

# Module

- Rollenspiel-Netzwerkverkehr
- Keepass-As-Group

# Rollenspiel-Netzwerkverkehr

Dieses Spiel soll versuchen Menschen den Ablauf, nicht aber die Funktionsweise von Netzwerkkommunikation am Beispiel von E-Mails ohne Verschlüsselung, mit Transportverschlüsselung und mit Ende-zu-Ende (und Transportverschlüsselung) zu veranschaulichen. Dabei ist es weniger wirklich ein Spiel, dass Spaß machen soll, sondern dient als eher Mittel dazu das Thema nicht nur mit einem Netzwerkdiagramm erklären zu müssen und somit für nicht-Nerds zugänglicher zu machen.

## Rollen

- 2x Server (systemli.org & gmail.com)
- 2x Kommunikationsparteien (Alice & Bob)
- 1x (oder mehr) Polizei (Eve)
- 3x Internet [Optional]

## Material

- 1x Blatt für Text
- 1x Blatt mit E-Mail Metadaten
- 3x Blatt mit IP-Metadaten für die Strecken zwischen den Knoten
- 2x Schild mit Namen der Server
- 2x Schild mit E-Mail und IP-Adresse der Kommunikationsparteien
- 1x kleine Kiste, welche mit Vorhängeschloss verschlossen werden kann (in welche das Blatt mit dem Text passt)
- 3x große Kiste mit Deckel (in welche die andere Kiste passt)
- 2x Vorhängeschloss
- 3x Stuhl
- Stifte

Im Idealfall werden die Blätter laminiert und mit Whiteboardmarker beschrieben. Dann können sie auch wiederverwendet werden.

## Ablauf

Zur Vorbereitung wird auf jede der großen Kisten einer der Internet Metadaten geklebt.

Dann werden die Rollen verteilt. Die Rolle der Polizei sollte am besten ein Mensch ohne großes technisches Wissen übernehmen, sodass für die Angriffe Kreativität gefragt ist. Die restliche Menschen schauen zu.

Die 2 Server und 2 Kommunikationsparteien stellen sich in einem Viereck auf. Die Server und Kommunikationsparteien bekommen die Schilder mit ihren Informationen umgehängt.

Zwischen die 4 Menschen wird jeweils 1 Stuhl gestellt auf den sich jeweils eine Person die das Internet spielt setzt. Zudem bekommen sie die Kiste mit den passenden Internet Metadaten.

Alice schreibt auf das Blatt für den Text eine Nachricht an Bob und auf das Blatt mit den Metadaten die nicht bereits ausgefüllten Metadaten.

Nun werden die verschiedenen Szenarien durchgespielt. Jedes Szenario wird einmal ohne MITM, einmal mit MITM (in unserem Fall durch die Polizei) gezeigt. Dabei ist die Rolle der Polizei angehalten, sich selbst auszudenken wie sie das Szenario angreifen kann. Ausgenommen werden lediglich Angriffe auf Alice und Bob welche nicht Ziel dieses Spiels sind. Zudem wird nicht behandelt inwiefern die Angriffe rechtlich möglich sind oder die Parteien die Daten an Behörden herausgeben würden, alle technisch möglichen Angriffe können behandelt werden. Die Polizei kann nur beim Internet und bei den Servern angreifen.

Wenn der Polizei selbst keine Angriffsmöglichkeit einfällt können die Zuschauenden aushelfen. Wenn auch diese keine Idee haben, kann die Moderation aushelfen.

Anschließend sollen die Zuschauenden erklären was passiert ist, ob der Angriff so funktioniert und welche Daten die Polizei bekommen hat.

## Unverschlüsselt

Anna gibt Internet die Blätter mit dem Text und den E-Mail Metadaten, gibt sie dem ersten Server, welcher sie wieder an das Internet gibt, der es zum zweiten Server bringt, der sie erneut dem Internet gibt welches die Blätter schließlich zu Bob bringt. Bei jedem Knoten werden die Blätter in die Kiste mit den entsprechenden IP Metadaten gelegt.

### Unverschlüsselt – MITM

Mögliche Angriffsziele sind:

- Das Internet
- Die Server

Bei beiden können alle Daten abgegriffen werden.

## Transportverschlüsselt

Diesmal werden die Kisten mit dem Deckel "verschlossen". Diese Kiste wird in dem Spiel zwar nicht verschlossen, jedoch wird darauf hingewiesen, dass sie trotzdem als sicher zu betrachten ist. Sie schützen allerdings nur auf dem Transportweg, die Knoten müssen die entsprechenden Kisten ja öffnen können.

Ansonsten läuft es wie beim unverschlüsselten Szenario. Es ist darauf zu achten, dass an jedem Knoten beide Blätter aus der Kiste geholt und anschließend in die passende andere Kiste hinein gepackt werden. Dies ist notwendig, da die Server ja die Metadaten brauchen um zu wissen, wohin sie die Mail weiterleiten müssen.

## Transportverschlüsselt – MITM

Mögliche Angriffsziele sind:

- Die Server

Dort können alle Daten abgegriffen werden.

## Ende-zu-Ende-Verschlüsselung

Zuerst wird erklärt, dass es bei Ende-zu-Ende Verschlüsselung einen öffentlichen und einen privaten Schlüssel gibt. Wir stellen denn öffentlichen Schlüssel als Vorhängeschloss und den privaten als Schlüssel für das Schloss dar. Es wird kurz darauf hingewiesen, dass dieser öffentliche Schlüssel so ausgetauscht werden muss, dass sicher ist, dass dieser auch zu der Person gehört. Für dieses Szenario machen wir das so, dass Bob persönlich zu Alice geht und ihr das Vorhängeschloss gibt.

Nun packt Alice den Zettel mit dem Text in die kleine Kiste, verschließt diese mit dem Vorhängeschloss und packt diese Kiste zusammen mit dem Blatt mit den Metadaten in die große Kiste. und übergibt diese an das Internet. Danach ist der Ablauf wie vorher, die große Kiste wird an jedem Knoten wieder ein und ausgepackt, bei Bob wird schließlich auch die kleine Kiste geöffnet.

## Ende-zu-Ende-Verschlüsselung – MITM

Mögliche Angriffsziele sind:

- Die Server

Dort können nun nur die Metadaten abgegriffen werden.

## Ende-zu-Ende-Verschlüsselung mit TOFU

Diesmal wird der öffentliche Schlüssel, wie so üblich per E-Mail ausgetauscht ohne dass dieser überprüft wird.

1. Alice schreibt Bob "gib mal Key"
2. Bob schickt Key
3. Alice schreibt Ende-zu-Ende verschlüsselt wie oben

## Ende-zu-Ende-Verschlüsselung mit TOFU – MITM

Mögliche Angriffsziele sind:

- Die Server

Dort können alle Daten abgegriffen werden.

Der Angriff läuft wie folgt ab:

1. Alice schreibt Bob "gib mal key"
2. Bob schickt Alice Key
3. Polizei greift den Key ab, ersetzt ihn durch eigenen.
4. Alice verschlüsselt Nachricht mit Key der Polizei
5. Polizei fängt die Nachricht ab und liest sie.
6. Polizei verschlüsselt Nachricht neu mit eigentlichem Schlüssel von Bob und sendet sie weiter

So bekommen weder Alice noch Bob etwas von dem Angriff mit die Polizei kann jedoch alles mitlesen. Durch den Austausch des Keys durch die Polizei wird hier ein zweites Vorhängeschloss benötigt.

# Keepass-As-Group

KeePassXC ist eigentlich keine Cloud-Software und deshalb so beliebt, weil dabei alle Passwörter den eigenen Rechner nicht verlassen. Um als Gruppe verschiedene Zugänge zu verwalten, ist das aber unpraktisch. Dann müsste bei jeder Änderung in der Datenbank (*neues Passwort hinzugefügt, Passwort geändert, usw.*) jedes Mal jedem einzeln die Änderungen mitgeteilt werden, damit alle bei sich lokal diese Änderungen übernehmen.

Neben Cloud-basierten Passwortmanagern, wie z.B. Bitwarden, können wir aber auch eine KeePassXC-Datenbank zu uns auf den Rechner synchronisieren und wie gewohnt ohne Browser mit KeePassXC öffnen und bearbeiten.

Voraussetzung dafür sind eingerichtete Nextcloud-Gruppen und Geräte Synchronisation.

Nach der erfolgreichen Installation und Einrichtung sollten wir unsere Persönlichen Cloud Dateien alle auf dem Rechner direkt zugänglich haben.

## Passwortdatenbank (und andere Dateien) teilen

Jetzt wird die Gruppen-Passwort-Datenbank (*im Folgenden nur noch Datenbank genannt*) vom **Gruppen-Account** in die eigenen Dateien hochgeladen:

database upload

### Datei teilen

- Auf das **Teilen**-Icon klicken (*oder unter den drei Punkten auf **Details***):

database upload

- Im Suchfeld den Namen des Teams eingeben und Team auswählen (*evtl muss der Name ausgeschrieben werden*):

database upload

- Der Gruppe Bearbeitungsrechte geben (*sonst dürfen die Teammitglieder die Datei nicht bearbeiten*):

allow editing button

Hier sieht man jetzt, wer alles Zugriff auf diese Ressource hat:

sharing info of file

Darauf hin sollten alle Team-Mitglieder Zugriff auf diese Datenbank haben.

# Geteilte Datenbank öffnen

- Im KeePassXC kann in der Leiste ganz oben links Datenbank öffnen ausgewählt werden.

open database in KeePassXC

- In dem aufgegangenen Fenster wählen wir die geteilte Datenbank aus dem Cloud Ordner aus.

select database from file manager