Jens Rüdinger

Auswirkungen von Seitenkanalangriffen auf das Design kryptographischer Algorithmen

Beiträge aus der Informationstechnik

Jens Rüdinger

Auswirkungen von Seitenkanalangriffen auf das Design kryptographischer Algorithmen

VOGT

Dresden 2009

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Bibliographic Information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibiograpic data is available in the internet at http://dnb.ddb.de.

Zugl.: Dresden, Techn. Univ., Diss., 2009

Die vorliegende Arbeit stimmt mit dem Original der Dissertation „Auswirkungen von Seitenkanalangriffen auf das Design kryptographischer Algorithmen“ von Jens Rüdinger überein.

Gesetzt vom Autor
Printed in Germany

ISBN 978-3-938860-27-4

Jörg Vogt Verlag
Niederwaldstr. 36
01277 Dresden
Germany

Phone: +49-(0)351-31403921
Telefax: +49-(0)351-31403918
e-mail: info@vogtverlag.de
Internet : www.vogtverlag.de

Technische Universität Dresden

Auswirkungen von Seitenkanalangriffen auf das Design kryptographischer Algorithmen

Jens Rüdinger

von der Fakultät Elektrotechnik und Informationstechnik der Technischen Universität Dresden

zur Erlangung des akademischen Grades eines

Doktoringenieurs

(Dr.-Ing.)

genehmigte Dissertation

Vorsitzender: Prof. Dr. rer. nat. habil. H. G. Krauthäuser
Gutachter: Prof. Dr.-Ing. habil. A. Finger
Prof. Dr.-Ing. G. Fettweis
Dr. K. Mayes

Tag der Einreichung: 07.04.2008
Tag der Verteidigung: 21.11.2008

Danksagung

Die vorliegende Dissertation entstand während meiner Tätigkeit als Systemspezialist der Vodafone D2 GmbH. Mein besonderer Dank gilt Herrn Andreas Dorstel sowie der Vodafone D2 GmbH für die Anregung zu dieser Arbeit sowie die Unterstützung während der Durchführung.

In gleichem Maße danke ich meinem betreuenden Hochschullehrer Prof. Dr.-Ing. habil. Adolf Finger vom Lehrstuhl Theoretische Nachrichtentechnik des Instituts für Nachrichtentechnik der TU Dresden für die Betreuung der Arbeit sowie die langjährige erfolgreiche Zusammenarbeit weit über den Rahmen der vorliegenden Dissertation hinaus.

Den Herren Prof. Dr.-Ing. Gerhard Fettweis, Lehrstuhl Mobile Nachrichtensysteme des Instituts für Nachrichtentechnik der TU Dresden und Dr. Keith Mayes, Direktor des Smart Card Centre der Royal Holloway University of London danke ich für die Übernahme der Gutachten sowie die intensive Auseinandersetzung mit meiner Arbeit.

Ein besonderer Dank gilt meiner Frau Ute sowie unseren Kindern Gordon und Nora ohne deren Unterstützung und Verständnis die Durchführung dieser Arbeit nicht möglich gewesen wäre.

Nicht zuletzt danke ich meinen Eltern, die durch ihre Förderung und Unterstützung vor vielen Jahren den Grundstein für die vorliegende Dissertation gelegt haben.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einführung

Die Kryptographie als die Wissenschaft des Entwurfs und der Analyse kryptographischer Algorithmen spielt eine immer größere Rolle in unserem Leben. So begegnen wir täglich mehrfach Implementierungen kryptographischer Verfahren und wenden diese an.

Kryptographische Verfahren kommen nicht nur in Form von Verschlüsselungssoftware auf dem PC oder beim Austausch von Zertifikaten zum sicheren Surfen im Internet zum Einsatz, sondern finden sich auch in den uns zahlreich umgebenden eingebetteten Geräten wieder.

Eingebettete Geräte (engl. embedded devices) sind spezielle Computer, die, anders als universelle Personalcomputer, für die Erfüllung dedizierter Aufgaben entwickelt wurden. Sie sind eingebettet in Maschinen und Systeme (z.B. Autos, Waschmaschinen, Videorecordern, Mobiltelefonen, usw.) und übernehmen Aufgaben der Steuerung und Kontrolle dieser Maschinen und Systeme.

Eine besondere Form eingebetteter Systeme sind Smartcards. Hierbei handelt es sich um Plastikkarten, die, anders als reine Speicherkarten oder Magnetstreifenkarten, über einen eigenen Prozessor – gegebenenfalls mit kryptographischem Koprozessor –, Speicher für die Speicherung von Programmen (Software) und Daten sowie Ein-/Ausgabeschittstellen für die Kommunikation nach außen verfügen. Die Schnittstellen nach außen können je nach Bauart kontaktbehaftet oder kontaktlos (NFC, engl. near field communication) erfolgen.

Smartcards kommen unter anderem zum Einsatz als SIM- bzw. USIM-Karten (engl. (universal) subscriber identity modul) in der Telekommunikation, als Bankkarten im Finanzwesen, als Entschlüsselungskarten im Bezahlfernsehen oder auch als Zugangs- und Berechtigungskarten im Transport- und Veranstaltungswesen.

Relativ neu und an Bedeutung gewinnend sind RFID-Tags (engl. radio frequency identification), die beispielsweise in den neuen deutschen Reisepässen zum Einsatz kommen.

Integraler Bestandteil der oben beschriebenen und weiterer Formen einge-

betteter Systeme sind kryptographische Verfahren. Sie sichern – meist transparent für den Nutzer – Berechtigungen beim Zugriff oder Zutritt der genutzten Systeme (Authentizität) und wahren die Geheimhaltung (Verschlüsselung) und Unveränderbarkeit (Integrität) vertraulicher Daten. Sie bilden damit die Basis für die Nutzung eines Systems.

Systeme mit eingebetteten Geräten beruhen darauf, dass die zugrunde liegenden kryptographischen Verfahren (Algorithmen und Schlüssel) sicher sind. Ihre Sicherheit beeinflusst sowohl die Akzeptanz und Nutzung der Systeme beim Kunden als auch das Geschäftsmodell des Betreibers.

Die Sicherheit kryptographischer Verfahren wird dabei von 2 Aspekten bestimmt:

1. Der Algorithmus selbst muss sicher sein. Das heißt, der Algorithmus weist keine kryptographischen Schwächen auf, die einen mathematisch-kryptoanalytischen Angriff gegen ihn ermöglichen.

2. Die Implementierung des Algorithmus muss sicher sein.

Seit den Arbeiten von Kocher (1996, Zeitanalyse [67]) und Kocher, Jaffe und Jun (1998, Stromanalysen [68]) haben sich Seitenkanalanalysen als effiziente Methode erwiesen, Implementierungen kryptographischen Verfahren anzugreifen.

Seitenkanalanalysen sind implementierungsabhängige Methoden kryptographische Verfahren anzugreifen. Sie beruhen auf Parametern, die während der Ausführung des Algorithmus gewonnen werden (Ausführungszeit, Stromverbrauch, usw.) und ergänzen somit traditionelle mathematischen Analysen, die nur auf Basis von Klartext und Chiffretext arbeiten.

Weisen Algorithmen keine kryptographischen Schwächen auf und sind rechnerisch sicher (engl. computational secure), so gewinnt die Sicherheit der Plattform an Bedeutung. Insbesondere statistische Seitenkanalangriffe auf Basis der differentiellen Stromanalysen (DPA, engl. differential power analysis) haben sich als besonders wirkungsvoll erwiesen. Ihnen ist nur schwer zu begegnen.

Prinzipiell gibt es 2 Möglichkeiten Seitenkanalangriffen zu begegnen:

Implementierungssicht Seitenkanalangriffe werden als Implementierungsangriffe betrachtet und ihnen wird auf Implementierungsebene begegnet. Ziel ist die Entwicklung von Hardware- und Software-Gegenmaßnahmen, um bestehende Algorithmen sicher zu implementieren.

Designsicht Wie im Rahmen der Arbeit gezeigt wird, sind Seitenkanalangriffe algorithmenspezifisch. Sie werden an den anzugreifenden Algorithmus angepasst, und sind damit abhängig vom Algorithmus. Die Designsicht beschäftigt sich daher mit den Fragen:

- Welche algorithmenspezifischen Merkmale beeinflussen die Anfälligkeiten des Algorithmus gegenüber Seitenkanalangriffen?
- Welche Algorithmen sind weniger anfällig als andere? Warum?
- Was kann im Designprozess getan werden Seitenkanalangriffen zu begegnen?

In der vorliegenden Arbeit geht es darum, den 2. Aspekt Seitenkanalangriffen zu begegnen, die Designsicht, näher zu betrachten. Die Betrachtung aus Designsicht hat weitgehende Konsequenzen für das gesamte Gebiet der Seitenkanalanalyse.

Die Seitenkanalanalyse ist ein relativ junges und dynamisches Wissenschaftsgebiet und wird erst seit Ende der 90er Jahre systematisch erforscht. Implementierungsbezogene Kryptokonferenzen wie die seit 1999 jährlich stattfindende CHES-Konferenz (engl. Workshop on Cryptographic Hardware and Embedded Systems) haben sich neben den mathematisch orientierten Kryptokonferenzen wie CRYPTO, EUROCRYPT und ASIACRYPT etabliert und verfolgen die Seitenkanalanalyse schwerpunktmäßig.

Dabei sind in den letzten Jahren sowohl zahlreiche Angriffe als auch Gegenmaßnahmen entwickelt und verbessert worden. Herkömmliche Gegenmaßnahmen betrachten vor allem die Implementierungsabhängigkeit der Seitenkanalangriffe und weisen hinsichtlich Wirksamkeit und Aufwand einige Limitierungen auf.

Anders als bei traditionellen kryptoanalytischen Angriffen ist der Erfolg eines Angriffs mittels Seitenkanalanalyse zudem von den Fähigkeiten und Fertigkeiten des Angreifers abhängig.

Ziel der Arbeit ist eine umfassende Betrachtung der Seitenkanalanalyse aus Algorithmensicht. Dabei geht es sowohl darum, bestehende Seitenkanalangriffe auf algorithmenspezifische Voraussetzungen zu untersuchen und zu klassifizieren, als auch darum, Designmerkmale von Algorithmen hinsichtlich ihres Einflusses auf die Voraussetzungen zu betrachten. Anhand dieser Merkmale soll es möglich sein, kryptographische Algorithmen in Bezug auf Anfälligkeit gegenüber Seitenkanalangriffen zu bewerten.

Der Schwerpunkt der Arbeit liegt dabei auf symmetrischen Verschlüsselungsalgorithmen und passiven nichtinvasiven Seitenkanalangriffen. Symmetrische Verschlüsselungsalgorithmen, insbesondere Blockchiffren, beruhen auf relativ einfachen Designprinzipien. Dadurch ist eine Beeinflussung der Anfälligkeit gegenüber Seitenkanalangriffen, anders als bei asymmetrischen Algorithmen - die auf komplexen mathematischen Problemen beruhen - durch Änderungen im Design möglich.

Passive nichtinvasive Angriffe sind sehr effektiv, einfach anzuwenden und setzen zum Teil keinerlei Kenntnis der Implementierung voraus. Anders als invasive und aktive nichtinvasive Angriffe sind sie nicht zu detektieren und mit herkömmlichen Gegenmaßnahmen schwer zu begegnen.