Fachhochschule Nordwestschweiz
Hochschule für Technik

Differentielle Kryptoanalyse

Artikel Kryptographie
Windisch, 18. Mai 2020

thirah_vorhangeschloss-schlussel-computer-icons_nodate

Autoren	Gabriel Nussbaumer und Fabian von Büren
Dozent	Dr. M. Hufschmid
Modul	Kryptographie (kryg)
Hochschule	Hochschule für Technik - FHNW
Studiengang	Elektro- und Informationstechnik

Inhaltsverzeichnis

1 Einleitung **1**

2 Historisches **1**

3 Funktionsweise **2**

4 Sicherheit **2**

5 Schluss **2**

1 Einleitung

Kryptosysteme sind Funktionen, welche darauf basieren mehrere Runden zu durchlaufen. Bei einer Runde von DES sind verschiedene Funktionen enthalten es gibt eine Bit-Permutation, arithmetische Operationen, EXOR-verknüpfungen und die S-Boxen. Die S-Boxen sind nichtlineare Übersetzungstabellen. Der gesamte Verschlüsselungsalorythmus, die Permutations Tabellen wie auch die Überstzungstabellen der S-boxen sind öffentlich bekannt. Die Geheimhaltung der Daten hängt also vom zufällig gewählten geheimen Schlüssel ab. Bei der Differenziellen Kryptoanalyse, wird ein Statischer angriff Angriff auf den den Verschlüsselungsalgorythmus, durchgeführt, bei dem der Angreifer selbstgewählte Klartext und Geheimtextpaare verwenden kann, es handelt sich also um eine chosen plaintext attack.

Wird ein Klartextangriff durchgeführt kann die Komplexität der DES Verschlüsselung in einer Runde um die Hälfte reduziert werden, da die Symmetrie durch Komplementierung genutzt werden kann.

Es werden Differenzen in den Klartextpaaren auf Differenzen in den Geiheimtextpaaren analysiert. Diese Differenzen werden verwendet um mögliche Schlüssel Wahrscheindlichkeiten zuzuordnen und den wahrscheinlichsten Schlüssel zu finden. Bei Anwendung dieser Methode auf den DES nimmt die Komplexität der Verschlüsselung mit der Anzahl der Runden zu, wobei sich die Differenziellekryptoanalyse nicht mehr bewehrt bei 16 Runden, im Bezug auf eine brute-force attack.

$$T = DES(P, K)$$

$$\bar{T} = DES(\bar{P}, \bar{K})$$

Somit entspricht der Wert X dem Bitweise komplementierten Wert $\bar{X}$. Die Eigenschaft wird bei der Kryptonanalyse ausgenutzt indem zwei Klartext-Textpaare P_1, T_1 und P_2, T_2 zur Verfügung stehen und es gilt $P_1, \bar{T}_2$ oder $P_2, \bar{T}_1$. Der Angreifer verschlüsselt P_1 unter allen 2^{55} Schlüsseln K, deren niederwertigstes Bit Null ist. Wenn im Geheimtext der Wert T gleich dem Wert T_1 ist, dann ist der entsprechende Schlüssel K wahrscheinlich der echte Schlüssel. Ist T gleich dem Wert $\bar{T}_2$ dann ist der Schlüssel wahrscheinlich $\bar{K}$.

2 Historisches

Die differenzielle Kryptoanalyse wurde im Juli 1990 von den israelischen Wissenschaftler Eli Biham und Adi Shamir veröffentlicht. In dieser Veröffentlichung wird die Methode beschrieben wie ein chosen plaintext Angriff auf den DES durchgeführt werden kann.

Der Data Encription Standard (DES) war in den 70 Jahren das damals meist verwendete Verschlüsselungssystem für die zivile Bevölkerung. Mit dem DES konnte in dieser Zeit ein grosser Widerstand gegen Angriffe bewiesen werden, und wurde im Jahre 1977 als offizieller Sicherheitsstandard für die US-Regierung vom Federal Information Processing Standard (FIBS) bestätigt.

3 Funktionsweise

4 Sicherheit

5 Schluss