Christian Schindelhauer

Freiburg, den 16. Juli 2014
Besprechung 22. Juli 2014

Übungen zur Vorlesung

Systeme II / Rechnernetze

Sommer 2014

Blatt 11 (13 Punkte)

AUFGABE 1: 5 Punkte

E-Mails werden im Internet überwiegend ohne Ende-zu-Ende versandt. Obwohl mehrere Methoden zur Verschlüsselung von E-Mails zur Verfügung stehen werden diese nur selten verwendet.

- Nennen sie mögliche Gründe dafür dass sich E-Mail Verschlüsselung (noch) nicht flächendeckend etabliert hat.
- Vergleichen sie die beiden Verschlüsselungsmethoden *S/MIME* und *PGP*. Gehen sie insbesondere auf folgende Punkte ein.
  1. Wo ist der Unterschied zwischen *S/MIME* und *PGP*?
  2. Welche Schutzziele werden von den jeweiligen Verschlüsselungen erfüllt?
  3. Welche kryptographischen Methoden werden jeweils verwendet?
- Beschreiben sie ein mögliches Angriffsszenario auf eine der beiden Methoden.

AUFGABE 2: 5 Punkte

Ein Server benutzt zur verschlüsselten Kommunikation das RSA-Verfahren mit folgendem Public-Key: $(N, e) = (622579, 21113)$

1. Wieso würde man solch einen Public-Key in der Realität nicht einsetzen?
2. Faktorisieren Sie N und errechnen Sie davon ausgehend dann d.
3. Sie haben folgende Daten bei einer Kommunikation zwischen dem Server und einem Client mitgeschnitten:
   $380157 \quad 615426 \quad 92340 \quad 57197$
   Entschlüsseln Sie die Daten[1]
4. Wie groß dürfen die zu verschlüsselnden Zahlen in diesem Fall maximal sein? Was passiert wenn eine Zahl größer ist?

[1] TIPP: Die Daten sind in UTF-8 kodiert. Jede Zahl vereint 2 Bytes und steht für zwei Zeichen.

AUFGABE 3: 3 Punkte

Ein Unternehmen möchte den Inhalt aller http(s)-Verbindungen im Unternehmensnetzwerk kontrollieren. Welche Sicherheitsziele sind verletzt?
Betrachten Sie:

1. http
2. https mit selbstsignierten Zertifikaten
3. https mit von einer CA signierten Zertifikaten

Beschreiben Sie für die drei Verbindungsarten was getan werden muss um die Verbindungen abzuhören.