Massachusetts, US, April 2013. URL https://www.w3.org/TR/xmlenc-core1/. (Eingesehen am 11.09.2019).

[11] Jens Müller, Marcus Brinkmann, Damian Poddebniak, Hanno Böck, Sebastian Schinzel, Juraj Somorovsky, and Jörg Schwenk. "Johnny, you are fired!" – Spoofing OpenPGP and S/MIME Signatures in Emails. 28th USENIX Security Symposium, 2019.

[12] Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky, and Jörg Schwenk. Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels. 27th USENIX Security Symposium, 2018.