Sicherheit

Philipp Adler

13. Oktober 2015

Inhaltsverzeichnis

1 Grundlagen Securityverfahren

1.1 Verschlüsselungsarten

1.2 Kommunikationsszenarien

1.3 Sicherheitsziele

1.4 Bedrohungsszenarien

2 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung reicht bis in die Antike. Damals wussten nur die Adressierten von dem Geheimnis, nach welchem Verfahren die Botschaft verschlüsselt wurde. Cäsar zum Beispiel verschob jeden Buchstaben um 4 Stellen. So wurde aus Hallo Kdoor. Aus diesem Verschlüsselungsalgorithmus entstanden zum einen Blockchiffren, auf den ich in dem folgenden Kapitel näher eingehen werde und die Stromchiffren.[1]

2.1 Blockchiffre

Blockchiffren teilen die Nachricht, die verschlüsselt werden soll, in eine fixe Anzahl an Blöcken, die entweder 64 oder 128 Bit groß sind. Typische, bekannte Blockchiffre sind Data Encryption Standard, Advanced Encryption Standard und International Data Encryption Algorithm.[1]

2.1.1 Der Data Encryption Standard - DES

"DES wurde 1977 vom amerikanischen 'National Institute of Standards and Technologies (NIST)' veröffentlicht."[1] Bei diesem Verfahren wird eine Blocklänge von 64 Bit und ein DES-Schlüssel von 56 Bits plus 8 PParity Check Bits"[1] eingesetzt. Die ersten 56 Bits werden immer zufällig generiert, wobei die letzten 8 Bits dafür sorgen, dass keine Übertragungsfehler auftreten. Da 56 Bit zufällig sind, können daraus 2^{56} Schlüsseln erzeugt werden. **Das Schema** Beim Verschlüsselungsverfahren werden aus dem Klartext Blöcke alle jeweils mit einer Länge von 64 Bit erzeugt. Dieser Block wird dann nochmals zerlegt, sodass daraus 2 mal 32 Bit Blöcke entstehen. Der Data Encryption Standard besteht aus 16 Runden. In jeder Runde wird auf die rechte Hälfte ein Verschlüsselungsalgorithmus f angewendet. Das daraus resultierende Ergebnis wird bitweise mit einem XOR-Gatter mit der linken Hälfte verknüpft und "bildet die rechte Seite der neuen Runde"[2].

wird die linke Hälft mit der Rechten vertauscht und anschließend wird die Linke mit einem Verschlüsselungsalgorithmus f bitweise mit einem XOR-Gatter verknüpft. In dieser Funktionen befinden sich zum einen der Parameter ki und zum anderemRi.

Abbildungsverzeichnis

Literatur

[1] Jörg Schwenk. *Sicherheit und Kryptographie im Internet.* Springer 4.Auflage, 2014.

[2] Thomas Schwarzpaul Albert Beutelspacher, Heike B. Neumann. *Kryptografie in Theorie und Praxis.* Vieweg 1.Auflage, 2005.