Kryptografie und -analyse, Zusammenfassung Vorlesung 2

Henry Haustein

Welche Angriffserfolge werden unterschieden?

Unterscheidung nach Ziel und Erfolg des Angriffs

- Finden des geheimen Schlüssels (vollständiges Brechen, total break)
- Finden eines zum Schlüssel äquivalenten Verfahrens (universelles Brechen, universal break)
- Brechen nur für manche Nachrichten (nachrichtenbezogenes Brechen):
  - für eine selbstgewählte Nachricht (selective break)
  - für irgendeine Nachricht (existential break)

Welche passiven und aktiven Angriffe werden bei kryptographischen Systemen unterschieden?

Passiver Angreifer nutzt Wissen über System (Algorithmen, Protokolle), Öffentliche Schlüssel/Parameter und Beobachtung (unsicherer Kanal)

- Reiner Schlüsseltext-Angriff (ciphertext-only attack)
- Klartext-Schlüsseltext-Angriff (known-plaintext attack)

Aktiver Angreifer: bringt Inhaber der geheimen bzw. privaten Schlüssel dazu, die entsprechenden Operationen für selbst gewählte Daten auszuführen

- Gewählter Klartext-Schlüsseltext-Angriff (chosen-plaintext attack CPA; *Verschlüsselungsorakel*)
- Gewählter Schlüsseltext-Klartext-Angriff (chosen-ciphertext attack; *Entschlüsselungsorakel*)

Was bedeutet informationstheoretische (perfekte) Sicherheit?

Auch einem unbeschränkten Angreifer gelingt es nicht, das System zu brechen.

Welche Bedingungen muss ein informationstheoretisch sicheres System erfüllen?

Ein System heißt informationstheoretisch sicher, wenn für alle Nachrichten und Schlüsseltexte gilt, dass die a posteriori Wahrscheinlichkeiten $p(m \mid c)$ der möglichen Nachrichten nach Beobachtung eines gesendeten

Geheimtextes gleich der a priori Wahrscheinlichkeiten $p(m)$ dieser Nachrichten sind:

$$\forall m \in M, \forall c \in C: \quad p(m \mid c) = p(m)$$

Warum werden in der Praxis kryptographische Systeme eingesetzt, die keine informationstheoretische Sicherheit bieten?

Perfekte Sicherheit kann nur symmetrische Verschlüsselung bieten, diese bietet aber keine Zurechenbarkeit.

Was bedeutet semantische Sicherheit?

Ein System heißt semantisch sicher, wenn alles, was bei Kenntnis des zugehörigen Schlüsseltextes effizient über den Klartext berechnet werden kann, auch effizient ohne Kenntnis des Schlüsseltextes berechnet werden kann.
⇒ Angreifer beschränkt, Beobachtung hilft nicht bei der Berechnung des Schlüssels

Was bedeutet Non-Malleability?

Ein System bietet Sicherheit gegen adaptive aktive Angriffe (Non- Malleability), wenn es für einen polynomiell beschränkten Angreifer nicht einfacher ist, bei Kenntnis eines Schlüsseltextes einen weiteren Schlüsseltext zu generieren, so dass die zugehörigen Klartexte in Relation zueinander stehen, als ohne Kenntnis dieses Schlüsseltextes.