Seminar Kryptographie & Zugriffskontrolle

Dozent: Roy Meissner roy.meissner@uni-leipzig.de

Challenge

Senden Sie mir eine verschlüsselte und signierte Nachricht an eine meiner E-Mail Adressen

- Was brauchen Sie, um mir eine verschlüsselte Nachricht zu senden?
- Was brauchen Sie, um diese Nachricht signieren zu können?
- Was brauche ich, damit ich Ihre Signatur überprüfen kann?
- Nutzen Sie Ihren nativen Client (bspw. Thunderbird) oder das Browser-Plugin Mailvelope zum Versand - https://mailvelope.com/de
- Warum empfehle ich Mailvelope?

- Mein Mail-Programm soll automatisch prüfen können, ob die Signatur korrekt ist!

Verschlüsselte E-Mail

-----BEGIN PGP MESSAGE-----
Version: OpenPGP.js v4.10.10
Comment: https://openpgpjs.org

wV4DfDP4sVLayAASAQdA4dXDyPxOZnC02Qtx3ItC8sOKNMpo2OF1nyXARsaj
Tm0w12Wu2x44bUCh9r9sQVtkLSIrh89DvJQ5E433yCxR++tv3l2tT8EtkMh4
6I2MbeGA0qEBcAhIkBhEituDNnYNzcE5g+2fP+6xQvhRSBrO2EVfghiEW9f2
J/45ae+lqA5XQfgEwPmnDO42RoGLiixH5wEx4f6cdJ/P1D/RzzpeP3SKGWWp
t/SJdvi+PKoNmYQnc9rQmauCTTvBK+MYdDPdkggvPSYJH8XROb5VJeA290TW
bskCpQzlR+98BEsuqShW2D5GkZigEfzCV6YsIOOhEsmByw==
=dnk/
-----END PGP MESSAGE-----

Warum kann ich diesen Text einfach hier abbilden?

Vorbereitung

- Verbinden Sie sich zu einer Linux-Distribution, bspw. per:

docker run -it --rm -v ./:/mountedVolume/ ubuntu:22.04

- Installieren Sie GnuPG & sudo

apt update && apt install -y gnupg sudo && gpg --version

- Erstellen Sie sich einen neuen Nutzer

adduser bob
usermod -aG sudo bob

- Loggen Sie sich als dieser ein

login test

Asymmetrische Verschlüsselung

OpenPGP (Pretty Good Privacy 1/2) via GnuPG

- Generieren Sie eine Schlüssel-Paar

gpg --full-generate-key

- Exportieren Sie Ihren Public Key

gpg --export --armor E-MAIL > pubkey.asc

- Geben Sie den Public Key Ihrem Sitznachbarn (bspw. per Chat, Mail, …)

- Importieren Sie den eben erhaltenen Public-Key

gpg --import alicepubkey.asc

OpenPGP (2/2) via GnuPG

- Verschlüsseln Sie eine Nachricht an Alice

gpg --encrypt --recipient EMAIL FILE

- Signieren Sie die verschlüsselte Nachricht

gpg --output message.sig --sign FILE.gpg

- Senden Sie Signatur und verschlüsselte Nachricht an Ihren Sitznachbarn

- Verifizieren Sie die Signatur der erhaltenen Nachricht

gpg --decrypt message.sig

- Was sehen Sie?
- Entschlüsseln Sie die an Sie verschlüsselte Nachricht

gpg --decrypt message.gpg

- Versuchen Sie selbst die an Alice verschlüsselte Nachricht zu entschlüsseln

Diskussion

- Worin besteht die Hürde bei dieser Art der Ver-/Entschlüsselung?
- Wie könnten Sie diese Hürde lösen?

- E-Mail Programme kapseln viele der manuellen Schritte. Warum wird E-Mail Verschlüsselung nicht breiter eingesetzt?

- Beschreiben Sie einen validen Angriff auf die eben erfolgte Kommunikation

Diskussion

- Verfahren, zum veröffentlichen von öffentlichen Schlüsseln:
    1. Keyserver, auf dem Sie Ihren Schlüssel hochladen
        - Problem: Gehört der öffentliche Schlüssel wirklich Ihnen?
    2. Wie 1., aber mit E-Mail Verifikation
    3. Ergänzung am bspw. DNS-Eintrag bei Ihrem E-Mail Anbieter
        - Nicht bei allen möglich, Schlüssel müssen Vorgaben erfüllen, bspw bei Posteo:
            - Leeres Namensfeld
            - Kein Kommentar
            - Schlüssel muss Ihre E-Mail Adresse beinhalten (exakt eine)
        - Warum diese Vorgaben?

Symmetrische Verschlüsselung

OpenPGP via GnuPG

- Verschlüsseln Sie eine Nachricht an Alice

gpg -o filename --symmetric --cipher-algo AES256 file.txt

- Senden Sie die verschlüsselte Nachricht an Ihren Sitznachbarn
- Tauschen Sie das Passwort mit Ihrem Sitznachbarn aus

- Entschlüsseln Sie die erhaltene Nachricht

gpg -o original_file.txt -d file.txt.gpg

- Wo besteht das Problem?
- Können Sie verschlüsselte Nachricht auch signieren? Wenn ja, was bringt das?

Diskussion

- Möglichkeiten zur Übertragung eines Schlüssels
  - Treffen & per Zettel
  - Merkles Puzzle – recherchieren Sie!
  - Asymmetrische Verschlüsselung
  - Weitere?
- Welche Nachteile haben die Verfahren bisher?
- Möglichkeiten zur Generierung eines Schlüssels
  - Diffie-Hellman-Verfahren – Mathematischer Teil der Vorlesung
    - Nicht sicher, wenn Angreifer Nachrichten verändern kann
- Recherchieren sie Forward-Secrecy

Zugriffskontrolle

File-Permission & Owner

• Sehen Sie sich ihr Home-Verzeichnis an

ls -lsa

- Analysieren Sie die Ausgabe
- Ändern Sie Rechte einer Datei per chmod, bspw

chmod o-w FILE

- Ändern Sie den Owner der Datei per chown, bspw

chown root FILE

- Können Sie weiter auf das File zugreifen?

- Ist das gesehene eine Access Control List?

Gruppen

• Listen Sie sich alle aktuell existierenden Gruppen auf

cat /etc/groups

- Finden Sie Ihren Nutzer darin
- Wie müsste validiert werden, ob ein Nutzer Zugriff auf eine Datei per Gruppe hat?
- Welcher Form der Access-Control entspricht dies?

- Ändern Sie die Gruppe einer Datei

chown root:root FILE

- Können Sie weiter auf das File zugreifen?

Nachtrag Challenge

Nutzen Sie diesen KeyServer https://keys.openpgp.org/