[IN] Zusammenfassung 2023-04-06

Martin Merkli

30. März 2023

Inhaltsverzeichnis

1 Lernziele

- Alle bisher gelernten Techniken und Begriffe sind präsent.
- Die Prinzipien von Sicherheit sind Ihnen bekannt und Sie wissen, wo und wie diese angewendet werden.
- Asymmetrische und symmetrische Verschlüsselung ist Ihnen als abstraktes Konstrukt und konkret mit RSA und DES bekannt und sie*[sic!]* können die Mechanismen erklären. RSA können Sie – im Gegensatz zu DES – auch berechnen.
- Sie haben verstanden, wie eine Nachricht chiffriert und signiert wird, sowie die Dechiffrierung die Authentifizierung als Auflösung der Verfahren. Auch die Kombination der beiden ist Ihnen schematisch zumindest geläufig.
- Sie wissen, warum diese Verfahren notwendig sind, welche Schwierigkeiten sich technisch und in der Umsetzung stellen (wie wird die Sicherheit gewährleistet, wie wird sie untergraben).
- Sie kennen Möglichkeiten bei sich selbst und im Netz eine gewisse Sicherheit zu gewährleisten, je nachdem welche Sicherheit notwendig ist, z.B. mit Passwörtern, verschlüsselten Dokumenten und E-Mails.
- PGP (Vertrauensnetz und Zertifizierung) ist verstanden und kann erklärt werden.
- Sie haben verstanden wie Firewalls, Antivirussoftware und IDPs funktionieren und können die Funktionsweise bis zu einem gewissen Grad erklären (es ist*[sic!]* keine grössere Tiefe erwartet als im Vortrag geliefert).

2 RSA

2.1 Grundlagen

2.1.1 φ-Funktion

Die eulersche Phi-Funktion gibt für jede natürliche Zahl n an, wie viele zu n teilerfremde natürliche Zahlen existieren, welche nicht grösser als n sind.

Da eine Primzahl p nur durch 1 und sich selber teilbar ist, ist sie zu den Zahlen 1 bis $p-1$ teilerfremd. Weil sie grösser als 1 ist, ist sie ausserdem nicht zu selbst teilerfremd. Es gilt daher: $\varphi(p) = p - 1$.

Für eine natürliche Zahl n bestehend aus zwei Primfaktoren p und q gilt ausserdem: $\varphi(n) = (p-1)(q-1)$

2.1.2 Modulo-Funktion

Die Modulo-Funktion ist der Rest, der bei einer Ganzzahl-Division entsteht.

2.2 Schlüsselerzeugung

Zwei (sehr grosse) Primzahlen p und q werden ausgewählt. Dabei ist zu beachten, dass $p \neq q$. Je grösser die Primzahlen, desto langsamer ist die Berechnung der eulerschen Phi-Funktion ohne die Primfaktoren und desto sicherer ist der Schlüssel. Deshalb sind diese meistens über 300 Stellen lang.

Sei n das Produkt von p und q: $n = p * q$.

Eine (grosse) natürliche Zahl e wird so gewählt, dass diese zu $\varphi(n)$ teilerfremd ist. D.h. $ggT(e, \varphi(n)) = 1$. Als e sind Primzahlen sehr beliebt.

Die natürliche Zahl d wird als das kleinste multiplative Inverse von e modulo $\varphi(n)$ definiert. Die Formel dafür ist etwas kompliziert, weshalb wir eine andere Gleichung aufstellen und diese mit Durchprobieren lösen. Für $e * d = k * \varphi(n) + 1$ muss die kleinste Lösung mit $d, k \in \mathbb{N}$.

2.3 Öffentlicher Schlüssel

Die Zahlen e und n ergeben zusammen den öffentlichen Schlüssel. Er darf (für den Nachrichtenaustausch sogar muss), wie der Name schon verrät, für alle zugänglich sein.

2.4 Privater Schlüssel

Die Zahlen d und n ergeben zusammen den privaten Schlüssel. Er (eigentlich nur d) muss unbedingt geheim gehalten werden. Ohne diese Geheimhaltung ist das gesammte Verfahren unnötig.

2.5 Verschlüsseln

Sei m die Nachricht als natürliche Zahl und kleiner als n. Dann ist die verschlüsselte Nachricht $c = m^e \mod n$.

2.6 Entschlüsseln

$m = c^d \mod n$

2.7 Signieren

Sei h der Hash der Nachricht als natürliche Zahl und kleiner als n. Dann ist die Signatur $s = h^d \mod n$.

2.8 Authentifizieren

$h = s^e \mod n$

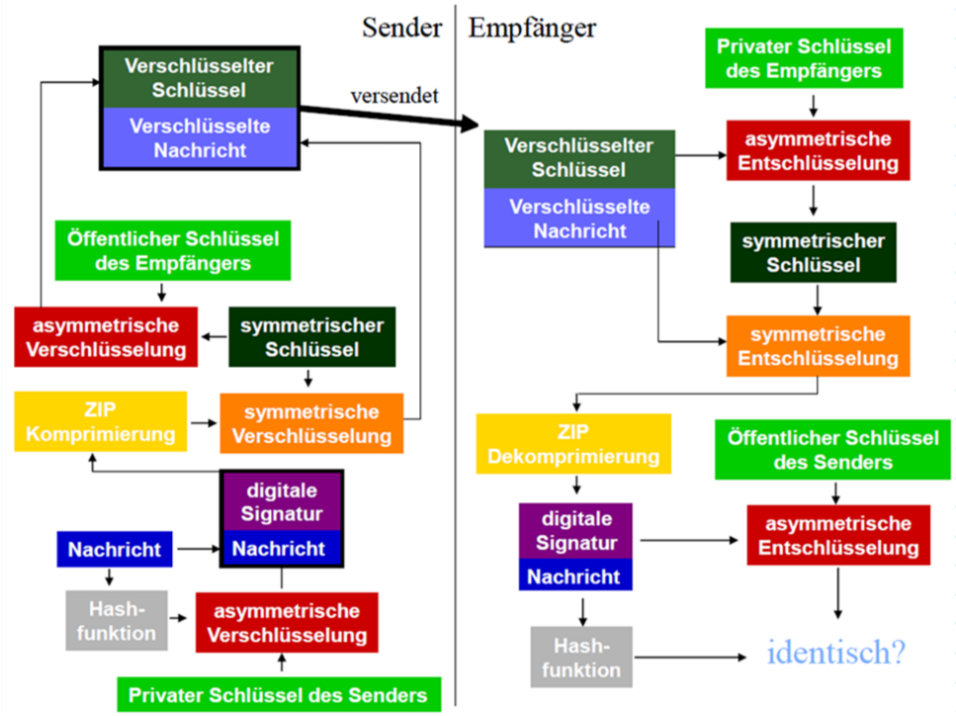
3 Hash

Eine Hash-Funktion (auch Einweg-Funktion genannt) ist wie ein Zufallszahlgenerator, nur mit zwei Unterschieden: Sie benötigt eine Eingabe und bei der gleichen Eingabe wird der gleiche Wert zurückgegeben. Die Ausgabe wird Hashwert oder auch Prüfsumme genannt.

4 PGP

4.1 Verschlüsselung

Das Rechnen mit asymmetrischen Schlüsseln verbraucht viel Rechenleistung. Ausserdem es Limitierungen der Nachrichtengrösse. Deshalb wird eine Mischung von as- und symmetrischen Verfahren angewendet. Des weiteren wird die Nachricht gleichzeitig signiert.



Dieses Prinzip schützt übrigens auch Ihre Verbindung mit `merkli.me`, wie am Schloss-Symbol in Ihrem Browser erkennbar ist.

4.2 Vertrauen

Es muss beim Beginn der Kommunikation sichergestellt werden, dass der Schlüssel auch wirklich der Person gehört, für die sie sich ausgibt. Dies kann zum Beispiel durch ein physisches Treffen sichergestellt werden.

4.3 Zertifizierung

Man kann einen Schlüssel zertifizieren, in dem man ihn mit RSA signiert. Dabei garantiert man anderen, dass man dem*der Schlüsselinhaber*in vertraut.

4.3.1 Vertrauensnetz

Durch mehrere Zertifizierungen entsteht langsam ein Vertrauensnetz. Das Vertrauensnetz beschreibt den Fakt, dass Person A Person C vertrauen kann, wenn Person A Person B und Person B Person C zertifiziert. Person A und Person C müssen sich also nicht mehr treffen.

4.4 Certification Authority

Eine Certification Authority (kurz CA) ist eine Dienstleistung, bei der Schlüssel signiert werden. Dadurch kann auch ohne viele physische Treffen und ohne grosses Vertrauensnetz die Richtigkeit der Schlüssel sichergestellt werden. Es müssen sich alle nur mit der CA treffen, deren öffentlichen Schlüssel erhalten und (nicht unbedingt) ihren eigenen Schlüssel signieren lassen.

5 (Wo/Hu)Man in the middle attack

Bei diesem Angriff auf die Kommunikation wird davon ausgegangen, dass eine Person X mit bösartigen Absichten die verschlüsselten Nachrichten abfangen und sogar abtauschen kann.

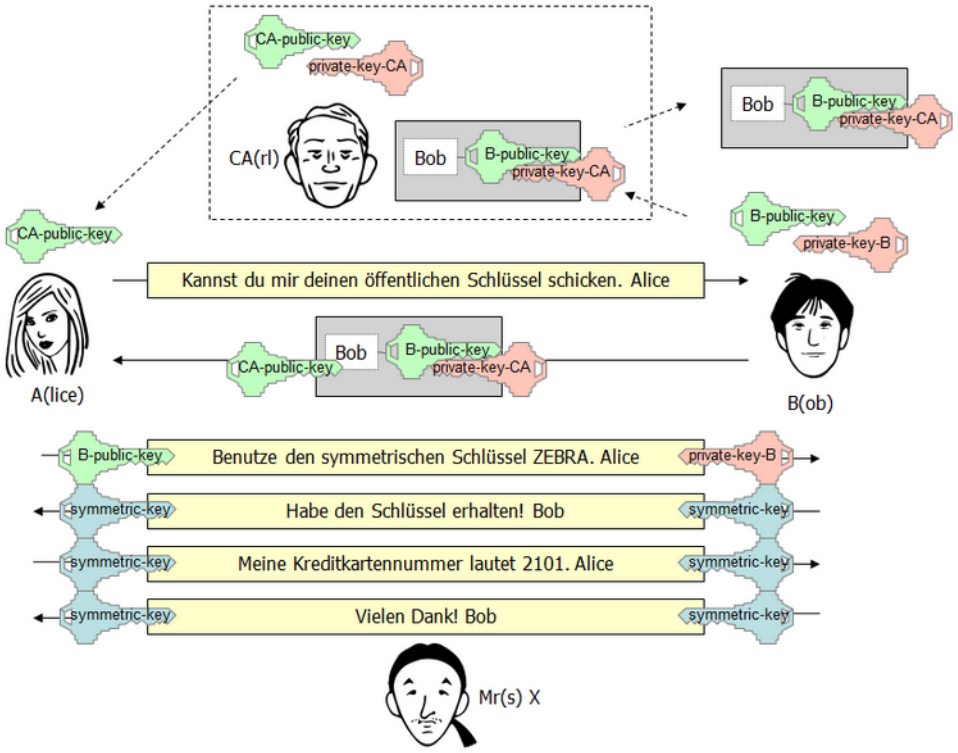
Falls beim Austausch von Schlüsseln keine Verschlüsselung angewendet wird, kann Person X den zurückgesendeten Schlüssel durch ihren eigenen austauschen. Damit sie die Nachrichten mitlesen kann und nicht auffliegt, entschlüsselt sie die Nachrichten und verschlüsselt sie wieder, diesmal mit dem richtigen Schlüssel.

Wenn eine CA nicht richtig benutzt wird, kann Person X erraten, wann ein Schlüssel angefragt wird. Diese Nachricht wird durch eine Anfrage für den Schlüssel von Person X ersetzt. Das Mitlesen der Kommunikation erfolgt gleich wie im vorherigen Beispiel.

5.1 Verteidigung

Person A möchte bei Person B einkaufen und muss deshalb ihre Kreditkartedaten übermitteln. Person B ist die Identität von Person A egal. Person B hat bei der CA ihr Schlüssel signieren lassen und Person A vertraut der CA. Person A fragt unverschlüsselt Person B nach ihrem öffentlichen Schlüssel. Dieser wird inklusive der Signatur der CA zurückgesendet. Person A generiert einen zufälligen Schlüssel und versendet diesem verschlüsselt an Person B. Ab dann wird dieser symmetrische Schlüssel verwendet. Person X hat

(falls keine der Personen dumm ist) keine Chance, irgendwelche Nachrichten ausser Anfragen für Schlüssel zu lesen. Sie könnte höchstens die Kommunikation unterbrechen.



6 Sicherheit als Grundprinzip

Es gibt verschiedene Wege, dieses Sicherheitsprinzip umzusetzen.

6.1 Vertraulichkeit

Daten können nicht von Dritten gelesen werden.

6.2 Integrität

Daten sind nicht unberechtigt manipuliert, weitergegeben oder gar verfälscht worden.

6.3 Authentizität

Es ist jederzeit klar, wem die Daten zugänglich sind und wer die Daten erstellt/verändert hat.

6.4 Verbindlichkeit

Im Nachhinein kann nicht bestritten werden, dass man die Daten verändert oder weitergegeben hat.

7 Firewall

Eine Firewall sperrt alles, was nicht richtig adressiert ist. Sie sieht passiv die Datenpakete an. Es gibt folgende Varianten:

7.1 Persönlich

Diese ist auf dem eigenen Computer installiert.

7.2 NAT

Diese sperrt zusätzlich allen Datenverkehr, welcher nicht vom Netzwerk angefordert wurde.

7.3 DMZ

Alle Geräte können nicht direkt auf das Internet zugreifen, sondern fragen die DMZ an, dies für sie zu erledigen.

8 Antivirussoftware

Eine Antivirussoftware sieht sich den Inhalt der Datenpakete an, nachdem diese entschlüsselt wurden. Jegliche Inhalte, welche verdächtig vorkommen, werden gelöscht oder zumindest unschädlich gemacht.

9 IDS

Ein Intrusion Detection System sucht aktiv nach Angreifer*innen. Sobald eine*r erkannt wird, wird die Adresse des*der Absender*in aufgeschrieben und zukünftige Anfragen direkt blockiert. Dafür wird häufig so getan, als ob es auf dem Computer oder im Netzwerk etwas spannendes zu entdecken gibt.

10 Sicherheitsprinzipien im Netz

10.1 Geringste Zugriffrechte

Es haben alle (Menschen und Computer) nur genau die Rechte, die sie gerade brauchen.

10.2 Verteidigung auf allen Ebenen

Redundante Sicherheitsmassnahmen existieren.

10.3 Kontrollpunkt

Es gibt genau einen Eingang, welcher sehr stark kontrolliert wird.

10.4 Schwächstes Glied

Das schwächste Glied in der Kette ist der unberechenbare Mensch.

10.5 Standardmässig verbieten

Alles wird verboten, eine Erlaubnis ist die Ausnahme.

10.6 "Alle an Bord"

Die Benutzer*innen werden zum Aufbau von Vertrauen und Verpflichtung eingebunden.

10.7 Einfachheit

Je einfacher ein System ist, desto offensichtlicher ist ein Fehler.