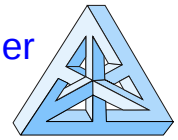
DresPleierCrypt Anwendung

Sinnvolle Tipps zur komfortablen Nutzung zur Datenübertragung

DresPleier GmbH



DresPleier GmbH, 84149 Velden, Deutschland

Im vorherigen Artikel[1] wurde DresPleierCrypt vorgestellt, das von der DresPleier GmbH entwickelte neuartige Verfahren zur superstarken symmetrischen Verschlüsselung mit Schlüsseln mit Längen mit 5000 Bits und mehr. Dieser Artikel beleuchtet ergänzend Aspekte bzw. Ideen zur Anwendung.

Installation

Zunächst muss man DresPleierCrypt zum Laufen bringen. **Für Linux-Systeme** bietet sich die Erklärung für Debian-Linux an, da dieses die Basis von vielen Linux-Derivaten ist. Eine Vorgehensweise ist wie folgt im Terminal: (1) GNU C-Compiler installieren, sofern nötig, z.B. sudo apt-get install gcc. (2) Den Anhang aus dem Artikel[1] in eine Datei kopieren, z.B. DresPleierCrypt.c, PDF-Zusatzinformationen entfernen, (3) übersetzen mit gcc -o dpc DresPleierCrypt.c und (4) Testen mit ./dpc, was zur Ausgabe der Basisdaten, einer Fehlermeldung und Usage-Informationen führt.

Für "Apfel"-Systeme bietet sich die Vorstellung für ein "Apfel"-Book an: Eine mögliche Herangehensweise ist wie folgt im Terminal (oder iterm): (1) Zur Installation von Applikationen brew installieren z.B. mit /usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)", dann (2) durchführen brew update ; brew upgrade ; brew gcc. Danach (3) den Anhang aus dem Artikel in eine Datei kopieren, PDF-Zusatzinformationen entfernen und (4) diese übersetzen mit gcc -o dpc DresPleierCrypt.c.

Mail als Transportmechanismus

Heutzutage werden Mail-Systeme zum Übertragen von Mails verwendet und zusätzlich für andere Zwecke genutzt wie das Vereinbaren von Terminen basierend auf Mails oder das Speichern von Kommunikation als Mails, zudem Programmerweiterungen[2] eingesetzt, um Funktionalitäten wie Verschlüsselung zu integrieren. Dies bietet mehr Funktionen und Bequemlichkeit, verkompliziert jedoch die Mail-Nutzung: Bei einem Wechsel der Mail-Anwendung kann eventuell nicht mehr auf die gespeicherten Daten zugegriffen werden, verschlüsselte Mails, intern oder extern gespeichert können eventuell nicht durchsucht oder gelesen werden, eine Abhängigkeit von der Verfügbarkeit von den Erweiterungen kann entstehen und diese bergen das Risiko verborgener unerwünschter Funktionen, was sicherheitskritisch sein kann. Eine solche Integration würde DresPleierCrypt unnötig verkomplizieren, da hierzu Mail-Client-spezifische Ergänzungen erstellt werden müssten, was in der Regel ein tiefgehendes KnowHow und ein ständiges Anpassen an die Client-Entwicklung bedingen. Solche Erweiterungen wären nicht ohne Weiteres von Jedermann / Jedefrau prüfbar und Abhängigkeiten könnten entstehen.

Es bietet sich daher der Einsatz des KISS-Prinzips, des Prinzips der Einfachheit an: Man nutzt Mail bzw. das Mail-System wieder in seiner ursprünglichen Intension als Medium zur Übertragung von Informationen (Text mit oder ohne Anhänge), also als Transportmechanismus. Erweiterte Funktionalitäten wie Verschlüsselung realisiert man außerhalb. Dies ist eine grundsätzliche Anwendungsentscheidung zur Art der Nutzung, die Benutzer oder Verantwortliche treffen müssen, wofür oder wogegen man sich aussprechen kann. Für die Intension von DresPleierCrypt bietet sich dies an, um Programmerweiterungen zu vermeiden und die Nutzung möglichst klar und einfach zu halten.

Nutzung mit DresPleierCrypt

Für die konkrete Anwendung bedeutet das: Man nimmt ein Verzeichnis, z.B. Kommunikation/2019, speichert dort seine Kommunikation ab, egal ob Briefe, Fax, Mails, sinnvollerweise mit nach Datum

1 DresPleier GmbH: DresPleierCrypt - Superstarke symmetrische Verschlüsselung sicher nutzen; www.DresPleier.de

2 PlugIns, AddOns

sortierbaren "sprechenden" Dateinamen wie 2019-08-31. Brief_an_XY_Angebot.pdf. Der Sender erstellt eine Datei in einem beliebigen Format (Textdatei, PDF oder gebündelt als tar.gz oder zip o.ä.), verschlüsselt diese mittels DresPleierCrypt, gegebenenfalls einem weiteren Verfahren, und versendet das Ergebnis als Mail-Anhang - hier gilt es aufzupassen, die richtige, also geschützte Datei zu verwenden. Der Empfänger bekommt diese Datei, speichert und entschlüsselt sie, zunächst das weitere Verfahren, dann DresPleierCrypt. Die Datei muss zur Mail-Übertragung geeignet kodiert werden, die base64-Kodierung als Teil der MIME-Spezifikation bietet sich hierzu an, entweder eingebunden in das weitere Verfahren (z.B. gpg --armor) oder explizit kodiert, z.B. via Kommando base64[3]. Die Logik ist also identisch wie die Nutzung von Fax, wo man Schriftstücke erstellt und Telefax als Übertragungsmechanismus nutzt. Der übertragene Dateiname kann zum Verbergen umbenannt werden, da seit DresPleierCrypt v0.99 der Originaldateiname geschützt mit übertragen und wiederhergestellt wird.

Diese Lösung ist leichtgewichtig, allgemein bzw. breit nutzbar und sehr zukunftssicher: Sender und Empfänger speichern die Informationen in einem Dateisystem, für einfachen Zugriff unverschlüsselt oder verschlüsselt, falls die Datei bzw. Inhalte besonders schützenswert sind. Man benötigt keine speziellen Erweiterungen, die man nachinstallieren oder updaten muss. Und man hält die Verschlüsselungssoftware möglichst "sauber", selbst übersetzt und direkt genutzt.

Schlüsselhandhabung mittels Standard-Keyfile und Scripte

Um die Schlüssel einfacher handhaben zu können, läßt sich bei Abwägung Sicherheit versus Komfort eine Schlüsseldatei einführen, z.B. ein großes Video, in das man alle Schlüssel packt bzw. dort versteckt. Dieses ist dann das "Standard-Keyfile", das man wie gehabt bestmöglich und mitnehmbar versteckt (also z.B. auf einen USB-Stick bei vielen anderen Dateien). Man kann die Schlüsseldatei regelmäßig eingeben. Alternativ baut man sich ein Script, um den Zugriff zu vereinfachen, da hier die Pfade von keyfile und Verschlüsselungsprogramm, gegebenenfalls weitere wie ein Editor, falls automatisch gestartet, hinterlegt sind:

```
#!/bin/bash
#dpce_file / encrypt a file using DresPleierCrypt and Twofish

prog=dpce_file
dpc=/media/dp/usbstick/dpc/dpc
keyfile=/media/dp/ustick/videos/holidays/2019/dolphin37.mpeg

echo $prog: encrypt a file using DresPleierCrypt and Twofish

echo ===== 1. enter DresPleierCrypt keyfile offset for recipient\(s\)
echo encrypting using your standard keyfile, please enter offset:
read offset
$dpc encrypt $1 $1.dpc $keyfile $offset
echo ok

echo ===== 2. enter gpg-twofish passphrase for recipient\(s\)
echo encrypting $1.dpc using gpg --symmetric using Twofish...
gpg --symmetric --cipher-algo TWOFISH --armor --output $1.dpc.2f < $1.dpc
result=$1.dpc.2f
echo ok

echo ===== 3. resulting file for transfer is:
echo $result

echo all done. Hit any key to close window
read waiting
```

Das Script speichert man mitnehmbar auf dem USB-Stick im Verzeichnis dpc. Und man kann dieses ausbauen, um mehr Komfort zu erlangen: z.B. automatisches Erstellen einer Textdatei mit Mail-Signature und Öffnen eines Editors oder automatisches Bündeln mehrerer Dateien oder eines

3 Binary2Ascii base64 < Binärdatei > Textdatei; Ascii2Binary base64 -d < Textdatei > Binärdatei

Verzeichnisses usw. Je mehr Funktionalitäten man integriert, desto eher erfolgt jedoch eventuell eine Fehlbedienung, was beim Einsatz von Verschlüsselung vermieden werden sollte. Deshalb ist eine möglichst einfache Funktionalität und Handhabung fehlerresistenter und empfehlenswerter, ideal also "nur" die Verschlüsselung einer Datei.

Die Scripte kann man in den Dateimanager integrieren, z.B. auf Debian-Linux mit XFCE-Desktop als "Benutzerdefinierte Aktionen", so daß ein Rechts-Klick auf eine Datei mit "DresPleierCrypt Encrypt File" das Script zum Verschlüsseln mit der selektierten Datei in einem Terminal startet und den Nutzer durch Ausgaben wizard-artig durch das Script führt.

Fazit

Verschlüsselung kann einfacher oder komplizierter genutzt werden. Aus Gründen der Einfachheit, allgemeinen Nutzbarkeit und Zukunftssicherheit bietet es sich an, diese ohne Zusatzsoftware wie Erweiterungen von Mail-Clients zu nutzen, sondern auf eine basis-orientierte Speicherung im Dateisystem zu setzen und Mail in seiner ursprünglichen, reinen Form als Transportmedium einzusetzen. Die Schlüsselhandhabung kann durch Scripte mit Integration in die Dateiverwaltungssoftware und einem Standard-Keyfile vereinfacht werden. Dies hält das Grundkonzept von DresPleierCrypt aufrecht, daß Jedermann und Jedefrau die Software selbst prüfen, übersetzen und anwenden kann.

DresPleier GmbH ; Vils 8 ; 84149 Velden ; Deutschland

Telefon: 08742 / 5870 894 ; Telefax: 03222 / 4170 655 ; Mail: info@DresPleier.de
Vertrauliche Kommunikation via OpenPGP-Verschlüsselung:
Kennung: DresPleier GmbH info@DresPleier.de
Fingerabdruck: 1F54 3062 37A7 9BEC A15A 111C 7F15 55F9 0130 E3E3

Webpräsenz: www.DresPleier.de

Weitere Informationen, Angebote, Seminare, Termine, Videos siehe www.DresPleier.de

Feedback ist gerne willkommen an info@DresPleier.de

Erstveröffentlichung 2019-09-09, Überarbeitung 2019-09-12 und 2019-11-30.