Datensicherheit, Zusammenfassung Vorlesung 8

Henry Haustein, Dennis Rössel

In welcher Reihenfolge sollten Kryptographie und Kanalkodierung angewendet werden? Warum?

Zuerst verschlüsseln, dann kodieren, sonst war die Kodierung sinnlos.

Welche Schutzziele können mit Kryptographie umgesetzt werden? Was genau kann erreicht werden?

Mit Kryptographie erreichbare Schutzziele

- Vertraulichkeit: Informationen werden nur Berechtigten bekannt.
- Integrität: Informationen können nicht unerkannt modifiziert werden.
- Zurechenbarkeit (spezielles Integritätsziel): Es kann gegenüber Dritten nachgewiesen werden, wer die Information erzeugt hat.

Der Schutz der Verfügbarkeit erfordert andere Maßnahmen, z.B. Redundanz oder Kontrolle der Ressourcennutzung.

Was besagt das Kerkhoffs-Prinzip?

Kerckhoffs-Prinzip: *Die Sicherheit eines Verfahrens darf nicht von der Geheimhaltung des Verfahrens abhängen, sondern nur von der Geheimhaltung des Schlüssels.*

- Keine *Security by Obscurity*
- Annahme: Angreifer kennt das Verfahren und die öffentlichen Parameter
- Sicherheit des Verfahrens begrenzt durch Sicherheit der Schlüsselgenerierung und Sicherheit des Schlüsselaustauschs

Kryptographie beruht grundsätzlich darauf, dass die Entschlüsselung durch Geheimhaltung von Daten verhindert wird. Der Unterschied besteht darin, ob ein Schlüssel oder auch der verwendete Algorithmus geheim gehalten wird – denn sobald der Algorithmus für viele Dinge verwendet wird, ist er nicht mehr geheim, sondern weit verbreitet. Security by obscurity wäre dann der Versuch, Dinge geheim zu halten, die weite Verbreitung finden. Ein starker Algorithmus, beispielsweise der Advanced Encryption Standard oder das RSA-Kryptosystem, erfordert aus der Sicht der reinen Kryptographie-Sicherheit keine Geheimhaltung des Verfahrens, sondern nur des verwendeten Schlüssels. Die Kryptographie-Sicherheit beschäftigt sich mit der Sicherheit eines Verfahrens. Gleichwohl werden immer wieder Verschlüsselungsalgorithmen geheim gehalten. Schließlich können durch deren Kenntnis die eventuellen Schwachstellen entdeckt werden, so dass sich erst später herausstellt, dass die Verschlüsselung nicht effektiv war. Ein Beispiel ist RC4, welcher sieben

Jahre lang geheim gehalten wurde, bis 1994 der Quellcode anonym veröffentlicht wurde – inzwischen gilt RC4 als massiv unsicher. Auf diese Weise führt security by obscurity zu einem Verlust von Sicherheit, da bei diesem Prinzip die vermeintlichen Sicherheitsmethoden nicht auf ihre Wirksamkeit überprüft und die unwirksamen Methoden nicht frühzeitig als solche verworfen werden können.[1]

Wie funktionieren prinzipiell symmetrische und asymmetrische Konzelations- und Authentikationssysteme?

Symmetrisches Konzelationssystem: Verschlüsselung und Entschlüsselung mit dem selben Schlüssel, nur die verschlüsselte Nachricht wird übertragen

Symmetrisches Authentikationssystem: Übertragung von Nachricht und verschlüsselter MAC (= Prüfsumme der Nachricht)

Asymmetrisches Konzelationssystem: mit dem öffentlichen Schlüssel kann eine Nachricht verschlüsselt werden, aber nur mit dem privaten Schlüssel kann die Nachricht wieder entschlüsselt werden

Asymmetrisches Authentikationssystem (digitales Signatursystem): Übertragung der Nachricht und der Signatur (Nachricht mit privatem Schlüssel verschlüsselt)

Warum kann nur mit digitalen Signatursystemen Zurechenbarkeit erreicht werden?

Weil nur derjenige eine richtige Signatur erstellen kann, der in Besitz des privaten Schlüssels ist.

Was sind Vor- und Nachteile symmetrischer bzw. asymmetrischer Systeme?

Performance ist bei asymmetrischen Systemen schlechter, allerdings gibt es das Problem des Schlüsselaustasuches nicht

Wie ist der prinzipielle Ablauf eines hybriden Konzelationssystems?

Schlüsselaustausch mittels asymmetrischer Verschlüsselung, dann wird auf symmetrische Verschlüsselung umgestellt

[1] https://de.wikipedia.org/wiki/Security_through_obscurity