Original-URL des Artikels: https://www.golem.de/news/pgp-smime-die-wichtigsten-fakten-zu-efail-1805-134493.html **Veröffentlicht:** 22.05.2018 14:27 **Kurz-URL:** https://glm.io/134493

PGP/SMIME

Die wichtigsten Fakten zu Efail

Im Zusammenhang mit den Efail genannten Sicherheitslücken bei verschlüsselten E-Mails sind viele missverständliche und widersprüchliche Informationen verbreitet worden. Wir fassen die richtigen Informationen zusammen.

Die E-Mail-Sicherheitslücke, mit der sich die Inhalte von verschlüsselten Mails exfiltrieren lassen, hat zu heftigen Diskussionen geführt. Vor allem die Electronic Frontier Foundation musste viel Kritik für ihre Empfehlung einstecken, Mailverschlüsselungstools vorerst zu deinstallieren. Den Autoren des E-Mail-Angriffs und einigen Journalisten wurde vorgeworfen, Panikmache zu betreiben. Auch im Golem.de-Forum gab es viel Kritik. Wir versuchen, die wichtigsten Fakten zu sortieren.

Wurden die Entwickler von GnuPG nicht informiert?

In einer ersten Reaktion auf dem Twitter-Account des GnuPG-Projekts wurde behauptet, dass die Autoren von Efail die GnuPG-Entwickler nicht kontaktiert hätten. Das stellte sich jedoch als falsch heraus. GnuPG war bereits im November 2017 über die Angriffe informiert worden. Was dann folgte, sieht vor allem nach einem Kommunikationsproblem aus: Die GnuPG-Entwickler erkannten offenbar nicht, wie schwerwiegend der Angriff war, und dachten fälschlicherweise, durch den Einsatz des MDC-Verfahrens (Modification Detection Code) werde der Angriff vollständig verhindert. Danach brach der Kontakt ab.

Ein Problem bei Efail war, dass zum Zeitpunkt der Veröffentlichung für viele der betroffenen Mailclients keine Updates bereitstanden. Dabei waren sie bereits Monate vorher informiert worden.

Updaten und alles ist gut?

Thunderbird wurde zum ersten Mal im Oktober 2017 kontaktiert. Die schwerwiegendste Lücke, die sogenannte Direct Exfiltration, wurde im Februar 2018 an Thunderbird gemeldet. Auch in der am Samstag veröffentlichten Thunderbird-Version 52.8.0 gibt es noch Probleme. Bisher überhaupt keine Reaktion gibt es von den Herstellern großer kommerzieller Mailclients. In Apple Mail funktioniert die Direct-Exfiltration-Lücke ebenfalls, ein Update gibt es nicht.

Noch desaströser sieht das Ganze in Sachen S/MIME aus, denn hier ist überhaupt nicht klar, wie man die Lücke fixen soll, da der Standard fundamentale Probleme aufweist. Das dürfte vor allem Nutzer von Microsoft Outlook, die bislang ihre E-Mails mit S/MIME schützen, vor die Frage stellen, was sie nun eigentlich tun sollen.

Obwohl es auch mit OpenPGP einige Probleme gibt, lautet daher möglicherweise der beste Ratschlag für S/MIME-Anwender, einen Umstieg auf PGP-basierte Systeme durchzuführen.

Handelte es sich nur um Bugs in E-Mail-Clients?

In ihrer ersten Stellungnahme schreiben die Entwickler von GnuPG und Gpg4Win, dass das Paper nur eine Auflistung von Bugs in Mailclients sei. In mehreren Medienberichten wurde zudem geschrieben, dass die Standards S/MIME und OpenPGP weiterhin sicher seien.

Doch das ist so nicht korrekt. Dass verschlüsselte Nachrichten manipuliert werden können, liegt an den verwendeten Verschlüsselungsverfahren. In beiden Fällen muss man den Standard als gebrochen bezeichnen, doch im Falle von OpenPGP gibt es die Möglichkeit, die Angriffe zu vermeiden.

Was ist das Problem im S/MIME-Standard?

Der jüngste S/MIME-Standard 3.2 sieht zur Verschlüsselung ausschließlich AES im CBC-Modus vor. Dieses Verfahren bietet keinerlei Schutz gegen Nachrichtenmanipulationen.

Es gibt mit RFC 5084 einen Standard, der den Einsatz von GCM (Galois/Counter Mode) und CCM (Counter with CBC-MAC) für die Verschlüsselung in Cryptographic Message Syntax (CMS) definiert. GCM und CCM sind authentifizierte Verschlüsselungsverfahren, die eine Nachrichtenmanipulation verhindern würden. CMS ist das Nachrichtenformat, das in S/MIME zum Einsatz kommt. Allerdings wird im S/MIME-Standard selbst nirgendwo auf diesen RFC verwiesen und er wird bislang auch nirgendwo unterstützt.

Was ist das Problem im OpenPGP-Standard?

Anders als in S/MIME ist im OpenPGP-Standard ein Verfahren vorgesehen, um Nachrichtenmanipulationen zu verhindern; der sogenannte Modification Detection Code (MDC). Dabei wird ein Hash der Nachricht mit SHA-1 erstellt und anschließend verschlüsselt an die Nachricht angehängt.

Das Verfahren ist aus kryptographischer Sicht eher ungewöhnlich, aber zumindest bisher sind keine Sicherheitslücken in MDC selbst bekannt. Auffällig ist die Verwendung der unsicheren Hashfunktion SHA-1. Google konnte voriges Jahr einen praktischen Kollisionsangriff gegen SHA-1 demonstrieren. Doch ein Kollisionsangriff scheint in diesem Fall keine Rolle zu spielen.

Problematisch ist aber, dass der Standard keine genauen Anweisungen enthält, wie eine Implementierung mit Nachrichten mit fehlerhaftem oder fehlendem MDC umgehen soll. Dort heißt es, dass ein fehlerhafter MDC als Sicherheitsproblem behandelt werden muss. Weiterhin soll dem Nutzer eine Fehlermeldung angezeigt werden.

Das Problem: Implementiert man OpenPGP naiv nach diesen Vorgaben, erscheint es naheliegend, eine Nachricht zunächst zu entschlüsseln und dann - bei fehlendem MDC - eine Fehlermeldung anzuzeigen. Genau das führt aber zu den Angriffsszenarien wie E-Fail.

Ein weiteres Problem: Die Verwendung des MDC ist optional. Der OpenPGP-Standard sieht verschiedene Pakettypen für verschlüsselte Daten vor. Pakete vom Typ 9 (Symmetrically Encrypted Data Packet) enthalten keinen MDC, Pakete vom Typ 18 (Symmetrically Encrypted Integrity Protected Data Packet) kommen mit MDC-Schutz. Da das Datenformat ansonsten fast identisch ist, kann ein Angreifer ein Paket mit MDC-Schutz einfach in ein ungeschütztes Paket umwandeln.

Wer den OpenPGP-Standard in einem Mailclient naiv implementiert, führt also zwei Sicherheitslücken ein. Man kann den Standard nur sicher implementieren, indem man ihn unvollständig implementiert und bei Fehlern strenger reagiert. Zwei Dinge müssen dabei berücksichtigt werden: Nachrichten mit MDC-Fehlern dürfen nicht angezeigt werden und Datenpakete ohne MDC dürfen nicht unterstützt werden.

In den aktuellen Versionen der meisten OpenPGP-Plugins wird das inzwischen so umgesetzt. Doch davon zu sprechen, dass der Standard völlig sicher sei, ist nicht korrekt.

Ein Entwurf für eine Aktualisierung des Standards existiert, doch die Arbeiten daran gingen bislang nur zäh voran.

Externe Inhalte, HTML-Mails und Sicherheit

Was ist das Problem mit der GnuPG-API?

Zunächst muss man wissen, dass GnuPG keine Bibliothek bereitstellt. Wenn ein anderes Programm GnuPG nutzen will, wird es über das Kommandozeileninterface aufgerufen. Es gibt eine Wrapper-Bibliothek namens GPGme, die wird aber nicht von allen Programmen genutzt.

Beim Kommandozeilentool gibt es genau das problematische Verhalten im Zusammenhang mit MDCs, das zu Sicherheitslücken führt: Bei einem fehlenden MDC oder einem Paket ohne MDC-Schutz wird trotzdem der entschlüsselte Plaintext ausgegeben. Anschließend erscheint eine Fehlermeldung.

Die Kritik daran: Dieses Interface lädt geradezu dazu ein, es unsicher zu implementieren. Ein Mailclient, der GPG aufruft, muss im Fall einer Fehlermeldung den Plaintext verwenden und darf ihn nicht anzeigen.

Die GnuPG-Entwickler halten dieses Interface für notwendig, um das Streamen von Daten zu ermöglichen. So kann etwa eine mehrere Gigabyte große Datei mit GPG entschlüsselt werden - den Inhalt zu puffern und erst nach korrektem MDC-Check auszugeben, ist nicht machbar.

Dieses Problem ließe sich lösen, wenn man große Nachrichten in mehrere Teile aufspaltet, die einzeln geschützt werden. Doch dafür müsste man wiederum den Standard ändern, mit dem bestehenden OpenPGP-Datenformat ist das nicht machbar.

Reicht es, externe Inhalte zu blockieren?

Die simpelsten Efail-Angriffe basieren darauf, in HTML-Mails externe Inhalte nachzuladen, etwa indem ein Bild vom Server des Angreifers geladen und die verschlüsselte Mail an den Request angehängt wird. Ob das Nachladen von Inhalten erlaubt ist, hängt vom E-Mail-Client und von den Einstellungen ab. In Thunderbird und Outlook ist das Laden externer Inhalte standardmäßig deaktiviert, in Apple Mail ist es standardmäßig aktiv.

Doch es gibt andere denkbare Szenarien. Wir hatten bereits darüber berichtet, dass man den verschlüsselten Mailinhalt in einem HTML-Formular platzieren und dann an den Angreifer schicken kann. Ebenso denkbar sind jedoch Angriffe mit völlig anderen Datenformaten. So ließe sich auch eine PDF konstruieren, die externe Inhalte nachlädt.

Trotzdem ist klar: Es ist generell eine gute Idee, das Nachladen von Inhalten in E-Mails zu unterbinden - völlig unabhängig vom Efail-Angriff. Schon alleine aus Datenschutzsicht ist es problematisch, da beispielsweise Tracking-Pixel in E-Mails Informationen über den Empfänger preisgeben können.

Reicht es, HTML-Mails abzuschalten?

Nein, solange die grundlegenden Probleme mit modifizierbaren Nachrichten nicht behoben sind, hilft

das Abschalten von HTML-Mails nur teilweise. Wie oben bereits erwähnt ist es möglich, auch mittels PDF-Dokumenten oder anderen Dokumentformaten eine Nachrichtenexfiltration zu konstruieren.

Allerdings gilt tatsächlich, dass ein Großteil der Angriffe auf HTML-Mails basiert. Wenn HTML-Mails deaktiviert sind und OpenPGP so implementiert ist, dass es nur Nachrichten mit korrektem MDC anzeigt, werden alle bisher bekannten Angriffsszenarien verhindert.

HTML-Mails und Sicherheit - passt das überhaupt zusammen?

Die Darstellung von HTML in E-Mails führt zu einer Reihe von Sicherheitsproblemen, völlig unabhängig von E-Fail. So werden beispielsweise immer wieder Cross-Site-Scripting-Lücken in Webmail-Interfaces gefunden.

Die Grundlagen von HTML-Mails sind in RFC 2110 definiert. Dieser Standard wurde bereits 1997 verabschiedet. Er enthält zwar einen Abschnitt über Sicherheit, doch der ist relativ kurz. Dass die Ausführung von Script-Code in HTML-Mails gefährlich ist, darauf wird verwiesen. Doch ob etwa Formulare in HTML-Mails zugelassen sein sollen oder wie Mailteile voneinander abgetrennt werden - dazu schweigt der Standard.

Ein grundsätzliches Problem ist daher, dass es für HTML-Mails kein durchdachtes Sicherheitskonzept gibt. Bislang versucht jeder Mailclient für sich, bekannte Sicherheitsprobleme zu verhindern.

Warum empfiehlt die Electronic Frontier Foundation (EFF) die Deinstallation von Mailverschlüsselung? Ist eine angreifbare Mailverschlüsselung nicht besser als gar keine?

Die Empfehlung der EFF hat zwei Hintergründe: Zum einen standen zum Zeitpunkt der Efail-Veröffentlichung keine Patches bereit, um die Probleme zu beheben. Zum anderen ermöglicht Efail das Entschlüsseln von Nachrichten aus der Vergangenheit. Wer also vor allem Wert darauf legt, seine Nachrichten aus der Vergangenheit zu schützen, der steht tatsächlich am besten da, wenn er vorläufig alle Mailverschlüsselungs-Funktionen deaktiviert.

Man muss die Einschätzung der EFF nicht teilen, aber es erscheint angesichts der Sachlage zumindest nachvollziehbar, wie es zu dieser Empfehlung kam. Es wäre sicher anders gelaufen, wenn von den beteiligten Softwareprojekten rechtzeitig entsprechende Updates bereitgestellt worden wären. (hab)

Verwandte Artikel:
PGP/SMIME: Thunderbird-Update notwendig, um E-Fail zu verhindern
(19.05.2018, https://glm.io/134472)
PGP/SMIME: Angreifer können sich entschlüsselte E-Mails schicken lassen
(14.05.2018, https://glm.io/134370)
E-Mail-Verschlüsselung: PGP und S/MIME abschalten
(14.05.2018, https://glm.io/134359)
E-Mail-Verschlüsselung: EU-Kommission hat Angst vor verschlüsseltem Spam
(22.06.2016, https://glm.io/121638)
Microsoft: Viel Neues rund um den Kalender und die App von Outlook
(02.05.2018, https://glm.io/134170)
