“Praktische Kryptanalyse von realen Systeme”

Benedikt Driessen

Diese Arbeit ist der Analyse von symmetrischen, kryptographischen Algorithmen gewidmet. Das Dokument konzentriert sich im speziellen auf proprietäre, nicht öffentlich dokumentierte Verfahren die in vier global eingesetzten Systemen verwendet werden. Alle untersuchten Verfahren wurden durch den Prozess des Reverse-Engineering rekonstruiert, drei davon im Verlauf dieser Arbeit (aber nur eines durch dessen Autor). Die gefundenen Konstruktionen wurden analysiert und konsequent attackiert. Bei den angegriffenen Systemen handelt es sich um den globalen Telefoniestandard GSM, sowie die zwei Standards für Satellitentelefonie GMR-1 und GMR-2. Als viertes System wurde ein digitales Schließsystem angegriffen. Unsere Untersuchungen zeigen, dass auch neuere Entwicklungen weiterhin unter schweren Designfehlern leiden. Dies ist überraschend, zumal es zunehmend mehr öffentlichen Publikationen gibt, welche die üblichen Anforderungen und Probleme von real eingesetzten Systemen adressieren.

Die Stromchiffren A5/1 und A5/2, die im GSM Standard eingesetzt werden, wurden bereits vor einem Jahrzehnt rekonstruiert und gebrochen. Obgleich die kryptanalytischen Attacken bereits so weit fortgeschritten sind, dass sie praktikabel eingesetzt werden können, hat uns dies dazu motiviert, deren Effizienz weiter zu steigern. In dieser Arbeit wird ein Entwurf für eine Hardware basierend auf OP-Verstärkern vorgestellt, die binäre, lineare Gleichungssysteme über den rationalen Zahlen lösen kann. Das schnelle Lösen solcher Systeme ist der Kern vieler Angriffe auf Stromchiffren, auch im Fall von GSM. Um aber die erhaltenen Lösungen für einen echten Angriff nutzbar zu machen, musste eine Methode gefunden werden um rationalen Lösungen in den Raum der binären Zahlen zu transformieren. Eine solche Methode wird beschrieben, sie ist aber auch unabhängig von der vorgeschlagenen Rechnerarchitektur interessant.

Im Anschluss wird die Stromchiffre A5-GMR-1 vorgestellt, die aus einem Satellitentelefon für den GMR-1 Standard extrahiert wurde. Die Chiffre wird analysiert und mittels einer Attacke gebrochen, die lediglich verschlüsselte Daten benötigt. Damit ist die Attacke extrem praktikabel, was praktisch demonstriert wird. Dies, sowie detaillierte Angaben zur Konfiguration eines GMR-1 Netzwerks, zeigt, dass auf die Sprachverschlüsselung in GMR-1 nicht vertraut werden sollte.

Im Weiteren wird die Analyse auf den zweiten Satellitentelefonie-Standard ausgedehnt. Es wird der Prozess beschrieben, der die Rekonstruktion von A5-GMR-2, der Chiffre im GMR-2 Standard, aus der Firmware eines Telefons ermöglicht hat. Diese Beschreibung enthält die Designprinzipien für einen rekursiven Disassembler und Techniken, um die Chiffre (die nur einen Bruchteil der 300 000 disassemblierten Codezeilen ausmacht) zu finden. Das Ergebnis der anschließenden Analyse wird dokumentiert und eine sehr effiziente Attacke präsentiert, die sich anhand des verfügbaren Schlüsselstroms parametrisieren lässt.

Als letztes System wird in dieser Arbeit das digitale Schließsystem SimonsVoss 3060 betrachtet und das eingesetzte Authentifikationsverfahren beschrieben. Das Verfahren setzt zwei proprietäre Konstruktionen (für Schlüsselableitung und Antwortberechnung) ein, die auf einem modifizierten DES und einer T-Funktion-ähnlichen Methode basieren. Die Kombination von vier verschiedenen Schwächen in dem Design mit Techniken der differentiellen Kryptanalyse und einer rekursiven Angriffsprozedur auf die T-Funktion ermöglicht zwei verschiedene Attacken. Beide Attacken sind praktikabel und erlauben das unautorisierte Öffnen von Türschlössern.

Durch die interdisziplinäre Natur dieser Arbeit eröffnet jedes Kapitel eine eigene Perspektive auf Angriffe auf real eingesetzte Systeme: Im ersten Kapitel wird der kreative Ansatz existierende Attacken zu beschleunigen beschrieben. Das zweite Kapitel zeigt, wie Kryptanalyse im Rahmen von einem globalen System eingesetzt und praktisch angewandt werden kann. Das dritte Kapitel zeigt den Aufwand, der hinter Reverse-Engineering Vorhaben im Umfeld von hoch-komplexen, eingebetteten Systemen steckt. Das vierte Kapitel zeigt schließlich, wie sich kryptanalytische Methoden im Verlauf einer Analyse (d.h. mit wachsendem Wissen über ein System) verbessern können.