Seitenkanalangriffe und Hardware-Security-Modules

Zusammenfassung von Mick Dahlhaus und Daniel Bachmann

Was sind Seitenkanalangriffe?

Ein Seitenkanalangriff ist eine Methode der Kryptanalyse (dem Gewinnen von Informationen aus verschlüsselten Texten, ohne den Schlüssel zu besitzen). Hierbei wird nicht das kryptographische Verfahren selbst angegriffen, sondern seine physische Implementierung auf einem Endgerät, bspw. einer Chipkarte, einem Security-Token oder einem HSM (siehe unten). Bei Seitenkanalangriffen gibt es eine Vielzahl von Angriffsvektoren, wie z.B. eine Kamera, welche auf das Pin-Eingabefeld gerichtet ist, einen Keylogger der den Klartext direkt bei der Eingabe abfängt oder das aufgeschriebene Passwort was am Bildschirmrand klebt. Im Folgenden werden einige nicht-triviale Angriffsvektoren erläutert, welche aber nur den Tellerrand dieses Themas darstellen.

Passive Angriffe

Ein passiver Angriff stört nicht den Ablauf des kryptographischen Verfahrens und gewinnt meist Informationen aus der Kombination des Ergebnisses einer Analyse und Informationen über die jeweilige Eingabe oder Zustand des verwendeten Verfahrens.

1) Simple Power Analysis (SPA)

Eine einfache Poweranalyse beobachtet den Energieverbrauch der Hardware bei der Ausführung des kryptographischen Verfahrens. Als Beispiel sei hier die Nutzung von RSA gegeben. Square-and-multiply Operationen bei RSA verbrauchen, je nachdem ob sie nur “squaren” oder “squaren” und “multiplyen”, verschiedene Mengen an Energie. Diese kleinen Unterschiede können schon mit einem handelsüblichen Oszilloskop beobachtet werden und ermöglichen Rückschlüsse auf die Eingabe.

2) Differential Power Analysis (DPA)

Ähnlich wie bei SPA wird hier der Energieverbrauch analysiert. Jedoch ist diese Attacke etwas raffinierter und komplexer, da sie eine statistische Analyse über mehrere Schritte des kryptographischen Verfahrens macht. Deswegen gibt es bei der DPA auch Möglichkeiten zur Fehlerkorrektur und Signalverarbeitung, was ihr die Fähigkeit verleiht, auch Messungen zu analysieren, die für die SPA zu ungenau oder verwaschen sind.

3) Sound Analysis

Eine Analyse der Betriebsgeräusche (Spulenfiepen, Vibration von Bauelementen etc.) kann, ähnlich wie bei der SPA, zu Rückschlüssen auf den verwendetet RSA-Schlüssel führen. Hierbei kann schon mit einem handelsüblichen Handymikrofon, das knapp 30 cm von dem Gerät entfernt platziert wurde und die entsprechende Software besitzt, ein ansonsten sicherer RSA-Schlüssel extrahiert werden.

4) Timing Attack

Dieser Angriff misst die Rechenzeit des implementierten Verfahrens für unterschiedliche Eingaben. Die Veränderungen in der Zeit ermöglichen dann einen Rückschluss (ähnlich SPA und DPA) auf den verwendeten Schlüssel oder die Eingabedaten.

5) Van-Eck-Phreaking (Tempest)

Die von einem Gerät produzierte elektromagnetische Strahlung lässt sich noch auf einige Entfernung messen (ca. 100 m) und erlaubt Rückschlüsse auf die durchgeführten Operationen. Besonders hiervon betroffene Geräte sind Computerbildschirme (DVI, HDMI und LCD) und ungeschirmte Datenleitungen. Dieses Wissen kann genutzt werden, um Datenverkehr am Endgerät abzuhören. Besonders das Videosignal kann hier effektiv rekonstruiert werden. Aber auch Stromschwankungen bei unterschiedlichen Operationen in Kombination mit einer SPA oder DPA bieten hier eine große Angriffsfläche. Das Wort Tempest (ehemals ein Lauschprogramm der NSA) steht heute für ein Gütesiegel, das genau gegen solche Angriffe schützt.

6) Shared Memory

Prozesse, die auf demselben Gerät durchgeführt werden, teilen sich möglicherweise dieselben Speicherbereiche (einzelne Register, Cache oder ganze Blöcke). Hier kann also der benutzte Speicher von einem Prozess Rückschluss auf den anderen Prozess ermöglichen oder sogar Zugriff auf sonst beschränkte Daten erlauben. Ein prominentes Beispiel ist die Sicherheitslücke “Spectre”, bei der ausgenutzt wurde, dass der Prozessor durch “Out-of-order” execution (nach Konditionierung durch häufiges Aufrufen einer bestimmten Speicherzelle) Zugriff auf sonst durch Sicherheitsmechanismen geschützte Daten erlaubte.

7) Bug Attack

Eine Bug Attack zielt auf die fehlerhafte Implementierung einer Funktion in Mikroprozessoren ab. In den meisten Anwendungen ist ein solcher Bug nicht relevant, bei kryptographischen Anwendungen wie RSA oder der ElGamal Verschlüsselung kann jedoch eine einzige falsche Berechnung den Schlüssel preisgeben.

Aktive Angriffe

Ein aktiver Angriff stört oder manipuliert das Verfahren von außen, um so Fehler zu provozieren, die Rückschlüsse auf den verwendeten Schlüssel ermöglichen.

1) Differential Fault Analysis (DFA)

Ähnlich einer Bug Attack wird hier das Fehlverhalten von Hardware ausgenutzt, jedoch werden keine Fehler der Hersteller oder Ingenieure ausgenutzt, sondern aktiv Fehler von außen hinzugefügt. Angriffsvektoren sind unter anderem: Veränderung der Spannung, Manipulation der Systemuhr, Strahlung oder ein Resetimpuls zum falschen Zeitpunkt. Derselbe Klartext wird dann einmal unter normalen Bedingungen und einmal unter Manipulation von außen verschlüsselt. Die entstandenen Chiffrentexte werden dann verglichen und Unterschiede in den Bits erlauben Rückschlüsse auf bspw. den Schlüssel. Eine Zerstörung der Hardware ist bei diesem Angriff eine reelle Möglichkeit.

2) Electromagnetic Fault Injection (EMFI)

EMFI versucht gezielt, die Ergebnisse von Securitychecks zu manipulieren oder sogar ganz zu überspringen. Hierzu wird ein Werkzeug eingesetzt, welches das Gerät (sehr punktuell) einer hohen Stromspannung aussetzt. Dies kann persistente Änderungen wie Bitflips in Registern provozieren oder aber kurzzeitige Fehler bei Abfragen hervorrufen, die dann ein falsches Ergebnis liefern. So können Sicherheitsroutinen, ohne jemals durchgeführt zu werden, umgangen werden.

3) Cold Boot Attack

Bei der Cold Boot Attack wird das Phänomen der Datenremanenz ausgenutzt. Ladungen in bspw. RAM-Modulen verflüchtigen sich nicht sofort bei der Systemabschaltung, sondern benötigen teilweise Sekunden bis Minuten, um das System vollständig zu verlassen. Eine Kühlung der Speichermodule verstärkt diesen Effekt dramatisch. Nun muss man sich noch Zugriff auf diese Daten beschaffen, indem man die Speicherelemente aus dem System entfernt oder ausliest. Die Analyse dieser gewonnenen Daten kann Rückschlüsse auf den verwendeten Schlüssel ermöglichen.

Hardware Security Modules (HSM)

Einleitung

Hardware Security Modules (deutsch: Hardware Sicherheitsmodule, HSM) sind Hardwareprodukte, die kryptographische Operationen in einer sicheren und effizienten Umgebung ermöglichen. Dazu gehört die sichere Erstellung und Verwaltung von Schlüsseln. Weitere Funktionen sind die symmetrische und asymmetrische Ver- und Entschlüsselung, digitale Signaturen, Hash Funktionen und die Generierung von echten Zufallszahlen oder Pseudozufallszahlen.

Das erste HSM wurde 1989 von IBM für militärische Zwecke entwickelt. Anschließend kam es vor allem im Bereich von ATMs (Automated Teller Machines) zum Einsatz. Heutzutage gibt es viele weitere Anwendungsbereiche.

Physikalische Sicherheit - Schutz vor Angriffen

1) Power Analysis

In der Firmware der HSMs sind die kryptographischen Verfahren so implementiert, dass die Rechenoperationen immer gleich viel Energie benötigen, wodurch die Power Analysis keine Rückschlüsse auf die Eingaben ziehen kann.
Eine weitere Schutzmaßnahme sind Kondensatoren, die bei hohem Energieverbrauch die auftretenden Stromspitzen abgefangen, wodurch der erhöhte Energieverbrauch nach außen nicht mehr zu erkennen ist.

2) Timing Attack

Die kryptographischen Algorithmen sind in der Firmware so implementiert, dass die Rechenoperationen eine konstante Dauer haben. Somit führen verschiedene Eingaben zur selben Rechenzeit. Dadurch lassen sich keine Rückschlüsse auf verwendete Schlüssel ziehen.

3) Cold Boot Attack

Die Temperatur des HSMs wird fortlaufend gemessen. Sinkt die Temperatur unter einen bestimmten Wert, kommt es zu einer Nullstellung. Unter einer **Nullstellung** (engl. “Zeroisation”) versteht man das Löschen von sensiblen Parametern (z.B. Schlüsseln) aus einem kryptographischen Modul, um die Offenlegung zu verhindern.

4) physischer Angriff

Um zu verhindern, dass sich Angreifer physischen Zugang zu den einzelnen Komponenten des HSMs verschaffen (z.B. mithilfe spezieller Werkzeuge oder Säure) und diese anschließend auswerten, bietet ein HSM folgende Maßnahmen:

- Ein Siegel auf dem Deckel des HSMs, welches bei physischem Zugang automatisch zerstört wird und somit einen Angriff sichtbar macht
- Die Platine wird mit einer Vergussmasse aus Harz geschützt. Versucht man das Harz zu entfernen, wird die Platine wahrscheinlich ebenfalls zerstört
- Die Platine kann mit einem Metallkörper geschützt werden, der die einzelnen Komponenten verdeckt. Der Metallkörper kann mit einem Schalter oder einem

Lichtsensor kombiniert werden, die eine Nullstellung auslösen, sobald der Metallkörper entfernt wurde, bzw. sobald Licht an die Platine kommt (weil der Körper entfernt wurde)

- Das HSM kann mit einer Sensorfolie aus verschränkten Leiterbahnen ummantelt werden. Sobald bei einem Angriff eine Leiterbahn durchtrennt wird, kommt es zur Nullstellung

Standards

Es gibt verschiedene Standards, die die nötigen Anforderungen an ein HSM regeln. Der wichtigste Standard ist FIPS 140 - 2 (Federal Information Processing Standards) vom NIST (National Institute of Standards and Technology). Er beschreibt die Sicherheitsanforderungen an ein kryptographisches Modul in vier Leveln mit ansteigenden Anforderungen. Jedes Level erfordert die Erfüllung aller Level darunter.

1. Level: Es wird mindestens ein korrekt implementierter kryptographischer Algorithmus verwendet
2. Level: Physikalische Angriffe müssen nachweisbar sein. Außerdem ist im Hardwaremodul eine rollenbasierte Authentifizierung der Nutzer implementiert
3. Level: Das Modul bietet einen Schutz, bzw. Widerstand gegen Angriffe. Außerdem werden Angriffe erkannt und anschließend darauf reagiert. Die rollenbasierte Authentifizierung wird durch die Identifizierung der Nutzer erweitert
4. Level: Für das höchste Level benötigt es eine Schutz-Ummantelung des kompletten Moduls, um Angriffe zu erkennen und darauf zu reagieren. Außerdem muss ein Schutz vor Temperaturen und Spannungen außerhalb des normalen Betriebs vorhanden sein, wodurch Level 4 Module besonders geeignet sind für die Nutzung in einer physisch ungesicherten Umgebung.

Ein Standard HSM befindet sich in Level 3, fortgeschrittene HSMs bedienen Level 4. Die Anforderungen bezüglich Authentifizierung und Identifizierung der Nutzer eines HSMs zeigen, dass nicht nur physikalische Schutzmaßnahmen wichtig sind. Außerdem ist sichere Infrastruktur wichtig, dazu gehört unter anderem der Schutz der Serverräume, verschlüsselte Kommunikation und strenge Regeln zur Verwendung der Schlüssel. Hierbei handelt es sich jedoch nicht um HSM-spezifische Maßnahmen, sondern um wichtige, allgemeine Sicherheitsmechanismen.

Anwendungsbereiche

HSMs haben viele verschiedene Anwendungsbereiche (Automobil-Industrie, Militär, Telekommunikation, Lotterie, etc.). Hier sind nur zwei Beispiele:

Banken

Mithilfe von HSMs kontrollieren Banken, ob eine eingegebene PIN mit der PIN übereinstimmt, die die Bank für diese Karte gespeichert hat. Außerdem ermöglicht ein HSM die sichere Überprüfung von Kredit-/Debitkarten-Transaktionen durch Kontrolle der Sicherheitscodes der Karten.

Zertifizierungsstellen

Die Zertifizierungsstellen, die z.B. X.509 Zertifikate (siehe elektronische Signaturen, Transport Layer Security - TLS) ausstellen, nutzen HSMs zum Generieren, Speichern und Verwalten von asymmetrischen Schlüsselpaaren.