Über die Prüftiefe und die Aussagekraft von IT-Sicherheitsgutachten

Wolfgang Killmann[1], Werner Schindler[2]

[1]T-Systems GEI GmbH
Rabinstrasse 8
53111 Bonn
Wolfgang.Killmann@t-systems.com
[2]Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185 – 189
53175 Bonn
Werner.Schindler@bsi.bund.de

Abstract: IT-Sicherheitsuntersuchungen dienen der objektiven Bewertung der Vertrauenswürdigkeit von Produkten und IT-Systemen im Interesse der Anwender und Hersteller. Die Zuverlässigkeit der gewonnenen Ergebnisse ist abhängig vom Umfang der verfügbaren Informationen, der aufgewandten Zeit und Hilfsmittel sowie der Qualifikation der Untersuchenden. An konkreten Beispielen wird der Zusammenhang zwischen Prüftiefe und aufgedeckten Schwachstellen sowie deren Bewertung untersucht.

1 Einleitung

Die Intensität der IT-Nutzung und die Komplexität der Applikationen haben sich insbesondere durch das Internet in den letzten Jahren weiter vertieft. Damit hat sich die Abhängigkeit von der sicheren Anwendung der IT verstärkt. Es ist aber auch das Sicherheitsbewusstsein der Anwender und die öffentliche Einstellung zur IT-Sicherheit gestiegen. Immer mehr Nutzer wollen ihre IT-Anwendungen gegen Bedrohungen schützen. Sie benötigen dafür sichere Produkte und die Fähigkeit, diese sachgemäß einzusetzen. Die IT-Industrie wird diesen Anforderungen zunehmend besser gerecht, wenn auch lange nicht so erfolgreich, wie dies von vielen Anwendern gewünscht wird.

Im folgenden werden Ursachen diskutiert, die zu Sicherheitsproblemen führen können. Anhand dreier ausgewählter Beispiele (Firewall, Hybridverschlüsselung von Nachrichten, Power-Attacken gegen Chipkarten) werden typische Fehler und Sicherheitslücken erläutert und Möglichkeiten aufgezeigt, diese Schwachstellen zu beheben. Wir beschäftigen uns mit der Frage, welche Arten von Sicherheitsuntersuchungen diese Schwachstellen erkennen und wo deren Grenzen liegen. Dieser Aufsatz beleuchtet die Frage, in

welchem Umfang Evaluierungen dem Nutzer der IT-Produkte ermöglichen, deren Vertrauenswürdigkeit zu beurteilen und ihre Anwendungen zu schützen. Die Aussagen werden an den bereits erwähnten drei Fallbeispielen veranschaulicht.

2 Notwendigkeit der Sicherheitsuntersuchungen

Die Bedrohungen sind mit der Fülle der Anwendungen und der Weiterentwicklung der Technik vielfältiger und raffinierter geworden. Der ursprüngliche Hack zum kostenlosen Telefonieren in den 50er Jahren findet heute seine Fortführung in penetranten 0190-Dialern. Aus Computerviren entwickelten sich Emailwürmer und verteilte Netzattacken (distributed denial of service attacks). Anwenderprogramme gehen zuweilen ungefragt ins Internet und informieren Hersteller über das Nutzungsverhalten des Verbrauchers. Spionageangriffe gelten nicht allein einzelnen Datenbanken, sondern Kreditkartennummern oder gar der Korrespondenz der Konkurrenzfirma. Aber auch das Spektrum der Angreifer hat sich verändert. Spezielle Werkzeuge versetzen selbst einen Anfänger (Scriptkids) in die Lage, gefährliche Sabotageprogramme zu bauen. Die Hackerszene, ob für Computerspiele, Pay-TV-Chipkarten oder den Einbruch in einen Bankrechner, wächst an Umfang und Qualifikation. Am oberen Ende der Skala finden sich Cyberterroristen und Spezialdienste, die für den elektronischen Krieg rüsten. Die Anwender benötigen deshalb Hilfe, die für ihre IT-Anwendungen relevanten Bedrohungen zu erkennen und deren angemessene Abwehr zu organisieren.

Hersteller messen der IT-Sicherheit einen sehr unterschiedlichen Stellenwert bei. Chipkarten werden als Sicherheitsprodukt entwickelt und produziert. Sie verfügen über sehr umfangreiche Sicherheitsmaßnahmen und widerstehen unterschiedlichsten aufwendigen Angriffen. Das macht sie für den Einsatz als elektronische Geldbörsen in der Kreditwirtschaft oder als Signaturerstellungseinheit geeignet. Betrachtet man dagegen die für die elektronische Signatur ebenfalls benötigte PC-Software, so ergeben sich gelegentlich unerwartete und nicht hinnehmbare (Sicherheits-)Untiefen (vgl. z.B. [CSL]), und Unterschiede in der erreichten Sicherheit werden deutlich sichtbar.

Inzwischen arbeiten weltweit Tausende von Forschern in Industrie und Hochschulen auf verschiedenen Gebieten der IT-Sicherheit. Sicherheitsmechanismen sind in vielen IT-Produkten implementiert, und es besteht ein breiter IT-Sicherheitsmarkt. Anders als noch vor zwanzig Jahren ist das Wissen über geeignete kryptographische Algorithmen geradezu Allgemeingut geworden. Referenzimplementierungen des Triple-DES, AES, SHA-1 etc. sind frei verfügbar. Trotzdem können Sicherheitsprodukte offene oder versteckte Schwachstellen vielfältigster Art besitzen: aus ungenügender Analyse des Sicherheitsproblems resultierende Designfehler, Sicherheitsstandards ignorierende individuelle Lösungen, faule Kompromisse für komplexe Funktionalität und gegen beherrschbare Sicherheit, dem Kosten- und Zeitdruck geschuldete Implementierungsfehler, Bedienerunfreundlichkeit und unzureichende Betriebsdokumentation u. v. m. Die Schwachstellen von Kryptoprodukten basieren selten auf der Verwendung schwacher kryptographischer Algorithmen, sondern vielmehr auf mangelhafter Implementierungen, proprietären Protokollen oder ungeeignetem Zusammenwirken der Mechanismen. Immer wieder

werden gravierende Schwachstellen erst nach Markteinführung der Produkte entdeckt. Obwohl es auch im Interesse des Herstellers und ihrer Kunden liegt, diese rechtzeitig zu erkennen und zu beseitigen, werden Sicherheitsanalysen durch die Hersteller selbst oder durch externe Experten oftmals grob vernachlässigt. Im Gegenteil, manche Hersteller versuchen, Sicherheitsprobleme geheim zu halten oder herunterzuspielen. Open Source Entwickler dagegen reagieren oft sehr schnell und konstruktiv auf aufgedeckte Schachstellen. Die Offenlegung des Quellcodes bietet sehr gute Voraussetzungen, selbst tiefer liegende Sicherheitsschwachstellen aufzudecken und zu beseitigen. Aber diese Möglichkeit haben sowohl die sie unterstützenden Sicherheitsanalytiker als auch die Angreifer. Deshalb erfordern auch sichere Open Source Lösungen systematische, sachkundige Entwicklung und Analyse.

Sicherheitslücken sind nicht zuletzt durch Berichte in den Massenmedien stärker bekannt geworden. Sicherheitsprodukte werden in Fachzeitschriften beschrieben und bewertet, Anwender berichten über ihre Erfahrungen, Hacker geben ihre Erfolge preis. Dadurch werden die Anwender sensibilisiert und zu eigenem sicherheitsbewusstem Handeln motiviert. Darüber hinaus muss aber die Fähigkeit und Bereitschaft entwickelt werden, den oft erheblichen Aufwand zum sicheren Betrieb seiner Anwendungen tatsächlich zu treiben. Die erfolgreiche Verbreitung der Internet-Würmer hat ja gerade gezeigt, dass die IT-Systeme nicht auf dem aktuellen Stand der Sicherheitsmaßnahmen waren, Sicherheitspatches nicht installiert waren, Server und Emailprogramme unsicher konfiguriert waren usw. Sicherheitsuntersuchungen der IT-Produkte decken Sicherheitsmängel auf und erhöhen das Vertrauen der Anwender in die Wirksamkeit der Sicherheitsmaßnahmen. Die konkreten IT-Systeme, die aus einer Vielzahl unterschiedlicher Computer, Dienste und Anwendungen bestehen, deren sicheres Management und deren operationeller Betrieb müssen folglich kontinuierlich untersucht werden.

3 Arten der Sicherheitsuntersuchungen

Sicherheitsuntersuchungen können mit sehr unterschiedlicher Zielsetzung, Methodik und Ergebnissen durchgeführt werden. Ein Hacker wird ein IT-System eines Anwenders auf ausnutzbare Schwachstellen absuchen, um an die damit verarbeiteten Informationen, angebotenen Dienstleistungen oder Werte zu gelangen. Ein einzelnes Produkt ist vor allem dann von Interesse, falls es weit verbreitetet ist und somit viele IT-Systeme eine einmal gefundene Schwachstelle aufweisen werden. Ist der Hacker fündig geworden, wird er das IT-System attackieren. Findet er nichts, so wird man nur selten von seinem Misserfolg erfahren. Ein Sicherheitsgutachten eines Produktes hat dagegen den Ausschluss weitgehend aller Schwachstellen zum Ziel, um möglichst umfassend jegliche für ein vorgesehenes Einsatzgebiet zu erwartenden Angriffe auszuschließen. Wenn ein Gutachten keine Schwachstellen aufdeckt, so wird dies die Überzeugung stärken, dass tatsächliche keine Schwachstellen vorhanden sind. Die Zuverlässigkeit der gewonnenen Ergebnisse ist stets abhängig vom Umfang der verfügbaren Informationen, der aufgewandten Zeit und Hilfsmittel sowie der Qualifikation der Untersuchenden zu bewerten. Im Vergleich zu Hackerangriffen zeichnen sich solche Untersuchungen im allgemeinen durch ein systematischeres Vorgehen aus, und der Auftraggeber der Untersuchung stellt

den Evaluatoren normalerweise Informationen zur Verfügung, die nicht öffentlich bekannt sind. Was die Hacker betrifft, spielen Innentäter bzw. Täter mit Insiderkenntnissen eine herausragende Rolle. Sicherheitsgutachten können in Ziel, Methodik und Umfang frei bestimmt werden. Ist der Hersteller an der Wirksamkeit bestimmter Sicherheitsmaßnahmen interessiert, so kann er Sicherheitsexperten beauftragen diese mit vorgegebenen Aufwand unabhängig zu untersuchen. In der Praxis können das Tigerteams sein, die in Abstimmung mit dem Auftraggeber Hackerangriffe gegen Netzwerke durchführen, oder Spezialisten können versuchen, Kryptogeräte zu manipulieren, um an intern gespeicherte Schlüssel zu gelangen. Diese freien Gutachten können sehr effektiv sein, ihre Ergebnisse sind aber sehr speziell und kaum vergleichbar.

Für die einzelne Bereiche der Produktklassen gibt es Gütesiegel unabhängiger Prüflabore wie ICSA, West Labs u. a. Diese beurteilen die Funktionalität von Antivirensoftware, Firewalls, Verschlüsselungsgeräten oder PKI-Programme nach eigenen Kriterien. Die deutsche Kreditwirtschaft fordert für alle technischen Komponenten des GeldKarten-Systems, von Geldausgabeautomaten und Datennetzen Sicherheitsgutachten nach spezifischen Kriterien. Die Kreditkartenorganisationen wie VISA oder Mastercard fordern wiederum Sicherheitsgutachten nach eigenen Kriterien. Die Prüfungen erfolgen durch lizenzierte Labore nach unveröffentlichten Verfahren.

Für Kryptomodule zum Schutz sensitiver, aber nicht als Verschlusssache eingestufter Daten wird durch staatliche amerikanische Stellen und zunehmend auch im kommerziellen Bereich eine Validierung nach dem amerikanische Standard FIPS 140-2 [NIST2] gefordert. Der Standard beschreibt in 4 Stufen funktionelle und sicherheitsspezifische Anforderungen kryptographische Techniken und für die Prüfung vorzulegende Informationen. Die Prüfung erfolgt nach [NIST3] durch das NIST lizenzierte Prüflabore. Sie basiert auf einem Konformitätsnachweis und berücksichtigt nur in geringem Maße eine produktspezifische Schwachstellenanalyse. Solche Untersuchungen sind aber für darüber hinausgehende Anforderungen (z. B. für qualifizierte elektronische Signaturen nach deutschem Signaturgesetz) nur bedingt geeignet.

Die Evaluation und Zertifizierung nach den Common Criteria (CC) soll die Universalität des Prüfschemas, sowie die internationale Anerkennung der Sicherheitszertifikate gewährleisten. Der Antragsteller bestimmt in den Sicherheitsvorgaben die zu prüfenden Aspekte der Sicherheitsfunktionalität. Die Schutzprofile ermöglichen aber auch Anwendern und Herstellergruppen verallgemeinerte Sicherheitsanforderungen für Anwendungsbereiche oder Produkttypen zu beschreiben. Der Umfang der Prüfung (die Evaluationsstufe) bestimmt den Umfang der Prüfung und damit die Zuverlässigkeit der Prüfungsergebnisse. Die Vergleichbarkeit und die Nachvollziehbarkeit der Evaluationsergebnisse erfordert einen entsprechende systematische Prüfung und eine umfassende Dokumentation der Ergebnisse. Eine normierte Prüfmethodik trägt zur Wiederholbarkeit und Objektivität der Ergebnisse bei, sie erfordert aber auch die technische Sachkenntnis und das Urteilungsvermögen der Evaluatoren. Um die Konsistenz von Evaluationsbefunden zu verbessern, werden die endgültigen Evaluationsergebnisse einem Zertifizierungsverfahren unterzogen.

4 Vertrauenswürdigkeit und Evaluationsstufe

CC Evaluationen haben drei „Freiheitsgrade“: (1) die in den Sicherheitsvorgaben beschriebene Sicherheitsfunktionalität, (2) das Angriffspotential, gegen den der Evaluationsgegenstand erfolgreich Widerstand leisten soll und das in der Stärke der Funktionen bzw. der Schwachstellenanalyse ausgedrückt wird, sowie (3) den Prüfumfang, der in den Evaluationsstufen und ggf. zusätzlichen Prüfaspekten (Vertrauenswürdigkeitskomponenten) festgelegt wird. Die Sicherheitsfunktionalität wird in den Sicherheitsvorgaben sowohl semiformal als funktionale Sicherheitsanforderungen mittels eines Katalogs [CC], Teil 2, als auch informell als Sicherheitsfunktionen in der EVG-Übersichtsspezifikation beschrieben. Während die funktionalen Aspekte der Evaluation durch die EVG-Übersichtsspezifikation für einen breiten Leserkreis leicht verständlich ist, bedürfen die Evaluationsstufen und das der Bewertung der Wirksamkeit zugrundeliegende Angriffspotential einer näheren Erläuterung.

Bei einer Prüfung auf der Stufe EAL1 werden die Sicherheitsfunktionen auf der Grundlage des Produkts einschließlich der Benutzerdokumentation untersucht. Es werden unabhängige Blackboxtests ohne Schwachstellenanalyse durchgeführt. EAL1-Evaluationen bestätigen somit nur die in den Sicherheitsvorgaben und der Benutzerdokumentation dargestellte Sicherheitsfunktionalität, ohne ihre Wirksamkeit gegen potentielle Angriffe zu bewerten.

EAL2 und EAL3 sind Zwischenstufen, die zusätzliche Informationen über die interne Struktur des Evaluationsgegenstandes und über Herstellertests der Sicherheitsfunktionalität mit einer Analyse unter Berücksichtigung bekannter Schwachstellen verbinden. Diese Prüfstufen sind z. B. für Firewalls und Netzwerklösungen geeignet. Sie sind mit weitverbreiteten Penetrationsangriffen vergleichbar, wobei die Herstellerdokumente die Evaluatoren effektiv unterstützen.

Die Prüfstufe EAL4 verbindet die Untersuchung der Entwicklerdokumentation bis hin zum Quellcode mit Whiteboxtests und mit einer – oft erweiterten und verschärften – Schwachstellenanalyse. Die Herstellerunterlagen, insbesondere die Verfeinerung der Entwicklungsdokumente bis zum Quellcode, ermöglichen eine effektive systematische Analyse ohne aufwendiges Re-Engineering, wie etwa beim „Hacken“ eines Programms. Sie ist notwendig, um auch den Widerstand gegen Angriffe mit hohem Angriffspotential bewerten zu können.

Die höheren Prüfstufen (EAL5 bis EAL7) beinhalten neben rigoroserem Testen die Anwendung formaler Evaluations- und Entwicklungsmethoden für höchste Sicherheitserfordernisse. Sie beinhalten auch ohne Erweiterung eine Bewertung von Angriffen mit mittlerem und hohem Angriffspotential. Sie sind nur für ausgewählte Produkte wie Chipkarten wirtschaftlich durchführbar.

Das Angriffspotential dient der Bewertung potentieller Angriffe [CEM], Anlage B.8. Es bewertet die Vorbereitung und die Durchführung eines Angriffs nach den Faktoren (1) Gesamtzeit, (2) Erfahrung des Angreifers, (3) notwendige Kenntnisse über das Design und die Anwendung des Evaluationsgegenstandes, (4) notwendigen Zugriff auf den Evaluationsgegenstand und (5) notwendige Hilfsmittel. Die Methodik der Schwachstel-

lenanalyse wird ständig weiterentwickelt [AVA]. So wird die Prüfung offensichtlicher Schwachstellen durch Prüfwerkzeuge unterstützt und technologiespezifische Dokumente zu Feststellung konkreter Schwachstellen und die Bewertung des Angriffspotentials erarbeitet (z. B. für Chipkarten [SDA]).

Die Evaluationsmethodik der CC ist mit der Evaluationsmethodik nach ITSEC [ITSEC] in vielen Aspekten vergleichbar [ITSEM], sie weicht aber zum Teil erheblich von der Prüfmethodik der FIPS140-2 ab. So werden für FIPS140-2 bereits auf der Stufe 1 der Quellcode und erst für die Stufe 2 eine funktionelle Spezifikation der äußeren Schnittstellen gefordert. FIPS140-2 schreibt sehr detailliert den physischen Schutz der Hardware-Kryptomodule vor. Für Software-Kryptomodule werden anstelle des physischen Schutzes bestimmter FIPS140-2 Stufen CC-evaluierte Betriebssysteme entsprechender EAL vorgeschrieben, so für die Stufe 2 die EAL2, für Stufe 3 EAL3 und für Stufe 4 EAL4 in Verbindung mit entsprechenden CC-Schutzprofilen. Oft können Ergebnisse der CC-Evaluationen in anderer Form in Gutachten gemäß FIPS140-2, für VISA oder für den Zentralen Kreditausschuss (ZKA) verwendet werden und umgekehrt.

4.1 Beispiel Firewall

Firewalls dienen der kontrollierten und protokollierten Nutzung der Dienste eines Netzwerkes, wobei der eingehende als auch ausgehende Informationsfluss durch die Firewall zugelassen, verhindert und / oder umgeleitet wird. Die Art der Sicherheitsfunktionalität und der Einsatzumgebung, wie wohldefinierte äußere Schnittstellen, ermöglichen sinnvolle Prüfungen ohne umfassende Produktdokumentationen.

Die ICSA Labs verwenden Testkriterien [ICSA] entwickelt, nach denen Firewalls mit automatischen Testtools bzw. Checklisten durch Blackbox-Tests überprüft werden. Eine Mitwirkung des Herstellers ist nur zur Klärung auftretender Fragen vorgesehen. Dieses Vorgehen entspricht etwa einer EAL1-Evaluation der in den Testkriterien aufgelisteten Sicherheitsfunktionen.

Allgemeiner in der geforderten Funktionalität, aber tiefgehender in der Untersuchung ist das Schutzprofil [FW1] der NSA. Es fordert auf der Evaluationsstufe EAL2 zusätzlich zu den Hersteller- und Evaluatortests einen Nachweis der Testabdeckung an den äußeren Schnittstellen (ATE_COV.1), Informationen zum internen Aufbau (ADV_HLD.1) und eine Schwachstellenanalyse (AVA_VLA.1). Allerdings können wegen der geringen zur Verfügung stehenden Information nur bekannte Angriffe mit niedrigem Angriffspotential untersucht werden. Kompliziertere oder sehr produktspezifische Schwachstellen wie ein Buffer Overflow sind so nur schwer feststellbar. (Der interessierte Leser sei z.B. auf [KPSS] und [CER2] verwiesen, in denen der technische Hintergrund von Buffer Overflows erläutert und auf aktuelle praktische Beispiele eingegangen wird.) Für Firewalls in Einsatzumgebungen mit mittlerem Angriffspotential sind deshalb umfangreichere Prüfungen vorgesehen. In den Schutzprofilen [FW2] und [FW3] ist die Evaluationsstufe EAL2 durch die Komponenten ADV_HLD.2 (Sicherheitsspezifischer Entwurf auf hoher Ebene), ADV_LLD.1 (Beschreibender Entwurf auf niedriger Ebene), ADV_IMP.1 (Teilmenge der Implementierung der TSF), ALC_TAT.1 (Klar festgelegte Entwick-

lungswerkzeuge) und AVA_VLA.3 (Mittlere Widerstandsfähigkeit) erweitert. Dadurch können die Evaluatoren z. B. Buffer Overflows bei der Datenübernahme mittels Quellcodeinspektion systematisch untersuchen. Die Verwendung geeigneter Entwicklungswerkzeuge (s. ALC_TAT.1) kann zudem das Risiko von Buffer Overflows bereits im Entwicklungsprozess minimieren.

4.2 Beispiel Hybridverschlüsselung

Hybridmechanismen sind zentrale Bausteine vieler kryptographischer Protokolle, etwa von HBCI oder SSL[26]. Das angestrebte Sicherheitsziel ist der vertrauliche Austausch unverfälschter, authentischer Datensätze. In diesem Beispiel nehmen wir eine vereinfachte Version eines Hybridmechanismus genauer unter die Lupe. Wir setzen voraus, dass jeder Teilnehmer über ein RSA-Schlüsselpaar verfügt, wobei der öffentliche Schlüssel authentisch (z. B. über eine PKI-Infrastruktur) verteilt wird und der private Schlüssel nur dem legitimen Inhaber zur Verfügung steht. Unser Protokollfragment soll ferner das unbemerkte Einspielen alter Nachrichten verhindern (etwa eine zweifache Überweisung beim Homebanking). Nachdem der Absender die gewünschte Nachricht N erzeugt hat, vollzieht er, oder genauer gesagt, dessen Software, folgende Schritte:

1. Die Nachricht N wird mit dem privaten Schlüssel des Absenders digital signiert.
2. Der Zufallszahlengenerator wird aufgerufen, um die Zufallsfolgen I (128 Bit) und K (256 Bit) zu erzeugen.
3. Die Folge K wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt (= Chiffrat 1), nachdem sie mit einem festen Muster (z.B. mit führenden Hexadezimalwerten „F“) von links aufgefüllt und als Binärdarstellung einer natürlichen Zahl interpretiert worden ist.[27]
4. AES-Verschlüsselung der signierten Nachricht N mit dem Sitzungsschlüssel K[28] im CBC-Mode mit dem Initialisierungsvektor I zum Chiffrat 2.
5. Übermittlung der Chiffrate 1 und 2, des Vektors I und einer fortlaufenden Sequenznummer an den Empfänger.

Die Software des Empfängers vollzieht folgende Schritte:

6. prüft, ob die Sequenznummer schon „verbraucht“ ist
7. entschlüsselt Chiffrat 1 und erhält nach Entfernen des bekannten Musters die Zufallsfolge K.
8. entschlüsselt das Chiffrat 2 mit K und I und erhält die signierte Nachricht N
9. Signaturprüfung

Verlaufen die Schritte 6.-9. erfolgreich, setzt das Programm des Empfängers das Protokoll wie vorgesehen fort.

[26] SSL wird u.a. beim Homebanking genutzt.
[27] Dieser Vorgang wird als Padding bezeichnet.
[28] bzw. einer Teilfolge von K

Eine ganz offensichtliche Schwachstelle, die bereits bei einer EAL1-Evaluation entdeckt wird, besteht darin, dass die Sequenznummer offen übertragen und in keinem Zusammenhang zur signierten und verschlüsselten Nachricht steht. Für einen potentiellen Angreifer ist es ein Leichtes, eine zuvor abgefangene und aufgezeichnete alte Nachricht mit einer noch nicht genutzten Sequenznummer zu versehen. Erforderlich ist die Verwendung zufälliger, von Sender und Empfänger geheim gehaltener Sequenznummern (wie die vom Homebanking bekannten TANs), was allerdings einen erhöhten Verwaltungsaufwand bedingt. Werden die noch nicht verwendeten Sequenznummern beim Sender oder Empfänger lokal auf der Festplatte gespeichert, stellen diese Dateien neue potentielle Angriffsziele dar, die aber zumindest schwieriger zu erreichen sind. Am sichersten wäre daher die Einbeziehung der Sequenznummer in das Chiffrat 2.

Bereits eine EAL1-Evaluation könnte aus der Benutzerdokumentation erkennen und durch Tests bestätigen, dass RSA-Schlüssel zu Modullängen von 512 Bit bis 2048 Bit zum Einsatz kommen und der öffentliche Exponent stets 3 beträgt. Aber erst eine Analyse bekannter Schwachstellen (AVA_VLA.2 ab EAL2) würde feststellen, dass, obwohl bereits eine Faktorisierung eines 512 Bit RSA-Moduls mit mittlerem Angriffspotential ausgeschlossen ist, der (für den Schlüsselaustausch mit bekanntem Padding) zu kleine öffentliche Exponent nur für kleine Modullängen unter 768 Bit sicher ist, kurioserweise aber gerade für größere Modullängen die Berechnung der geheimen Schlüssel ermöglicht (s. z. B. [Co][29]). Für einen solchen Angriff wäre ein handelsüblicher Personalcomputer mit einem speziellen, aber ggf. frei im Internet verfügbarem Programm innerhalb weniger Sekunden Rechenzeit erfolgreich (siehe z.B. [Sch]). Tatsächlich konnte auf ähnliche Weise ein von Vanstone und Zuccherato empfohlenes Kryptosystem gebrochen werden (vgl. [Co], Section 11). In unserem Beispiel könnte die Schwachstelle übrigens zuverlässig behoben werden, indem der zum Verschlüsseln des Sitzungsschlüssels K verwendete öffentliche Exponent größer als 3 (z B. 17) gewählt wird oder in Schritt 3 das Padding mit einem bekannten Muster durch das Padding mit zufälligen Werten (z B. PKCS#1) ersetzt wird.

Eine solche Schwachstelle kann gerade bei einem Produktupdate bzw. bei dessen Sicherheitsuntersuchung leicht übersehen werden. Aus gegebenem Anlass (hier: aufgrund der gestiegenen Faktorisierungsleistung) wird das Produkt einer geringen Modifikation unterzogen (hier: Erhöhung der Modulgröße von 512 auf 1024 Bit). Die Versuchung liegt nahe, sich ausschließlich auf das primäre Ziel der Modifikation zu konzentrieren, ohne auf überraschende „Seiteneffekte“ zu achten.

Eine Evaluation auf höherer Evaluationsstufe würde ggf. weiterhin feststellen, dass ein schwacher deterministischer Zufallsgenerator in Schritt 2 eine Berechnung des Sitzungsschlüssels K aus dem unverschlüsselt übertragenen Initialisierungsvektor I ermöglicht (z. B. lineare Funktion über dem Zustand eines linearen Schieberegisters mit 63 Bit Länge). Dieser funktionale Zusammenhang könnte erst aus der Beschreibung des Schritts 2, z. B. bei ITSEC E2 im Feinentwurf oder bei CC EAL4 im Entwurf auf niedri-

[29] In diesem besonderen Fall (öffentlicher Schlüssel = 3, Modullänge > 768 Bit) ist es möglich, ein Polynom mit ganzzahligen Koeffizienten zu konstruieren, für das der String K (aufgefasst als Binärdarstellung einer natürlichen Zahl) Nullstelle über Z ist. Ein solches Nullstellenproblem ist aber leicht zu lösen.

ger Ebene oder im Quellcode, erkennbar sein. Einfache statistische Tests wie z. B. in [Mar] beschrieben, sind dazu nicht in der Lage. Für Evaluationen sind deshalb spezifische Nachweise gefordert ([AIS20]). Ein hochwertiger deterministischer oder ein physikalischer Zufallsgenerator würden für Angreifer nutzbare funktionale Zusammenhänge zwischen K und I ausschließen. Zur Beurteilung von Angriffen mit hohem Angriffspotential auf derartige Zufallsgeneratoren sind allerdings ebenfalls tiefergehende Untersuchungen notwendig ([AIS20], [AIS31], [KS], [SK]).

Die FIPS 140-2 konzentriert sich auf die Verwendung vom NIST bestätigter Kryptomechanismen, während proprietäre Lösungen im allgemeinen nicht tiefergehend untersucht werden.

4.3 Beispiel Analyse der Stromaufnahme bei Chipkarten

Die technische Implementierung eines kryptographischen Algorithmus kann sowohl über ihre datenabhängige Energieaufnahme als auch wegen unerwünschter Energieabgabe (Stichwort Tempest) angegriffen werden. Die Ausnutzung dieser allgemeinen Schwachstelle wurde in [Ko] erstmals für Chipkarten als SPA („Simple Power Analysis“) und DPA („Differential Power Analysis“) veröffentlicht. Die passive Informationsgewinnung kann auf die elektromagnetische Abstrahlung und das zeitliche Verhalten der Prozesse erweitert werden. Zusammen mit der Analyse des Verhaltens im Fehlerfall bilden sie die Side Channel Cryptanalysis.

Die erste DPA beruhte auf allgemeinen statistischen Methoden und war bei Chipkarten ohne spezielle Gegenmaßnahmen als reine Black-Box-Angriffe nur bei Kenntnis der externen Schnittstellen erfolgreich. Mit der Einführung von Hard- und Software-Gegenmaßnahmen zur Verschleierung der Stromaufnahme mussten die statistischen Methoden verfeinert und angepasst werden. Power Analysis gehört heute auch bei niedrigen Evaluationsstufen (EAL1 erweitert bis EAL3) zum Standard der Schwachstellenanalyse, da sie bei niedrigem bis mittlerem Angriffspotential ohne Kenntnisse der internen Implementierung möglich, wenn auch nicht immer erfolgreich ist.

Allerdings zeigt sich, dass DPA-Angriffe auch für bestimmte Implementierungsmethoden und deren typische Gegenmaßnahmen entwickelt werden können (s. [BLW]). Die dazu notwendigen Informationen sind bei speziellen Gegenmaßnahmen als Expertenwissen einzustufen, das für höhere Evaluationsstufen bereit gestellt wird (bei CC ab EAL4 im Entwurf auf niedriger Ebene oder im Quellcode). Einige veröffentlichte Gegenmaßnahmen können allerdings auch durch SPA identifiziert werden.

Side Channel Attacken sind nicht auf Chipkarten begrenzt. Insbesondere Schwachstellen im Zeitverhalten kryptographischer Protokollimplementierungen sind veröffentlicht worden ([Bl], [CERT2]). Bereits [NIST1] wies auf die Notwendigkeit hin, die Korrektheit kryptographischer Berechnungen zu kontrollieren, bei festgestellten Fehlern die Verarbeitung zu stoppen und die Datenausgabe zu blockieren (s. [BLD], [BS]). Side Channels werden in FIPS140-2 [NIST2] explizit als potentielle Schwachstelle von Kryptomodulen angegeben (mitigation of other attacks) und sind - falls relevant - zu

untersuchen [NIST3]. Die Analyse und Bewertung von Side Channel Attacken stellt insbesondere bei hohem Angriffspotential (z. B. bei Signaturchipkarten) sehr hohe Anforderungen an Hersteller und Evaluatoren.

5 IT-Systeme

Der Einsatz geprüfter sicherer IT-Komponenten ist aber nur eine Voraussetzung für sichere IT-Systeme. In der Praxis sind vielfältige technische, organisatorische und personelle Sicherheitsmaßnahmen zu treffen, um die Sicherheit der Anwendungen zu gewährleisten. Die Produktevaluation kann in der Betriebsdokumentation die Maßnahmen zum sicheren Betrieb nur beschreiben, umsetzen müssen es die Anwender selbst. Das IT-Grundschutzhandbuch ([GSH]) mit seinen Empfehlungen zu Standard-Sicherheitsmaßnahmen stellt einen Quasi-Standard für IT-Sicherheit dar. Für das Sicherheitsmanagement gibt ISO 17799 wertvolle Orientierung. Die tatsächlich erreichte Sicherheit eines IT-Systems im Wirkbetrieb sollte ebenfalls geprüft werden. Dies kann durch Systemverantwortliche intern geschehen, die ggf. durch externe Sicherheitsexperten als Tigerteam oder Berater unterstützt werden. Die dadurch festgestellten Schwachstellen müssen bewertet und durch zusätzliche Maßnahmen begegnet werden.

Die Einhaltung der Sicherheitsstandards kann durch Zertifikate auf der Basis von Audits bestätigt werden. Aber auch hier gilt, dass IT-Sicherheit kein Zustand, sondern ein Prozess ist. Für Produktevaluationen wurde hier ein Konzept zum Erhalt der Vertrauenswürdigkeit bei der Weiterentwicklung der Produkte entwickelt [AMA]. Die dort entwickelten Ideen, wie z. B. die Kombination von Untersuchungen eines Sicherheitsanalytikers des Herstellers und deren regelmäßige Kontrolle durch die Prüfstelle und die Zertifizierungsstelle, können auch auf IT-Systeme nutzbringend angewandt werden.

6 Schlussfolgerungen

IT-Sicherheitsprüfungen sollen das Vertrauen in die Sicherheit der eingesetzten Produkte und Systeme begründen. Es liegt im Interesse der Hersteller, nicht nur sichere Produkte anzubieten, sondern deren Sicherheit auch durch eigene und unabhängige Prüfungen nachzuweisen. Die Sicherheitsgutachten können und sollen dem Anwender das Vertrauen in die Sicherheit der Produkte vermitteln. Eine normierte Analysemethodik fördert die Systematik, die Zuverlässigkeit und die Aussagekraft der Prüfungsergebnisse.

Es gibt verschiedene Konzepte, Sicherheitsprüfungen zu gestalten. Welche Schwachstellen letztlich entdeckt werden, hängt, die korrekte Durchführung der Prüfung vorausgesetzt, entscheidend von der Art und der Prüftiefe der Untersuchung ab. Allerdings betrifft dies in demselben Maß den zeitlichen Aufwand und damit die Kosten, die mit deren Durchführung verbunden sind. Die behandelten Beispiele zeigen, dass bereits niedrige Evaluationsstufen wesentliche Schwachstellen aufzeigen und zur Abwehr von Angriffen mit niedrigem Potential ausreichend sein können. Dem angestrebten Ausschluss aller praktisch relevanten Schwachstellen zum Schutz wichtiger

Werte, wie z. B. eines Schlüssels für qualifizierte Signaturen, sind umfangreiche Prüfungen unumgänglich.

Literaturverzeichnis

[AIS20] Bundesamt für die Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 1 (02.12.1999), http://www.bsi.bund.de/zertifiz/zert/interpr/ais20.pdf

[AIS31] Bundesamt für Sicherheit in der Informationstechnik: Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1 (25.09.2001), http://www.bsi.bund.de/zertifiz/zert/interpr/ais31.pdf

[AMA] CCIMB-2001/0032R Evaluation Methodology Supplement: AMA - Assurance Maintenance, Version 0.9, Feb. 2003, http://www.commoncriteria.org/review_docs/index.html

[AVA] CCIMB-2002-07-001 Supplement: Vulnerability Analysis and Penetration Testing Version 0.68 July 2002, http://www.commoncriteria.org/review_docs/index.html

[Bl] D. Bleichenbacher: Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS # 1. In (H. Krawczyk (Hrsg.)) Advances in Cryptology - Crypto 98. Springer, LNCS, Vol. 1462, Berlin 1998, 1-12.

[BLD] Dan Boneh, Richard Lipton, Rich DeMillo: On the Importance of Checking Cryptographic Protocols for Faults. In (W. Fumy (Hrsg.)) Advances in Cryptology – Eurocrypt' 97, Springer, LNCS, Vol. 1233, Berlin 1997, pp. 37-51.

[BLW] B. den Boer, K. Lemke, G. Wicke: A DPA Attack against the Modular Reduction within a CRT Implementation of RSA. In (B.S. Kaliski Jr., C.K. Koc, C. Paar (Hrsg.)) Cryptographic Hardware and Embedded Systems – CHES 2002. Springer, LNCS, Vol. 2523, Berlin 2003, 228-243.

[BS] E. Biham, A. Shamir: Differential Fault Analysis of Secret Key Cryptosystems. In (B.S. Kaliski Jr. (Hrsg.)) Advances in Cryptology - Crypto '97. Springer, LNCS, Vol. 1294, Berlin 1997, 513-525.

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3; Version 2.1, August 1999 and ISO 15408:1999, http://www.commoncriteria.org/cc/cc.html

[CCPL] Liste evaluierter Netzwerkprodukte http://www.commoncriteria.org/ccc/epl/productType/eplinfo.jsp?id=3

[CEM] Common Methodology for Information Technology Security Evaluation CEM-99/045, Part 2: Evaluation Methodology, Version 1.0 (August 1999), http://www.commoncriteria.org/cem/cem.html

[CER1] CERT Vulnerability Note VU#210937 IBM Tivoli Firewall Toolbox contains vulnerability, s. http://www.kb.cert.org/vuls/id/210937

[CER2] CERT Vulnerability Note VU#997481 Cryptographic libraries and applications do not adequately defend against timing attacks, s. http://www.kb.cert.org/vuls/id/997481

[Co] D. Coppersmith: Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J. Crypt. 10 (no. 4), (1997), 233-260.

[CSL] A.B. Cremers, A. Spalka, H. Langeweg: Vermeidung und Abwehr von Angriffen Trojanischer Pferd Programme auf Digitale Signaturen. In: 7. Deutscher IT-Sicherheitskongress des BSI (Tagungsband), SecuMedia Verlag, Ingelheim 2001, 113-125.

[FW1] U. S. Department of Defense: Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April , 1999, http://www.commoncriteria.org/ppRpt/firewalls_traffic_medium.pdf

[FW2] U. S. Department of Defense: Application-level Firewall Protection Profile for Medium Robustness Environments, Version 1.0, June 28, 2000, http://www.commoncriteria.org/ppRpt/firewalls_app_medium.pdf

[FW3] U. S. Department of Defense: Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, Version 1.0, May 1, 2000, http://www.commoncriteria.org/ppRpt/firewalls_traffic_medium.pdf

[GH] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch, Stand Juli 2002.

[ICSA] ICSA Labs: Modular Firewall Product Certification Criteria version 4.0, TruSecure corporation, s. http://www.icsalabs.com/html/communities/firewalls/certification/criteria/criteria_4.0.shtml

[ITSEC] Europäische Gemeinschaften – Kommission: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), 1991, http://www.bsi.bund.de/zertifiz/itkrit/itsec.htm

[ITSEM] Europäische Gemeinschaften – Kommission: Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), 1994, http://www.bsi.bund.de/zertifiz/itkrit/itsec.htm

[KS] W. Killmann, W. Schindler: Ein Vorschlag zu: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.1 (25.09.2001), mathematisch-technische Referenz zu [AIS 31], http://www.bsi.bund.de/zertifiz/zert/interpr/trngkr31.pdf

[Ko] P. Kocher, J. Jaffe and B. Jun: Differential Power Analysis. In (M. Wiener Hrsg.)) Advances in Cryptology – CRYPTO '99, Springer, LNCS, Vol. 1666, Berlin 1999, 388-397.

[KPSS] S. Kallnik, D. Pape, D. Schröter, Stefan Strobel: Das Sicherheitsloch Buffer-Overflows und wie man sich davor schützt. In Computertechnik c't 23/01, 216 ff.

[Mar] G. Marsaglia: Diehard (Test Suite for Random Number Generators). www.stat.fsu.edu/~geo/diehard.html

[MDS] T. S. Messerges, E. A. Dabbish, R. H. Sloan: Investigations of Power Analysis Attacks on Smartcards, USENIX Workshop on Smartcard Technology, USENIX Association, 1999, 151-161.

[NIST1] NIST: Federal Information Processing Standards Publication Security Requirements For Cryptographic Modules FIPS Pub 140-1 (11-01-1994), http://csrc.nist.gov/cryptval/

[NIST2] NIST: Federal Information Processing Standards Publication Security Requirements For Cryptographic Modules FIPS Pub 140-2 (12-03-2002), http://csrc.nist.gov/cryptval/

[NIST3] NIST: Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules February 12, 2003 Draft, http://csrc.nist.gov/cryptval/

[NIST4] NIST Computer Security Division's Cryptographic Toolkit http://csrc.nist.gov/CryptoToolkit/

[Sch] R. Schunk: RSA-Verschlüsselung mit kleinen Exponenten. Diplomarbeit, TU Darmstadt, Fachbereich Mathematik, 1999.

[SDA] Common Criteria Supporting Documents: Application of Attack Potential to Smartcards, Version 1.1, July 2002, http://www.commoncriteria.org/supporting_docs/index.html

[SK] W. Schindler, W. Killmann: Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications. In (B.S. Kaliski Jr., C.K. Koc, C. Paar (Hrsg.)) Cryptographic Hardware and Embedded Systems – CHES 2002. Springer, LNCS, Vol. 2523, Berlin 2003, 431-449.