Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inform. Heiko Niedermayer
Dipl.-Inf. Ali Fessi

Übungen zur Vorlesung „Netzsicherheit“
Übungsblatt 3, WS09/10

Ausgabe:	Do 26. Nov. 2009
Abgabe:	Do 10. Dez. 2009
Besprechungstermin:	Do 17. Dez. 2009

Aufgabe 1: Kryptographische Hash-Funktionen – Grundlagen

a) Wie viele Bits soll eine ideale kryptographische Hash-Funktion als Ausgabewert haben, damit der Aufwand, eine Kollision zu finden, mit einem Brute-Force Angriff auf einer symmetrischen Blockschiffre mit 100 Bits Schlüssellänge vergleichbar wäre?
b) Welche Gefahr muss man beachten, wenn man SHA-1 für Digitale Signaturen verwendet möchte?
c) Die Berechnung eines Hash Wertes mit dem SHA-1-Algorithmus bei einem Textblock mit 512 Bits erfordert 80 Schritte. Nach wie vielen Schritten ist jedes Bit von der Eingabe in die Berechnung des Hashwertes mit eingeflossen?
d) Was ist bei SHA-1 der Wert W_{19} und wie lässt sich der Wert W_{19} berechnen?

Aufgabe 2: Authentisierungsprotokolle; das Needham-Schröder-Protokoll

a) In der Vorlesung wurde ein Replay-Angriff auf das Needham-Schröder-Protokoll (symmetrische Variante) beschrieben. Welche Voraussetzung muss bzgl. des „Session Keys“ $K_{A,B}$ erfüllt werden, damit dieser Angriff möglich wird.
b) Dieser Angriff wurde bei dem Kerberos-Protkoll behoben. Erweiten Sie das Needham-Schröder-Protokoll, so dass der Replay-Angriff verhindert wird.

Aufgabe 3: Authentisierungsprotokolle; Kerberos

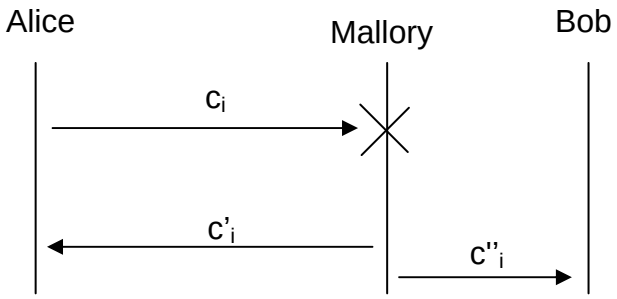
a) Schreiben Sie das Kerberos-Protokoll so um, dass es ohne Zeitstempel und daher auch ohne synchronisierte Uhren auskommt.
b) Begründen Sie, warum das Kerberos Protokoll die Eigenschaft der "`Forward Secrecy'" nicht erfüllt.
c) Erweitern Sie das Kerberos-Protokoll, so dass für die Kommunikation zwischen *Alice* und dem Service *S1* die „Forward Secrecy“-Eigenschaft erfüllt wird.
d) In wie weit werden die Möglichkeiten für einen Wörterbuch-Angriff bei Kerberos V5 im Vergleich zu V4 eingeschränkt?

Aufgabe 4: Angriffe auf (Un)sichere Kanäle

Angenommen, beim Entwurf eines Protokolls zur Absicherung der Kommunikation zwischen jeweils 2 Kommunikationspartner werden folgende Design-Entscheidungen getroffen:

- Für die Datenintegrität soll eine kryptographische Hash-Funktionen verwendet werden, nämlich SHA-1 und bei jeder Nachricht die ersten 96 Bits des Hash-Wertes anschließend an die Nachricht dran gehängt:
  (m , first-96-bits(H(m)))
- Diese Kombination aus Nachricht und Hashwert wird dann verschlüsselt. Für die Verschlüsselung soll ein gemeinsamer vorkonfigurierter 256-bit langer Schlüssel *K* verwendet werden.
- Für die Verschlüsselung nimmt man die Performance-Vorteile von AES im CTR-Mode in Anspruch und verwendet den Schlüssel *K* für die Berechnung der notwendigen „Key Streams". Um zusätzlichen Aufwand für den Schlüsselmanagement einzusparen, wird derselbe Schlüssel *K* in beide Richtungen eines Kommunikationskanals verwendet.
- Für die Generierung des „Key Streams" k_i für eine Nachricht werden jeweils die Sequenznummer *i* der jeweiligen Nachricht mit einem Counter *j* für jeden einzelnen Block dieser Nachricht zusammen konkateniert (*i* || *j*) und gemeinsam mit *K* als Eingabe für die AES-Block-Chiffre-Funktion verwendet. Die Sequenznummer *i* wird mit Null initialisiert und bei jeder neuen Nachricht um Eines erhöht. *j* wird bei jeder Nachricht mit Null initialisiert und bei jedem Block innerhalb dieser Nachricht um eins erhöht.
  k_i = E(i||0, K) || E(i||1, K) || E(i||2, K) || ….

a) Angenommen „Alice" und „Bob" benutzen das oben beschriebene Protokoll für ihre Kommunikation. Ein Angreifer „Mallory" fängt die verschlüsselten Nachrichten c_i von Alice ab und verhindert, dass sie bei Bob anzukommen. Angenommen „Mallory" kann zusätzlich bei manchen Nachrichten den Plaintext m_i raten. Begründen Sie, warum in diesem Fall:
   - „Mallory" eigene Nachrichten an Alice c'_i zurück schicken kann, so dass wenn Alice diese Nachrichten zu m'_i entschlüsselt nicht merkt, dass die Nachrichten nicht von Bob kommen.
   - „Mallory" sogar eigene Nachrichten c''_i an Bob verschicken kann, bei denen Bob nicht unterscheiden kann, ob sie von „Alice" oder von „Mallory" kommen.



b) Begründen Sie, warum der Entwurf dieses Protokolls einige Schwachstellen hat, und schlagen Sie Verbesserungen vor, um dieses Protokoll sicherer zu gestalten.