Grundlagen der Systemsoftware

Modul: InfB-GSS

Veranstaltung: 64-091

Utz Pöhlmann
4poehlma@informatik.uni-hamburg.de
6663579

Louis Kobras
4kobras@informatik.uni-hamburg.de
6658699

Marius Widmann
4widmann@informatik.uni-hamburg.de
6714203

6. Juli 2016

Zettel Nr. 6 (Ausgabe: 27. Juni 2016, Abgabe: 06. Juli 2016)

5.1 Zentrale Begriffe der Kryptographie

5.1.2 Schlüsselaustausch (Pflicht; 2 Punkte)

Für n Personen gibt es $\binom{n}{2}$ Paare.

symmetrisch: Bei n Personen muss jeder seinen Schlüssel an $n-1$ Personen weitergeben. Es gibt also n Schlüssel, die $n-1$ mal weitergegeben werden, also $n*(n-1) = n^2 - n$ Tauschaktionen. Falls die Kommunikation in paarweise beide Richtungen stets mit dem gleichen Schlüssel stattfindet, bleiben $\frac{n^2-n}{2} = \binom{n}{2}$ Schlüsseltauschaktionen. So viele Schlüssel muss es auch geben.

asymmetrisch: Jede Person muss ein Schlüsselpaar generieren, einen `private key` und einen `public key`. Der Public Key wird per Broadcast oder als automatisierter Mailanhang verschickt, somit ensteht für jeden `private key`-Halter genau eine Aktion betreffs Schlüsselweitergabe. Dies macht bei n Personen n 'Tausch'-Aktionen, bei $2n$ generierten Schlüsseln.

5.1.3 Hybride Kryptosysteme (Pflicht; 3 Punkte)

Umstände: Hybride Kryptosysteme eignen sich bei großen Nachrichten, da symmetrische Verschlüsselung um mehrere Zehnerpotenzen schneller arbeiten als asymmetrische Verschlüsselungen. Durch die asymmetrische Verschlüsselung des vergleichsweise kurzen Keys (i.d.R. 128-256 Bit) wird trotzdem die erhöhte Sicherheit gewährleistet, falls eine dritte Partei den übermittelten Schlüssel erhält (dieser kann durch die Asymmetrie nicht entschlüsselt werden außer vom legitimen Empfänger).

Detail-Verfahren:

1. sie verschlüsselt die Nachricht N symmetrisch mit dem von ihr erzeugtem Schlüssel S
2. S wird asymmetrisch mit Bobs public Key K_p^B verschlüsselt
3. Alice übermittelt $(K_p^B(S), S(N))$ an Bob
4. Bob entschlüsselt $K_p^B(S)$ mit K_s^B
5. Bob entschlüsselt $S(N)$ mit S symmetrisch

Nachricht: Folgt aus eben: $N' = \{(K_p^B(S), S(N))\}$, also die symmetrisch verschlüsselte ursprüngliche Nachricht sowie der asymmetrisch verschlüsselte Key.

5.2 Parkhaus

5.2.2 Sicherheitsanalyse (Pflicht; 4 Punkte)

5.2.3 Umsetzung mit kryptographischen Techniken (Pflicht; 4 Punkte)

5.3 Authentifizierungsprotokolle

5.3.2 Authentifikationssystem auf Basis indeterministischer symmetrischer Verschlüsselung (Pflicht; 2 Punkte)

5.3.3 Challenge-Response-Authentifizierung (Pflicht; 2 Punkte)

5.5 RSA-Verfahren

5.5.2 Anwendung (Pflicht; 6 Punkte)