Efail: Angriffe auf S/MIME und OpenPGP

Damian Poddebniak,[1] Christian Dresen,[1] Jens Müller,[2] Fabian Ising,[1] Sebastian Schinzel,[1] Simon Friedberger,[3] Juraj Somorovsky,[2] Jörg Schwenk[2]

Kurzfassung:
OpenPGP und S/MIME sind die wichtigsten Standards für die Ende-zu-Ende Sicherheit von E-Mails. In unserem Artikel beschreiben wir zwei neuartige Angriffstechniken: *malleability Gadgets* und *direct exfiltration*. Malleability Gadgets erlauben es, den Klartext verschlüsselter E-Mails zu ändern und so schädliche Klartext-Bruchstücke in verschlüsselte E-Mails einzuschleusen. Diese Bruchstücke missbrauchen bestehende und standardkonforme *Backchannels (Rückkanäle)* und erlauben es nach der Entschlüsselung, den gesamten Klartext zu exfiltrieren. Bei direct exfiltration-Angriffen wird ausgenutzt, dass Mail-Clients auch dann entschlüsseln, wenn der Chiffretxt nur ein Unterknoten im MIME-Baum der Nachricht ist. Beide Angriffsarten werden ausgelöst, sobald der Empfänger eine einzelne E-Mail vom Angreifer entschlüsselt.
Die Wirksamkeit dieser Angriffe wurde sowohl für OpenPGP als auch für S/MIME durch Proof-of-Concept-Implementierungen nachgewiesen. Wir konnten Exfiltrationskanäle für 23 der 35 getesteten S/MIME E-Mail-Clients, und 10 der 28 getesteten OpenPGP-E-Mail-Clients nachweisen.

Stichworte: Efail, E-Mail, Kryptografische Angriffe, OpenPGP, S/MIME,

1. Einführung

E-Mail ist im Kern ein Kommunikationsmedium aus den Anfängen des Internet, das Nachrichten im Klartext von einem Postfach über mehrere Mailserver hinweg in ein anderes Postfach überträgt. Mittlerweile wird für viele Kommunikationspfade von E-Mails TLS als Transportverschlüsselung eingesetzt, was jedoch eine Ende-zu-Ende-Versschlüsselung nicht ersetzen kann: In den Postfächern und auf den Mailservern liegen die E-Mails im Klartext vor, und die Verschlüsselung kann nicht auf allen Transportwegen garantiert werden. Eine Ende-zu-Ende-Verschlüsselung schützt E-Mails außerdem bei unberechtigtem Zugriff auf IMAP-Postfächer.

Eine reine abschnittsweise Transportverschlüsselung ist besonders für solche Benutzer nicht ausreichend, die sensible Inhalte vor mächtigen Angreifern schützen müssen, wie z. B. Journalisten, politische Aktivisten oder Whistleblower. Für solche Benutzergruppen gibt es die beiden Ende-zu-Ende-Verschlüsselungstechnologien PGP und S/MIME. Beide Standards sind auf kryptografischer Ebene ähnlich und entstanden in den 90er Jahren. PGP wurde 1991 von Phil Zimmermann entwickelt und wurde später unter dem Standard OpenPGP weiterentwickelt. Das letzte Update bekam OpenPGP mit RFC4880 im Jahre 2007. Die Bestrebungen, OpenPGP erneut zu überarbeiten, wurden von der IETF 2017 wegen Inaktivität eingestellt. Seitdem führt der GnuPG-Chefentwickler Werner Koch die Überarbeitung des Standards weiter. Um PGP in den weit verbreiteten

[1] Fachhochschule Münster
[2] Ruhr-Universität Bochum
[3] NXP Semiconductors

Clients verwenden zu können, muss man üblicherweise Plugins installieren, um die PGP-Ver- und -Entschlüsselung im E-Mail-Client verwenden zu können.

S/MIME wurde erstmalig im Jahre 1995 spezifiziert und in den meisten verbreiteten E-Mail-Clients standardmäßig eingebaut. Es bekam das letzte Update mit RFC 5751 im Jahre 2010, wobei ein neues Update aktuell bei der IETF zur Begutachtung vorliegt.

Der Verschlüsselungsprozess ist bei beiden Standards ähnlich: der Absender generiert einen zufälligen symmetrischen Schlüssel und verschlüsselt damit eine E-Mail, z. B. über den AES-Algorithmus. Dieser AES-Schlüssel wird jetzt mit den öffentlichen Schlüsseln des Empfängers und des Absenders verschlüsselt und in die verschlüsselte Nachricht eingefügt. Der Empfänger entschlüsselt dann zuerst den AES-Schlüssel mit seinem privaten Schlüssel und kann damit die eigentliche Nachricht entschlüsseln.

Beide Standards vereint, dass verschlüsselte Nachrichten selbst gegen starke Angreifer geschützt sein sollten, die Netzwerkstrecken, Transportverschlüsselung, ganze E-Mail-Server oder gar das E-Mail-Konto von Opfern kontrollieren. Solange der Angreifer die privaten Schlüssel des Absenders oder eines der Empfänger nicht kennt, kann er nicht auf die Inhalte zugreifen.

Efail bezeichnet zwei grundlegend unterschiedliche Angriffsarten, die genutzt werden können, um die Klartexte von mit OpenPGP oder S/MIME verschlüsselten E-Mails zu erlangen. Die erste Variante ist der „Malleability Gadget“-Angriff, der Eigenschaften des CBC-Entschlüsselungsmodus in S/MIME und des CFB-Entschlüsselungsmodus in OpenPGP ausnutzt, um sich selbst exfiltrierende Nachrichten zu generieren. Die zweite Variante ist der „Direct Exfiltration“-Angriff, der Schwachstellen in E-Mail-Clients ausnutzt.

2. Der CBC Gadget-Angriff bei S/MIME

S/MIME nutzt bei der symmetrischen Verschlüsselung standardmäßig den Verschlüsselungsmodus Cipher Block Chaining (CBC). In diesem Modus wird bei der Entschlüsselung eines Chiffratblocks C_n der vorhergehende Chiffratblock C_{n-1} auf den entschlüsselten Text verxodert. Für den ersten Block C_0 gibt es keinen vorigen Block, weshalb ein sogenannter Initialisierungsvektor (IV) C_0 vorangestellt wird, siehe Bild 1.

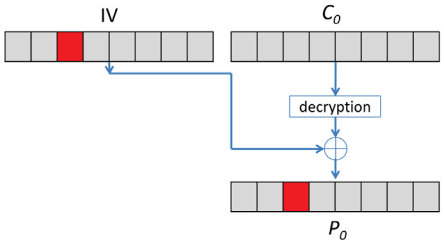

Abbildung 1. Der CBC-Entschlüsselungsmodus

Daraus geht auch hervor, dass die Änderung eines einzigen Bits an Stelle x im IV auch zu einer Änderung des x-ten Bits in P_0 führt. Daraus folgt, dass ein Angreifer mit Zugriff auf den Ciphertext den zugrundeliegenden Klartext präzise modifizieren kann.

Diese Eigenschaft nennt man in der Kryptologie "Formbarkeit" (engl. malleability). Der Efail-Angreifer nutzt diese Eigenschaft gezielt aus, um einen präparierten Klartext zu erstellen, der sich selbst exfiltriert, sobald das Opfer den Chiffretext entschlüsselt und die modifzierten Klartextdaten in einer entsprechenden Anwendung öffnet.

Interessanterweise ist grundsätzlich jedes Datenformat als Zielformat geeignet, das einen Rückkanal (engl. Backchannel) zum Angreifer öffnen kann, um einen selbst-exfiltrierenden Plaintext zu erstellen. HTML-E-Mails eigenen sich dafür sehr gut, da sie z. B. mittels verlinkter Bilder oder CSS-Styles Verbindungen zu beliebigen Domains öffnen können.

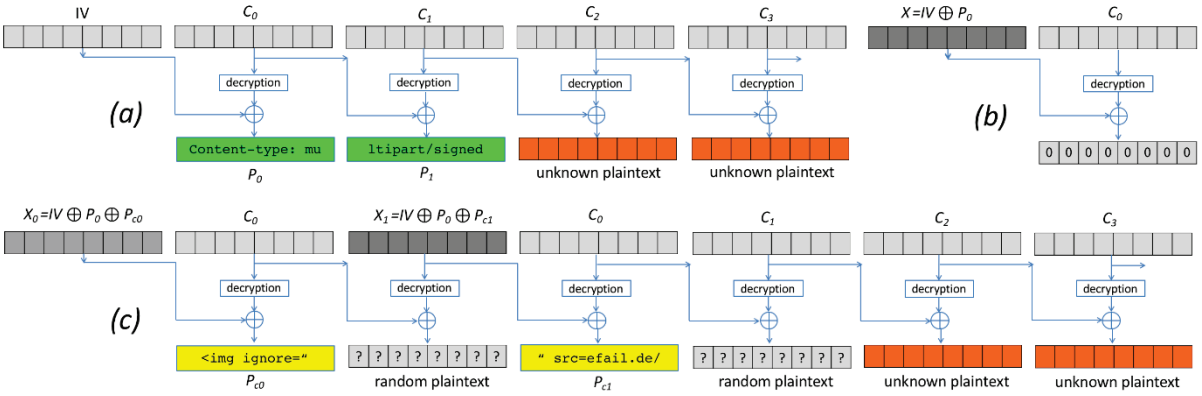

Abbildung 2. Der Aufbau von Malleability Gadgets

Als Grundvoraussetzung für den Angriff muss der Angreifer den Klartext von mindestens einem verschlüsselten Block kennen. Bild 2 (a) zeigt einen solchen Chiffretext C, bei dem die Inhalte der beiden Klartextblöcke P_0 und P_1 bekannt sind. In Bild 2 (b) verxodern wir P_0 mit dem Initialisierungsvektor IV und erhalten dadurch einen Klartextblock, der ausschließlich aus Null-Bytes besteht. Dieses „weisse Blatt Papier“ kann der Angreifer jetzt beliebig beschreiben, indem er den Angriffsklartext P_{c0} ebenfalls auf den Initialisierungsvektor verxodert. Wir nennen dieses Paar aus IV und C_0 ein CBC Gadget. Der Clou ist, dass man dieses CBC Gadget beliebig oft verändern und verketten kann, um sich praktisch beliebige Klartexte zu erstellen. Bild 2 (c) zeigt einen veränderten Klartext, der die hinteren unbekannten Plaintexte exfiltriert, sobald das Opfer den Klartext öffnet. Es zeigt auch, dass durch die veränderten Initialisierungsvektoren zwischen den Klartexten jeweils ein Block mit zufälligem Klartext steht, dessen Inhalt der Angreifer weder kennt noch bestimmen kann. Das ist eine Einschränkung für den Angreifer und er muss seinen Angriff so präparieren, dass diese zufälligen Datenmüllblöcke ignoriert werden. Bild 2 (c) löst dieses Problem für das HTML-Ausgabeformat, indem der Inhalt der Müllblöcke jeweils in ein HTML-Attribut eingefügt wird, das beim Rendern der E-Mail ignoriert wird.

Da der aktuell implementierte S/MIME-Standard keine Möglichkeit bietet, modifizierte Chiffretexte zu erkennen, können sich S/MIME-Implementierungen vor diesem Angriff aktuell nicht zuverlässig schützen. Das Abschalten von HTML bei der Entschlüsselung ist zwar sinnvoll, da es den Angriff über HTML-E-Mails wie oben dargestellt verhin

dert. Es verhindert aber nicht, dass ein Angreifer in das Chiffrat andere Dateiformate einbaut, die ebenfalls die Möglichkeit haben, Klartexte an den Angreifer zu schicken.

3. Der CFB Gadget-Angriff bei OpenPGP

PGP nutzt den Cipher Feedback Verschlüsselungsmodus, der ähnlich wie CBC funktioniert und ebenfalls die Malleability-Eigenschaft besitzt. Daher lassen sich auch hier Malleability Gadgets, im Folgenden CFB Gadgets genannt, erzeugen, mit denen selbstexfiltrierende Nachrichten erstellt werden können. Es gibt jedoch zwei Eigenschaften von PGP, die die Angriffe substanziell erschweren. OpenPGP komprimiert den Klartext vor der Verschlüsselung, womit das Raten eines Klartextblocks erschwert wird. Zweitens fügen moderne OpenPGP-Anwendungen einen Modification Detection Code (MDC) ein, der die für die Erstellung von CFB Gadgets nötigen Chiffrat-Modifikationen erkennt. Im Folgenden beschreiben wir, wie wir die Daten trotz Kompression exfiltrieren konnten.

Das Raten eines Klartextblocks ist bei S/MIME-verschlüsselten E-Mails relativ leicht, da der Klartext immer mit einer MIME-"Content-type"-Angabe startet, die E-Mail-Clients statisch setzen und die somit vom Angreifer leicht geraten werden können. Bei OpenPGP-Chiffretexten ist das nicht ganz so einfach. Zwar enthält der Klartext auch einen MIME-Content-type, allerdings wird der Klartext vor der Verschlüsselung komprimiert, was das Erraten einzelner Bytes wesentlich schwieriger macht. Wir haben dafür zwei Fallstudien durchgeführt, um die Komplexität abschätzen zu können, die benötigten elf bekannten Klartextbytes erraten zu können. Die erste Fallstudie wurde über automatisch generierte E-Mails geführt, die einen Link zum Neusetzen seines Facebook-Passworts enthielten. Dieses Beispiel wurde gewählt, da Facebook seinen Usern erlaubt, seine öffentlichen PGP-Schlüssel zu konfigurieren, um künftig nur noch PGP-verschlüsselte E-Mails von Facebook zu erlangen. Diese E-Mails sind, bis auf einige IDs im Link und in der Anrede statisch, weshalb der Angreifer den Großteil des Plaintexts kennt. Im Ergebnis sind die ersten elf Bytes des komprimierten Klartextes auf insgesamt nur rund 1.500 Möglichkeiten beschränkt. Da ein Mail-Client in unseren Tests bis zu 500 Chiffrate pro E-Mail entschlüsseln konnte, würden demnach drei Angriffs-E-Mmails reichen, um über PGP verschlüsselte Facebook-Passwort-Reset-E-Mails zu exfiltrieren.

Um diese Messung auch bei weniger strukturierten E-Mails durchzuführen, haben wir den Enron-Datensatz auf die gleiche Weise analysiert. Der Datensatz besteht aus rund 500.000 unstrukturierten E-Mails, bei denen die ersten elf Bytes nur einen von rund 2700 Werten annehmen konnten. Eine dieser E-Mails kann demnach über rund sechs AngriffsE-Mails exfiltiert werden.

4. Direct Exfiltration

Zusätzlich zu den gezeigten Kern-Angriffen von Efail, gab es noch eine Reihe anderer Schwachstellen, die keinen direkten Bezug zu S/MIME und PGP haben, sondern die Besonderheiten von MIME-Parsing in E-Mail-Clients ausnutzen. So nutzt der Direct Exfiltration-Angriff Schwachstellen in Mozilla Thunderbird, Apple Mail und iOS Mail

aus, um den Klartext einer verschlüsselten E-Mail direkt zu exfiltrieren. Diese Schwachstellen müssen in den jeweiligen E-Mail-Clients geschlossen werden und funktionieren wie folgt: Der Angreifer erstellt eine neue E-Mail mit drei MIME-Teilen. Der erste MIME-Teil hat den Content-Type HTML und endet mit einem HTML-Image-Tag, dessen src-Attribut zwar geöffnet, aber nicht mit Anführungszeichen geschlossen wird. Die URL des Bildes bleibt daher offen. Der zweite MIME-Teil enthält den OpenPGP oder S/MIME ciphertext. Der dritte MIME-Teil hat ebenfalls den Content-Type HTML und schließt die Bild-URL aus dem ersten MIME-Teil, siehe Bild 3.

```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

Abbildung 3. Der Direct Exfiltration-Angriff

Der Angreifer sendet die E-Mail jetzt zum Opfer. Der E-Mail-Client entschlüsselt den zweiten MIME-Teil und fügt die drei Body-Teile zu einem HTML-Dokument zusammen, wie in Bild 4 gezeigt.

```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

Abbildung 4. Der E-Mail-Client baut die drei MIME-Teile zu einem Teil zusammen.

Man sieht hier, dass in Zeile 1 eine Bild-URL geöffnet wird, aber erst in Zeile 4 geschlossen wird. Die URL erstreckt sich demnach über vier Zeilen. Anschließend kodiert das E-Mail-Programm alle nicht-druckbaren Zeichen (z.B. %20 ist das Leerzeichen) und fragt die URL ab. Da der URL-Pfad den Klartext enthält, schickt der E-Mail-Client des Opfers den Klartext an den Angreifer, siehe Bild 5.

```
http://efail.de/Secret%20MeetingTomorrow%209pm
```

Abbildung 5. Die angefragte URL enthält den Klartext

Der Direct Exfiltration-Angriff funktioniert gleichermaßen für OpenPGP- und S/MIME-Chiffretexte. Wichtig ist hierbei zu erwähnen, dass hier nicht nur verschlüsselte E-Mails betroffen sind. Über diese Schwachstelle können auch Chiffrate

gebrochen werden, die in nicht-E-Mail-Anwendungen oder auf der Kommandozeile erstellt wurden, solange das gleiche Schlüsselpaar auch im E-Mail-Client verwendet wird.

5. Evaluierung

In unserer Studie haben wir zwei unabhängige Begriffe eingeführt: Rückkanal und Exfiltratioskanal [1]. Ein Rückkanal ist jede Funktionalität, welche einen E-Mail-Client dazu zwingt, eine Verbindung nach außen herzustellen. Nicht jeder Backchannel kann jedoch für Exfiltrierung der entschlüsselten Klartexte eingesetzt werden. Dies kann unterschiedliche Gründe haben. Zum Beispiel HTML-Inhalt, der zum Laden externer Bilder in unverschlüsselten E-Mails verwendet werden kann, wird normalerweise nicht in veralteteten PGP/INLINE-Nachrichten interpretiert. Eine Übersicht der getesteten Rückkanäle wird in unserem Artikel aufgelistet [1].

OS	Client	S/MIME	PGP		
			-MDC	+MDC	SE
Windows	Outlook 2007	∠	∠	∠	√
	Outlook 2010	∠	√	√	√
	Outlook 2013	⊥	√	√	√
	Outlook 2016	⊥	√	√	√
	Win. 10 Mail	∠	–	–	–
	Win. Live Mail	∠	–	–	–
	The Bat!	⊥	√	√	√
	Postbox	∠	∠	∠	∠
	eM Client	∠	√	∠	√
	IBM Notes	∠	–	–	–
Linux	Thunderbird	∠	∠	∠	∠
	Evolution	∠	√	√	√
	Trojitá	∠	√	√	√
	KMail	⊥	√	√	√
	Claws	√	√	√	√
	Mutt	√	√	√	√
macOS	Apple Mail	∠	∠	∠	∠
	MailMate	∠	√	√	√
	Airmail	∠	∠	∠	∠
iOS	Mail App	∠	–	–	–
	Canary Mail	–	√	√	√

OS	Client	S/MIME	PGP		
			-MDC	+MDC	SE
Android	K-9 Mail	–	√	√	√
	R2Mail2	∠	√	∠	√
	MailDroid	∠	√	∠	√
	Nine	∠	–	–	–
Webmail	United Internet	–	√	√	√
	Mailbox.org	–	√	√	√
	ProtonMail	–	√	√	√
	Mailfence	–	√	√	√
	GMail	∠	–	–	–
Webapp	Roundcube	–	√	√	∠
	Horde IMP	⊥	√	∠	∠
	AfterLogic	–	√	√	√
	Rainloop	–	√	√	√
	Mailpile	–	√	√	√

∠ Exfiltration channel (no user interaction)
⊥ Exfiltration channel (user interaction required)
√ No exfiltration channel
– encryption scheme not supported

Abbildung 6. Exfiltration der Klartexte in 23 S/MIME Email-Clients möglich. OpenPGP Email-Clients haben besser abgeschnitten. Dies ist vor allem dank dem Schutz von Modification Detection Codes (MDCs).

Im Vergleich zu einem Rückkannal kann ein Exfiltrationskanal für eine Klartext-Exfiltration direkt eingesetzt werden. Abbildung 6 zeigt eine Übersicht der 35 E-Mail-Clients, die S/MIME oder PGP unterstützen und für Efail anfällig sind.[4] 23 der untersuchten S/MIME E-Mail-Clients waren für eine direkte Exfiltration anfällig. Davon haben 5 dieser Angriffe eine Benutzer-Interaktion benötigt, etwa Klick auf ein Element oder explizite Erlaubnis zum Nachladen eines Bildes. Nur zwei der getesteten S/MIME E-Mail-Clients waren für Efail nicht anfällig.

Die OpenPGP E-Mail-Clients haben in unserer Evaluierung besser abgeschnitten. Eine Klartext-Exfiltration war in vielen der Clients nicht möglich, weil sie MDCs streng geprüft haben. Ein MDC wird als SHA1 über den Klartext vor der Verschlüsselung

[4] Die genauen Versionen der getesteten Email-Clients ist in unserem Artikel aufgelistet [1].

berechnet. Da unsere Efail-Angriffe den Chriffretext und damit auch den resultierenden Klartext manipulieren, wird der MDC nach der Entschlüsselung ungültig. Trotzdem ist es uns gelungen die MDCs in 10 der getesteten OpenPGP E-Mail-Clients zu umgehen, siehe Abbildung 6. Dies war auf drei Arten möglich. Erstens war es möglich die MDCs zu entfernen (-MDC). Zweitens haben einige der Clients komplett ignoriert und nicht überprüft, ob der MDC korrekt ist. Sie haben auch manipulierte Chiffretexte bearbeitet (+MDC). Drittens war ein Downgrade von SEIP-[5] auf SE-Pakete[6] möglich, in welchen MDCs nicht vorhanden sind.

Die untersuchten Rückkanäle, die zur Exfiltration geführt haben, lassen sich in folgende Gruppen unterteilen:

- Web-basierte Rückkanäle: Die prominentesten Web-basierten Rückkänäle sind Bilder, die in 13 der getesteten E-Mail-Clients sogar automatisch nachgeladen wurden. HTML hat aber viele zusätzliche Elemente, die zur Exfiltration ausgenutzt werden können, z.B. `meta` oder `link`-Elemente. Web-Technologien bieten aber auch andere Formen von Rückkanälen. Dazu gehören spezifische Cascading Style Sheets (CSS) Elemente oder Javascript-Funktionen, siehe [1].
- S/MIME-spezifische Rückkanäle: Bei der Überprüfung von S/MIME Zertifikaten können externe Ressourcen angefragt werden. Dies kann mit Nachladen von intermediate Zertifikaten oder OCSP[7] mit CRL[8] Requests möglich sein.
- OpenPGP-spezifische Rückkanäle: Ein E-Mail-Client, der eine mit OpenPGP signierte Nachricht empfängt, kann versuchen, den entsprechenden öffentlichen Schlüssel automatisch herunterzuladen. Wir haben in unserer Studie mindestens einen E-Mail-Client gesehen, der anhand einer Key-ID versucht hat den Schlüssel nachzuladen.
- Externe Anhänge: Der `message/external-body` Inhaltstyp ermöglicht Verweise auf externe Ressourcen als MIME-Teile, anstatt sie direkt in die Mail aufzunehmen. `Remote-Attachment-Url` lädt externe Anhänge nach.

Unser Artikel summarisiert alle Rückkanäle und deren Anwendbarkeit auf die getesteten E-Mail-Clients [1].

6. Gegenmaßnahmen

Die Präsenz eines Rückkanals ist entscheidend, ob unsere Angriffe anwendbar sind und ob entschlüsselte Klartexte exfiltriert werden können. Ein zuverlässiges Blockieren aller Rückkanäle, einschließlich derer, die nicht auf HTML basieren, würde alle Angriffe wie dargestellt verhindern. Sie behebt jedoch nicht die zugrunde liegende Sicherheitsanfälligkeit in den S/MIME- und OpenPGP-Standards. In einem umfassenderen Szenario kann ein Angreifer auch binäre Anhänge einfügen oder bereits angehängte Anhänge modifizieren, sodass die Exfiltration später durchgeführt wird, auch wenn kein E-Mail-

5 SEIP: Symmetrically Encrypted and Integrity Protected

6 SE: Symmetrically Encrypted

7 Online Certificate Status Protocol

8 Certificate Revocation Lists

Client beteiligt ist. Dies kann etwa mit dem Anhängen von PDF-und Word-Dokumenten ermöglicht werden, oder mit dem Einsatz von E-Mail-Firewalls, welche die entschlüsselten Daten nicht direkt bearbeiten. Daher ist das Blockieren von Rückkanälen nur eine kurzfristige Lösung. Im Folgenden stellen wir langfristige Maßnahmen vor, die eine Aktualisierung der Standards erfordern.

6.1. Gegenmaßnahmen gegen Direct Exfiltration Angriffe

Diese Angriffe nutzen die komplexe MIME-Struktur aus, die Verschachtelung der E-Mail-Inhalte ermöglicht. Es werden unterschiedliche E-Mail-Teile nach der Entschlüsselung zusammengesetzt (durch `multipart/mixed`), so dass der Angreifer sehr präzis seine Exfiltrationskanäle definieren kann. Weder S/MIME noch OpenPGP definieren, wie sich E-Mail-Clients in solchen Fällen verhalten sollen.

In Web-Szenarien ist ein typischer Schutz gegen diese Art von Angriffen eine Same Origin Policy. Ähnliche Schutzmechanismen könnten auch in E-Mail-Szenarien angewendet werden. Diese sollten sicherstellen, dass E-Mail-Teile mit unterschiedlichen Sicherheitseigenschaften nicht kombiniert werden.

So ein Schutzmechanismus würde allerdings nicht in allen Fällen helfen. Wenn eine E-Mail-Firewall die entschlüsselten Inhalte weiterleitet, kann eine Exfiltration im Backend enforciert werden. Daher ist in solchen Szenarien empfehlenswert, nur den ersten E-Mail-Teil zu entschlüsseln und die restlichen Teile als Anhänge darzustellen.

Gegenmaßnahmen gegen Direct Exfiltration Angriffe wurden mittlereweile in mehreren der anfälligen E-Mail-Clients implementiert. Einige der Clients erlauben eine Entschlüsselung nur dann, wenn die E-Mail aus einem Teil besteht.

Wir hoffen, dass diese Gegenmaßnahmen in den zukünftigen Standards adressiert werden.

6.2. Gegenmaßnahmen gegen Malleability Gadget Angriffe

Das grundlegende Problem von Efail ist die Malleability-Eigenschaft der eingesetzten Betriebsmodi; CBC und CFB erlauben es die Klartexte zu modifizieren, ohne Zugriff auf den kryptografischen Schlüssel zu haben. Kryptografisch könnten diese Angriffe mit dem Einsatz einer authentisierten Verschlüsselung (Authenticated Encryption) verhindert werden. Wenn diese eingesetzt wird, werden Modifikationen auf den Chiffretexten sofort erkannt. Damit ist jene Modifikation der resultierende Klartexte unmöglich. Zu diesen Verfahren gehören zum Beispiel Betriebsmodi wie AES-GCM oder EAX.

Allerdings ist anzumerken, dass der Einsatz einer authentisierten Verschlüsselung nicht alle Probleme direkt beseitigt. Backwards Compatibility oder Streaming-basierte Entschlüsselung kann zu spezifischen Angriffen führen, die auch adressierte werden sollten [1].

Motiviert durch unsere Angriffe wurden neue Betriebsmodi in die zur Zeit spezifizierten Standards von S/MIME [4] und OpenPGP [5] eingefügt.

7. Ausblick

Sowohl OpenPGP als auch S/MIME nutzen kryptografische Konstruktionen, die in anderen Protokollen wie TLS und SSH mehrfach zu kritischen Schwachstellen geführt haben. OpenPGP und S/MIME sind bisher glimpflich davon gekommen, da man annahm, dass beide Standards sogenannte Offline-Protokolle sind. Die meisten der Angriffe gegen TLS und SSH setzten voraus, dass der Angreifer mehrfach ausgewählte Chiffrate zum Server hinschicken kann und der Server dabei als Orakel wirkt. Die Efail-Angriffe haben gezeigt, dass zumindest bei der E-Mail-Verschlüsselung die Offline-Protokolle OpenPGP und S/MIME zu Online-Protokollen werden. Der E-Mail-Client des Opfers wird dabei zu einem Entschlüsselungs-Orakel, das der Angreifer nutzen kann, um den vollen Klartext verschlüsselter E-Mails zu erlangen.

Der aktuell praktisch verabschiedete TLS 1.3-Standard hat den Maßstab gesetzt, wie moderne Kryptografie aussieht. Richtig wäre jetzt, sich daran zu orientieren und zu diskutieren, wie man OpenPGP und S/MIME anpasst, um auch für die Zukunft genügend Puffer zu liefern, dass sie selbst in Online-Szenarien sicher betrieben werden können.

Literaturhinweise

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

[2] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer. OpenPGP message format. November 2007. RFC4880.

[3] B. Ramsdell, S. Turner. Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3.2 message specification. January 2010. RFC5751.

[4] J. Schaad, B. Ramsdell, S. Turner. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. Draft. September 2018

[5] W. Koch, B. Carlson, R. Tse, D. Atkins. OpenPGP Message Format. Draft. November 2018.

[6] N. Freed, N. Borenstein. Multipurpose Internet Mail Extensions (MIME) part one: Format of Internet message bodies. November 1996. RFC2045.