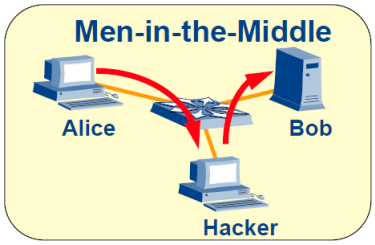
Netzwerke, Kapitel 3.8

Fragen 1

1. Welche Sicherheitslücken kann ein Netzwerk haben, welche Schäden können auftreten?
   - *Geheimhaltung verletzt (Daten Verlust/Diebstahl)*
   - *Technisch schlechte Konfiguration (default PWDs)*
   - *Störung des Betriebs / Sabotage (Denial-of-Service)*
   - *Verfälschung von Daten*
   - *Echtheit des Absenders gefälscht*
   - *Mitarbeiter als Sicherheitsrisiko*

   ⇨ *Mechanismen dagegen*
   - *Logische Massnahmen (Verschlüsslung)*
   - *Physische Sicherheit (grösser Zaun, Videoüberwachung)*
   - *Organisatorische Massnahmen (Mitarbeiter)*

2. Erklären Sie eine MITM-Attacke

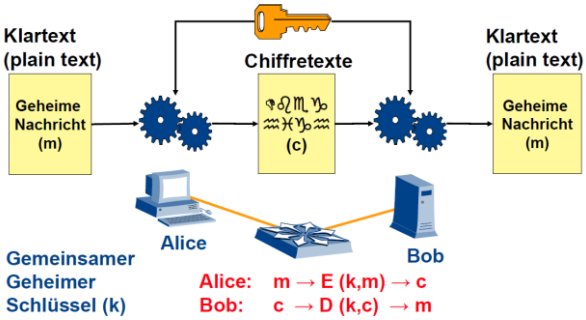


   - *Der Angreifer steht dabei entweder physikalisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern.*
   - *Der Angreifer hat komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.*
   - *Beispiel: Vortäuschen eines falschen WLAN Access Points bei öffentlichen WLAN Hotspots; Tools: Ettercap, Cain & Abele*
   - *Genmassnahme: Authentifizierungsprotokolle (z.B. Kerberos)*
   - ⇨ *Gegenmassnahmen: Starke Authentifikation in beide Richtungen*

3. Was ist der Unterschied zwischen einem Virus und einem Wurm?
   - *Virus: ein sich selbst vermehrendes Programm, infiziert ausführbare Dateien (oder Bootsektor, Makro), Verbreitung durch Weitergabe dieser infizierten Dateien*
   - *Wurm: Programm, das sich über Netzwerke verbreitet, und dafür eine Wirtsapplikation (z.B. E-Mail), Netzwerkdienste oder eine Benutzerinteraktion benötigt.*

4. Was ist sicherheitstechnisch die Schwachstelle bei der symmetrischen Verschlüsselung.

   Geheimer Schlüsselaustausch.

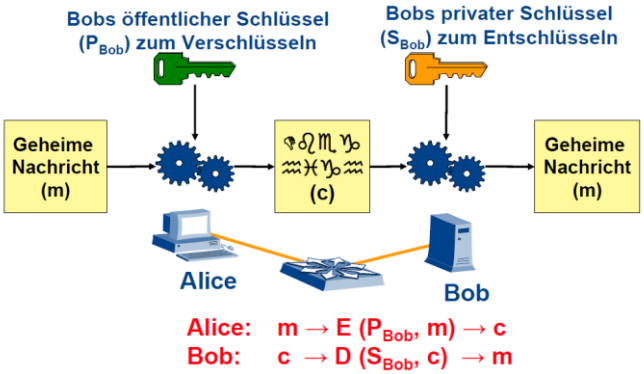


   *Anzahl Schlüssel: (n * (n -1)) / 2*

   *Anzahl Schlüssel: (Anz. Teilnehmer * Anz. Teilnehmer ohne mich) / 2*

   /2 weil der Retourweg den gleichen Schlüssel verwendet.

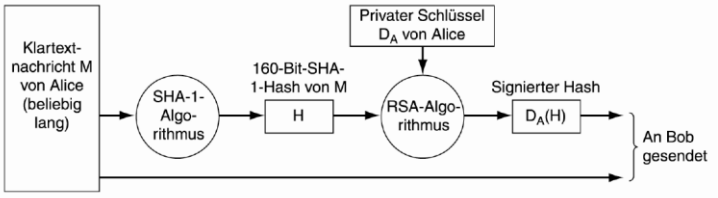
5. Bei der Public-Key-Verschlüsselung können auch mehrere Public-Keys (von verschiedenen Personen) benutz werden, um eine Datei zu verschlüsseln. Jede der Personen kann alleine mit ihrem jeweiligen privaten Schlüssel die Nachricht entschlüsseln. Was ist der Vorteil den diese Möglichkeit bietet?



Nur 1x verschlüsseln

Nur 1 Datei muss an alle verschickt werden.

6. Was ist der Vorteil eines Hash im Vergleich zu einer verschlüsselten Datei?



- Bob berechnet auch Hash-Wert H
- Bob entschlüsselt signierten Hash mit öffentlichem Schlüssel von Alice
- Falls beide H identisch, dann: Nachricht gültig

Aus den Daten werden mittels einer Funktion (mittels Key) einen Hash berechnet.

Der Hash ist kurz (z.B. 128/160Bit)

Authentifizierung sichergestellt – Nachricht ist nicht verschlüsselt!

7. Warum ist bei einer Firewall das Logging wichtig?

Zur Überprüfung der Einhaltung der Regel.