Netzsicherheit I, WS 2011
Übung 3

Prof. Dr. Jörg Schwenk

Betreuer: Florian Feldmann, Florian Giesen

Abgabe: Montag, 14. November 2011, 11:00h

In der Übung, am Kasten vor ID 2/467, oder per Mail an Florian.Giesen AT rub.de
Gruppenarbeit bis max. 3 Studenten pro Gruppe ist erlaubt und erwünscht.

1 Wörterbuchangriffe

Ein System speichert Passworte als 128-Bit Hashwerte. Betrachten Sie einen Wörterbuchangriff mit einem Wörterbuch mit 500.000 Einträgen.

a) Bei der Berechnung des Hashwertes wird kein Salt verwendet. Wieviel Speicherplatz benötigt eine vollständige (Passwort/Hashwert)-Tabelle *mindestens*? (Betrachten Sie dabei zur Vereinfachung nur die Länge des Hashwertes.)

b) Bei der Berechnung des Hashwertes wird ein 28-Bit Salt verwendet. Wieviel Speicherplatz benötigt eine vollständige (Passwort/Hashwert/Salt)-Tabelle *mindestens*? (Betrachten Sie dabei zur Vereinfachung nur die Länge des Hashwertes.)

c) Für eine Hashfunktion $H : D \to R$ definieren wir verschiedene Sicherheitsziele:

- *Preimage resistance*: Gegeben einen Hashwert $y \in R$, ist es nicht möglich $x \in D$ zu finden sodass $H(x) = y$.
- *Second preimage resistance*: Gegeben einen Wert $x_1 \in D$, ist es nicht möglich $x_2 \in D$ zu finden sodass $H(x_1) = H(x_2)$.
- *Collision resistance*: Es ist nicht möglich $x_1, x_2 \in D$ zu finden sodass $H(x_1) = H(x_2)$.

i. Geben Sie pro Sicherheitsziel ein Beispiel an, welches die Definition motiviert.

ii. Zeigen Sie: Wenn eine Hashfunktion *collision resistant* ist, dann ist sie *second preimage resistant*. (Tipp: Bruce Schneier würde einen Widerspruch erzeugen oder eine Reduktion machen).

2 PPTP

1. Abstrahieren Sie vom konkreten PPTP Angriff. Erklären Sie, welche Designschwächen der beschriebene Angriff ausnutzt, und skizzieren Sie geeignete Gegenmaßnahmen.

2. In Bild 1 ist eine vereinfachte Variante des bei PPTP verwendeten Authentikationsverfahrens gegeben. Führen Sie den Angriff von Mudge und Schneier auf diese Variante aus. Woraus bestehen die einzelnen Angriffsschritte?

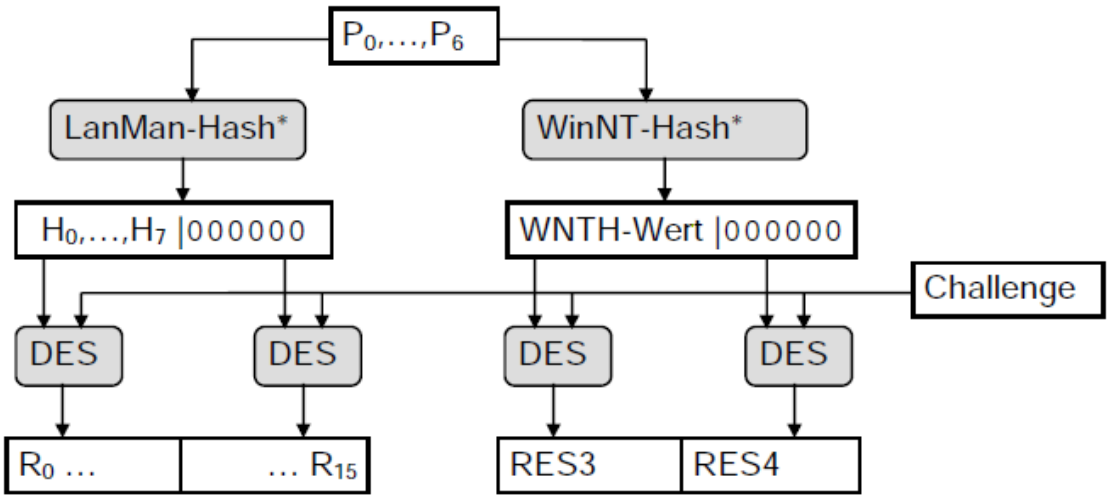

Abbildung 1: Vereinfachte Variante des PPTP Protokolls