FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Seitenkanalangriffe & Hardware Security Modules

Mick Dahlhaus und Daniel Bachmann

19.01.2022

Aufteilung

Aufteilung des Vortrags:

Teil 1 - Seitenkanalangriffe

Teil 2 - Hardware Security Modules

Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe
- Passive Angriffe
- Aktive Angriffe

Was sind Seitenkanalangriffe ?

Ein Werkzeug der Kryptanalyse.

Ein Angriff, der nicht auf das kryptographische Verfahren selbst abzielt, sondern auf dessen physische Implementierung.

Inhaltsverzeichnis

Teil 1

Was ist ein passiver Angriff ?

Ein passiver Angriff:

- Stört den Ablauf des Verfahrens nicht.
- Kombiniert (meist) Informationen aus Analyse und Ablauf.
- Kann gut zum Abhören genutzt werden.

Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe

- Passive Angriffe

- Aktive Angriffe

Was ist eine **S**imple **P**ower **A**nalysis ?

Analyse des Energieverbrauches.

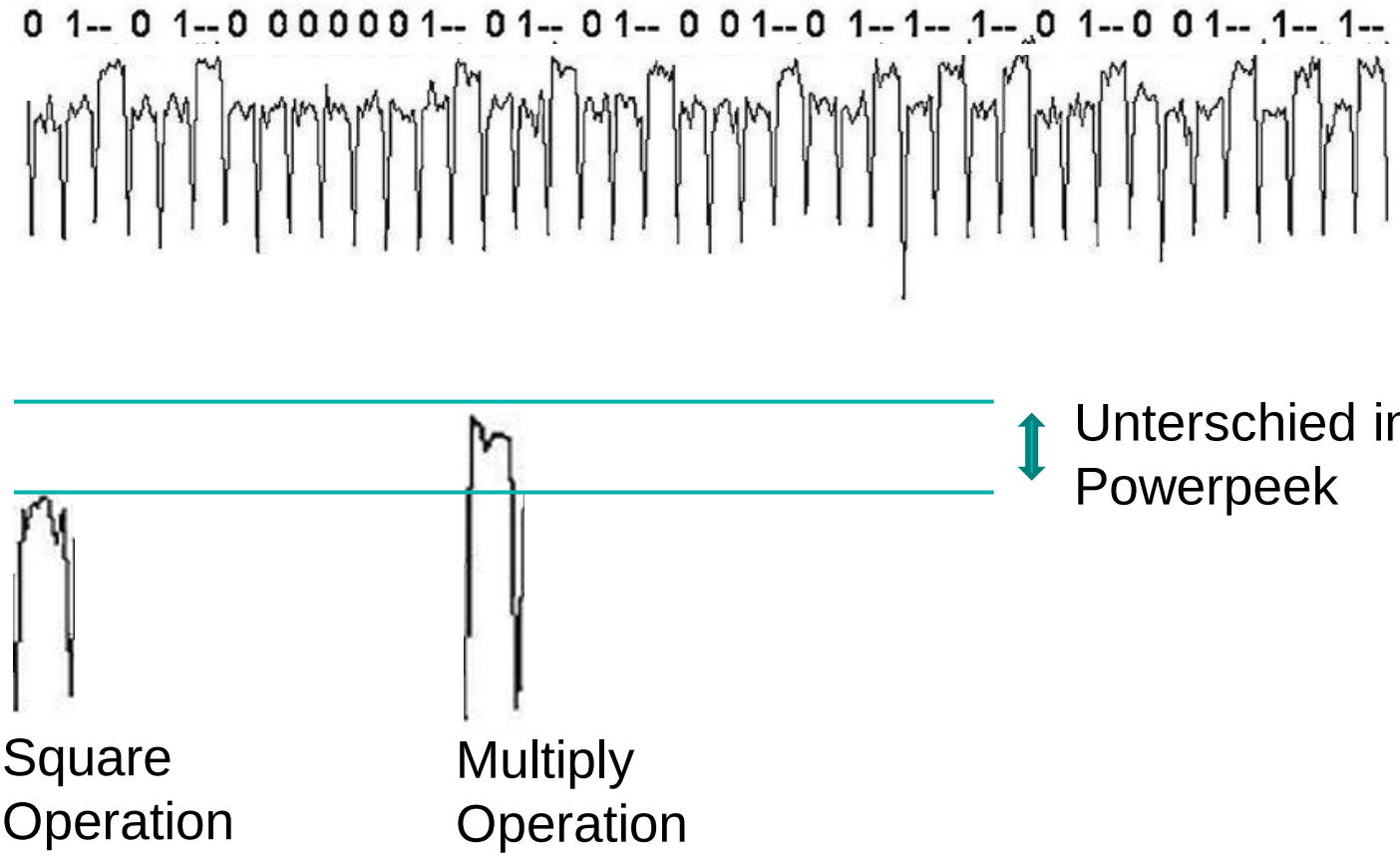
Beispiel an Square-and-multiply bei RSA:

$$m = c^d \bmod n$$

Exponent ***d*** wird als Binärzahl interpretiert.

1 = Square-and-multiply
0 = Square

Passive Angriffe
SPA



Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe

- Passive Angriffe

    1) SPA
    2) DPA
    3) Sound Analysis
    4) Timing Attack
    5) Van-Eck-Phreaking
    6) Shared Memory
    7) Bug Attack

- Aktive Angriffe

Was ist eine **D**ifferential **P**ower **A**nalysis?

Ähnlich der SPA in der Vorgehensweise aber:

- Mehrere Schritte des Verfahrens.
- Analyse des Energieverbrauchs als Datensatz.
- Ermöglicht Fehlerkorrektur & Signalverarbeitung.
- Ist „robuster“ im Bezug auf die zu verarbeiteten Daten.

Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe

- Passive Angriffe

    1) SPA
    2) DPA
    3) Sound Analysis
    4) Timing Attack
    5) Van-Eck-Phreaking
    6) Shared Memory
    7) Bug Attack

- Aktive Angriffe

Was ist eine Sound Analysis?

Die Quelle der Information ist hier:

- Spulenfiepen einzelner Komponenten.
- Vibration von Bauelementen.

Wird in Kombination mit einer SPA oder DPA genutzt.

Aber auch triviale Quellen:

- Tastaturklicken
- Druckergeräusche

Inhaltsverzeichnis

Teil 1

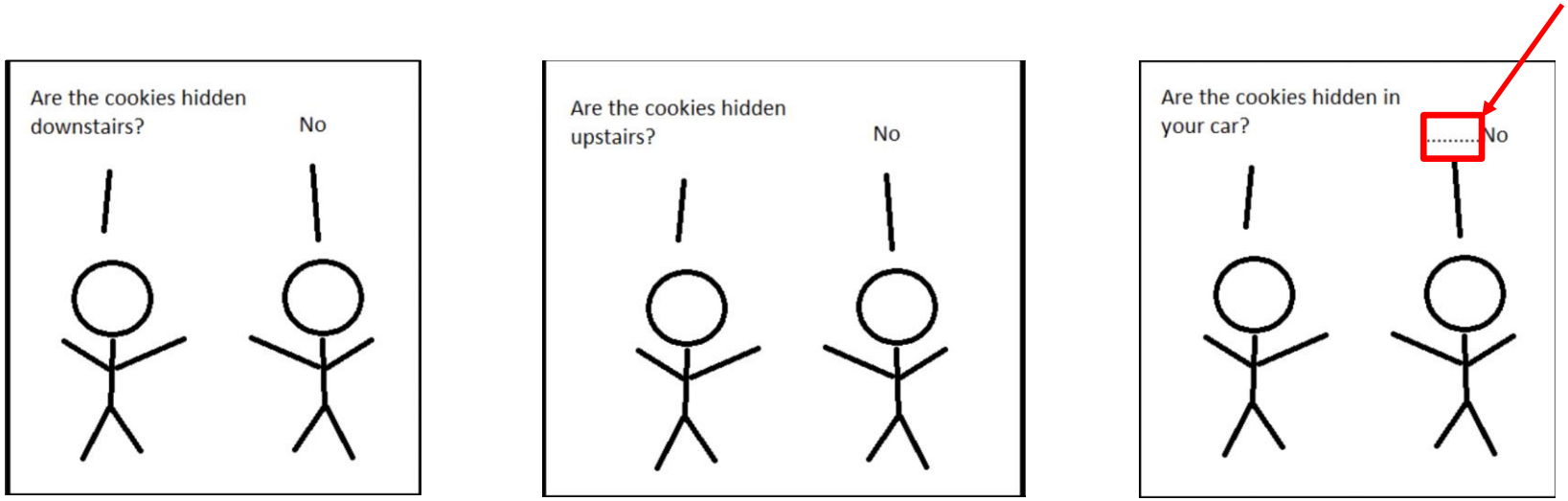
- Seitenkanalangriffe

- Passive Angriffe

    1) SPA
    2) DPA
    3) Sound Analysis
    4) Timing Attack
    5) Van-Eck-Phreaking
    6) Shared Memory
    7) Bug Attack

- Aktive Angriffe

Was ist eine Timing Attack?



Unterschiedliche Operationen brauchen unterschiedliche Mengen an Zeit.

Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe

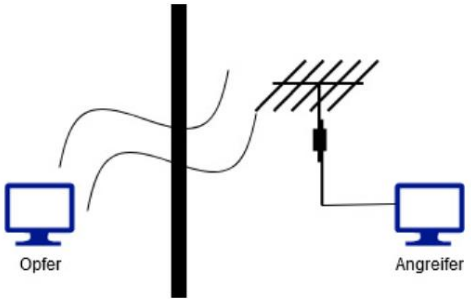
- Passive Angriffe

    1) SPA
    2) DPA
    3) Sound Analysis
    4) Timing Attack
    5) Van-Eck-Phreaking
    6) Shared Memory
    7) Bug Attack

- Aktive Angriffe

Was ist Van-Eck-Phreaking ?

Auch bekannt unter dem Namen Tempest.
Elektromagnetische Strahlung nach 100 m immer noch Messbar.



Angreifbar:

- Ungeschützte Datenleitungen und Videosignale (HDMI, DVI etc.).
- Stromschwankungen auch analysierbar mittels SPA oder DPA.
- Direkt unverschlüsselt am Endgerät mitlesen.

Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe

- Passive Angriffe

    1) SPA
    2) DPA
    3) Sound Analysis
    4) Timing Attack
    5) Van-Eck-Phreaking
    6) Shared Memory
    7) Bug Attack

- Aktive Angriffe

Was ist eine Shared Memory Attack?

Mehrere Prozesse teilen sich dieselben Speicherregister, Blöcke oder Cache.

Benutzter Speicher von einem Prozess kann also Rückschlüsse auf den anderen ermöglichen.

Ein Beispiel dafür ist:

- Sicherheitslücke aus 2018
- Nutzt:
  spekulative Ausführung
  &
  Out-of-order execution

Spectre als Beispiel

```
//Ziel ist Register 10
int targets[] = {1,2,3,4,5,6,7,8,9,10};

//Besitzen wir nur bis Register 9
int accessRights;

//Zeigt auf unser Ziel
int* pointerToTarget;

void victim(int x){

  //Komplexer Sicherheitscheck
  if(isValid(acessRights)){

    //Zieldaten
    tmp = targets[x];

  }

}
```

1) Konditionierung des Prozessors.
2) x wird hochgezählt.
3) x erreicht unser Zielregister.
4) Prozessor lädt gutmütig Register 10 vor.
5) Securitycheck schlägt fehl.

Selbst wenn der Prozessor das Out-of-order Ergebnis verwirft bleibt aufgrund der Datenremanenz Information über das Zielregister vorhanden.

Inhaltsverzeichnis

Teil 1

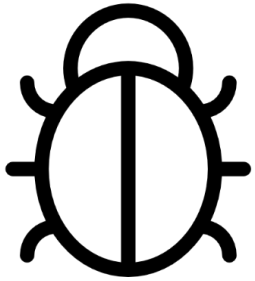
- Seitenkanalangriffe

- Passive Angriffe

    1) SPA
    2) DPA
    3) Sound Analysis
    4) Timing Attack
    5) Van-Eck-Phreaking
    6) Shared Memory
    7) Bug Attack

- Aktive Angriffe

Was ist eine Bug Attack?



Eine einzelne falsche Berechnung kann den Schlüssel preisgeben.

Bug Attacks nutzen vorhandene Fehlimplementierungen von berechnenden Befehlen aus.

Divisionen und Multiplikationen als Ziel aufgrund deren Optimierung.

Meist wird hierbei eine Chosen Cipher Text Attacke angewendet um den Bug auszunutzen.

Mehr Info:
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.192.5629&rep=rep1&type=pdf

Inhaltsverzeichnis

Teil 1

Was ist ein aktiver Angriff ?

Ein aktiver Angriff:

- Stört den Ablauf des Verfahrens.
- Kann das Gerät beschädigen.
- Benutzt (meist) zusätzliche Werkzeuge.

Inhaltsverzeichnis

Teil 1

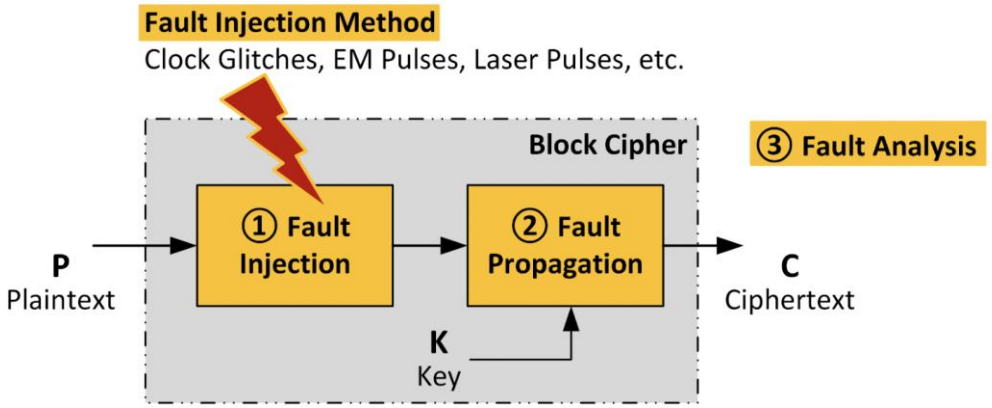
- Seitenkanalangriffe

- Passive Angriffe

- Aktive Angriffe

Was ist eine Differential Fault Analysis?

Hierbei provoziert man Fehlverhalten von außen.



Vergleichen von A und B ermöglicht Rückschluss auf Schlüssel.

Es werden dann 2 Ciphertexte (mit selbem Cleartext) generiert.

Ciphertext A = Mit normalem Ablauf des Verfahrens
Ciphertext B = Mit gestörtem Ablauf des Verfahrens

Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe

- Passive Angriffe

- Aktive Angriffe

    1) DFA
    2) EMFI
    3) Cold Boot Attack

Was ist eine **E**lectro**m**agnetic **F**ault **I**njection?

```
if(check() == 1){
  load_firmware();
}else{
  print("Check failed");
}
```

Hierbei wird ein starker elektromagnetischer Impuls verwendet.

Ziel:

- Bitflips in Registern
- Überspringen von Befehlen

Inhaltsverzeichnis

Teil 1

- Seitenkanalangriffe

- Passive Angriffe

- Aktive Angriffe

    1) DFA
    2) EMFI
    3) Cold Boot Attack

Was ist eine Cold Boot Attack?

Hierbei wird die Datenremanenz ausgenutzt.

Kühlung verstärkt diesen Effekt.

Die Speicher ausbauen und auslesen.

Mit diesen Daten sind Rückschlüsse auf den Schlüssel möglich.

Ende Teil 1

Gibt es noch Fragen ?

Hardware Security Modules

Inhaltsverzeichnis

Einleitung
Was ist ein Hardware Security Module?

- Deutsch: Hardware Sicherheitsmodul (HSM)
- Kryptographische Operationen in einer sicheren und effizienten Umgebung
- Erstellung und Verwaltung von Schlüsseln

Inhaltsverzeichnis

Einleitung
Funktionen

- Symmetrische & asymmetrische Ver- & Entschlüsselung
- Digitale Signaturen
- Hashfunktionen
- Generierung von echten Zufallszahlen
  - True Random Number Generator (TRNG)
- Generierung von Pseudozufallszahlen
  - Pseudo-Random Number Generator (PRNG)

Inhaltsverzeichnis

Einleitung
Geschichte

- Erstes HSM 1989 von IBM für militärische Zwecke entwickelt
- Anschließend vor allem im Bereich ATMs (Automated Teller Machines) genutzt
- Heutzutage gibt es viele weitere Anwendungsbereiche

Inhaltsverzeichnis

Einleitung
Formen

- PCIe Karte (Peripheral Component Interconnect Express)
  - Integration in eigene Rechner/Server
- Netzwerk Applikation inkl. Server

Inhaltsverzeichnis

1. Maßnahme

- Erhöhter Energieverbrauch -> Stromspitzen treten auf
- Kondensatoren im HSM fangen die Stromspitzen ab
- Erhöhter Energieverbrauch ist nach außen nicht mehr sichtbar

2. Maßnahme

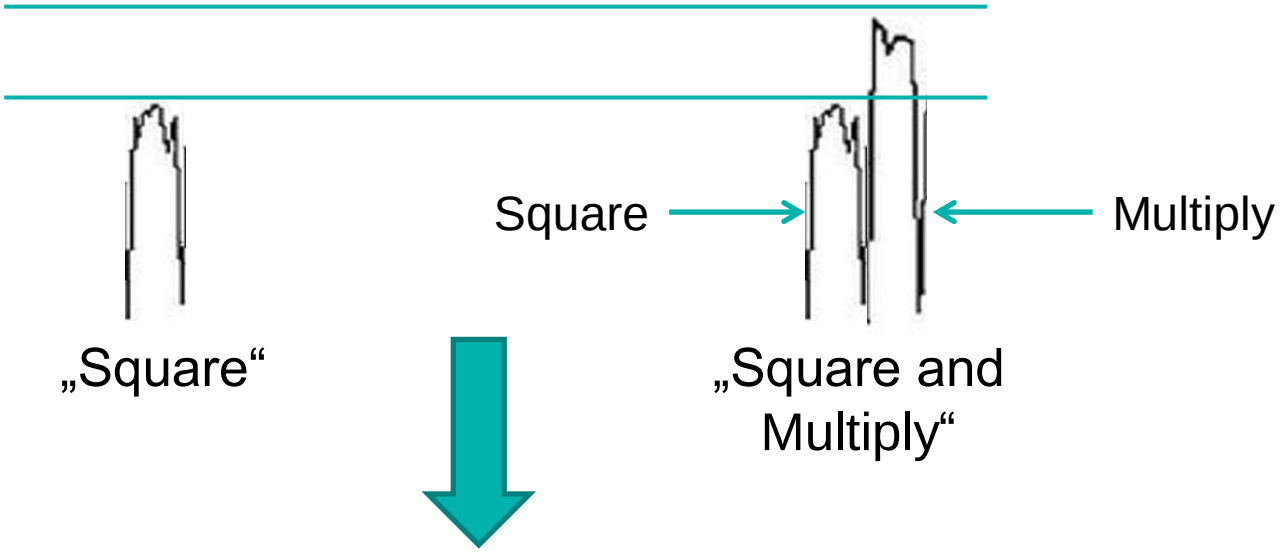
- Kryptographische Operationen verbrauchen immer gleich viel Rechenzeit & Energie

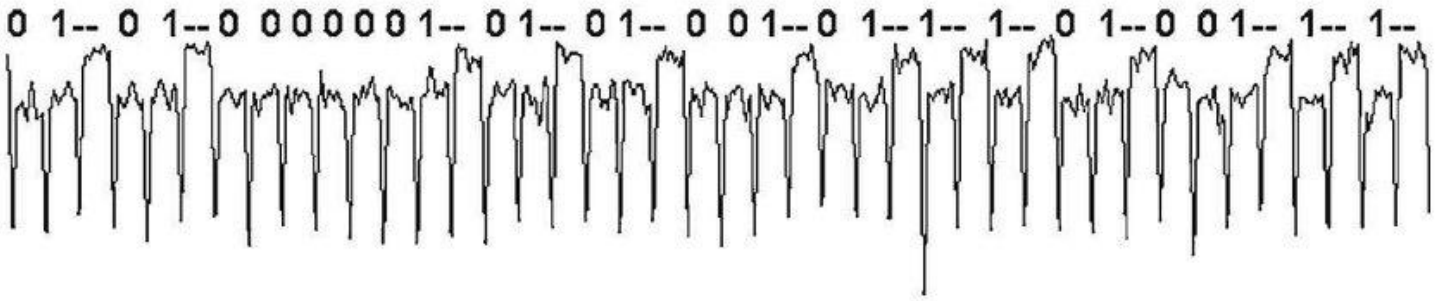
- Bsp. RSA: Falls nur eine „square" Berechnung gemacht wird
  - Zusätzliche „Dummy" Berechnungen
  - „Square" verbraucht genau so viel Zeit & Energie wie „square and multiply"

- Keine Rückschlüsse auf Eingaben oder verwendete Schlüssel möglich

- Schützt auch vor Sound Analysis

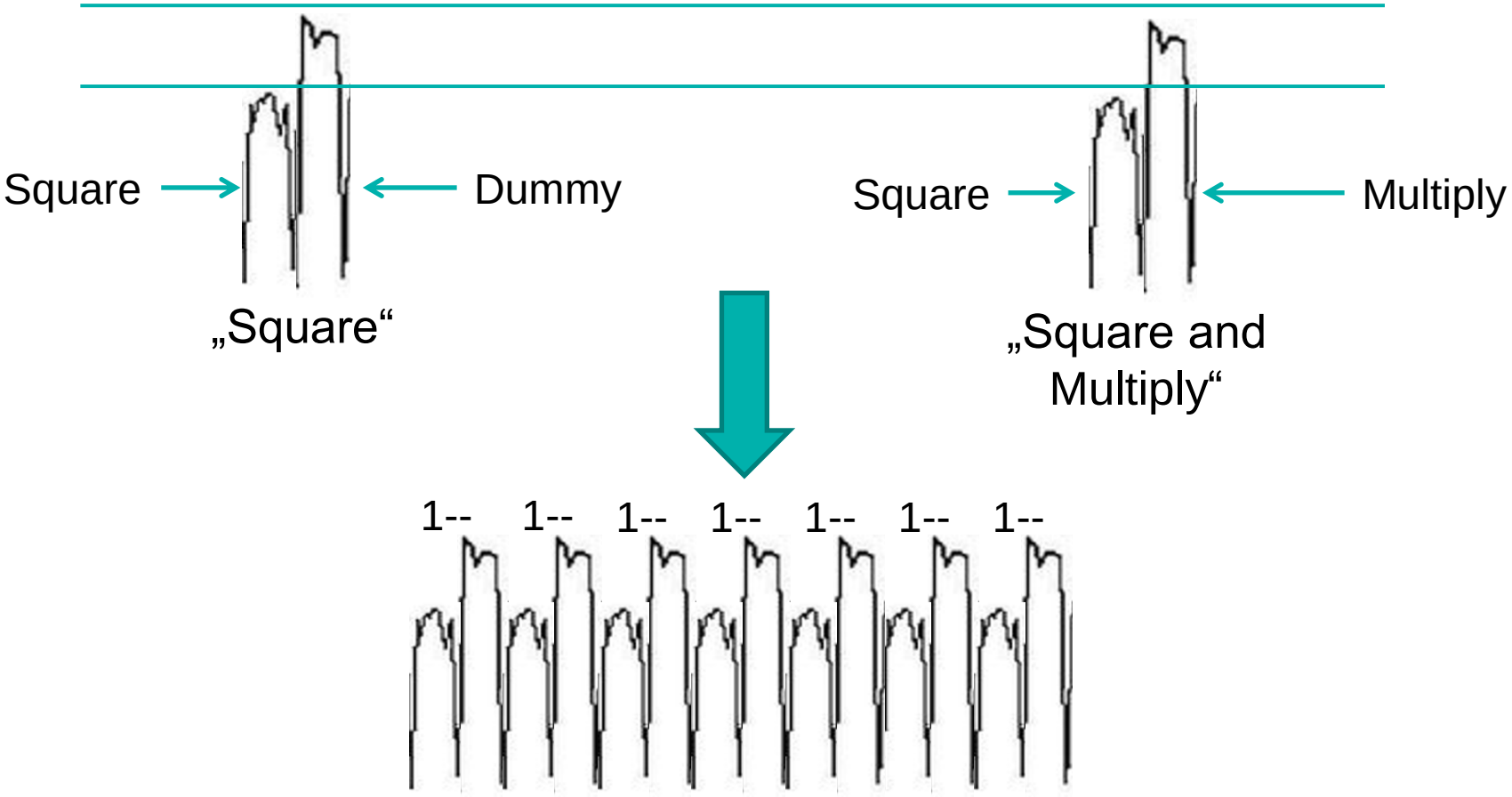
Ohne Schutzmaßnahme





Physikalische Sicherheit
Power Analysis & Timing Attack

Mit Schutzmaßnahme



Inhaltsverzeichnis

Physikalische Sicherheit
Cold Boot Attack

- Temperatur des HSMs wird durchgehend gemessen
- Fällt die Temperatur unter einen bestimmten Wert, kommt es zur **Nullstellung** (engl. „Zeroisation“)
  - Löschen von sensiblen Parametern (z.B. Schlüssel) aus einem kryptographischen Modul
- Zusätzlich physischer Angriff benötigt
- Ähnliche Mechanismen gegen DFA (Differential Fault Analysis)

Inhaltsverzeichnis

Physikalische Sicherheit
Physischer Angriff

Angriff:

- Angreifer bekommt einzelne Hardwarekomponenten des HSMs in die Hände

- **Wie?** Nutzung spezieller Werkzeuge oder Säuren

- **Warum?** Auswertung der Komponenten

Physikalische Sicherheit
Physischer Zugang

1. Maßnahme

- Siegel auf dem Deckel eines HSMs
- Bei physischem Zugang wird das Siegel automatisch zerstört
- Angriff ist sichtbar und nachweisbar

2. Maßnahme

- Platine wird mit einer Vergussmasse aus Harz geschützt
- Bei Entfernung des Harz wird die Platine wahrscheinlich zerstört

3. Maßnahme

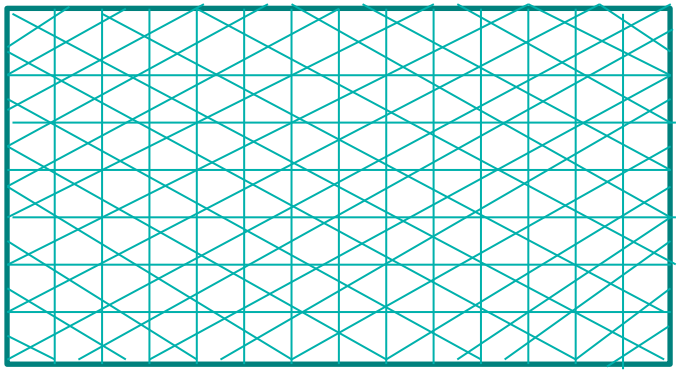
- Platine wird mit einem Metallkörper geschützt, der die einzelnen Komponenten des HSMs verdeckt

- Kombination mit einem…
  - …Schalter: Bemerkt die Entfernung des Metallkörpers
  - …Lichtsensor: Bemerkt, ob Licht an die Platine kommt
  - **Nullstellung**, sobald eines der Ereignisse eintritt

4. Maßnahme

- HSM wird mit einer Sensorfolie aus verschränkten Leiterbahnen ummantelt

- Sobald eine Leiterbahn durchtrennt wird -> Nullstellung



Kosten HSMs

- 4000€ bis zu 27000€ je nach Performance
    - Durchschnitt: 15500€
- Fortgeschrittenere Modelle fangen bei 9000€ an
- HSMaaS (HSM as a Service)

Inhaltsverzeichnis

Teil 2

Hardware Security Modules

- Einleitung
- Physikalische Sicherheit
- Standards
  - FIPS
- Anwendungsbereiche

Standards

- FIPS 140 – 2 (Federal Information Processing Standards)
  - NIST (National Institute of Standards and Technology)
  - 4 Level mit ansteigenden Anforderungen
- Common Criteria und PCI HSM (Payment Card Industry)
- Neben physikalischer Sicherheit auch sichere Infrastruktur
  - Authentifizierung, Identifizierung, Rechte, etc.
  - Schutz der Serverräume
  - Verschlüsselte Kommunikation
  - Etc.

Inhaltsverzeichnis

Standards
FIPS

- Level erfordern Erfüllung aller Level darunter

Level 1:

- Mindestens ein korrekt implementierter kryptographischer Algorithmus

Level 2:

- Physikalische Angriffe müssen nachweisbar sein
- Rollenbasierte Authentifizierung der Nutzer

Standards
FIPS

Level 3:

- Schutz/Widerstand gegen Angriffe
- Erkennung und Reaktion auf Angriffe
- Identifizierung der Nutzer

Level 4:

- Schutz-Ummantelung des gesamten Moduls, die Angriffe erkennt und darauf reagiert
- Schutz vor Spannungen und Temperaturen außerhalb des normalen Betriebs (auch Angriffe)
- Nutzung in ungesicherter Umgebung

- Standard HSMs -> Level 3, fortgeschrittene Modelle -> Level 4

Inhaltsverzeichnis

Anwendungsbereiche

Banken

- Kontrolle der PIN Eingabe (Geldautomaten, etc.)
- Überprüfung von Kredit-/Debitkarten-Transaktionen durch Kontrolle der Sicherheitscodes

Zertifizierungsstellen (z.B. von X.509 Zertifikaten)

- Generieren, Speichern und Verwalten von asymmetrischen Schlüsselpaaren

Anwendungsbereiche
weitere Bereiche

Quellen für beide Teile

Wissen:
https://de.wikipedia.org/wiki/Seitenkanalattacke
https://github.com/phonchi/awesome-side-channel-attack#side-channel-attack
https://circuitcellar.com/research-design-hub/electromagnetic-fault-injection/
https://de.wikipedia.org/wiki/Spectre_(Sicherheitsl%C3%BCcke)
https://blog.f-secure.com/cold-boot-attacks/
https://www.nsideattacklogic.de/van-eck-phreaking-und-moegliche-schutzmassnahmen/
https://de.wikipedia.org/wiki/Kaltstartattacke
https://de.wikipedia.org/wiki/Van-Eck-Phreaking
https://www.heise.de/security/meldung/I-f-Hackerin-demonstiert-Van-Eck-Phreaking-trotz-HDMI-4123699.html
http://www.cs.tau.ac.il/~tromer/acoustic/
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Seitenkanalresistenz/seitenkanalresistenz_node.html
https://www.security-insider.de/was-ist-ein-hardware-sicherheitsmodul-hsm-a-727090/
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
https://application.wiley-vch.de/HSM_for_Dummies_html/page_1.html
https://en.wikipedia.org/wiki/Hardware_security_module
https://en.wikipedia.org/wiki/Zeroisation
https://ras51.informatik.uni-stuttgart.de/cosade19/cosade15/presentations/session6_b.pdf
https://store.newae.com/chipshouter-kit/

Comic und Grafiken:
https://www.simplethread.com/great-scott-timing-attack-demo/
https://anysilicon.com/side-channel-attacks-differential-power-analysis-dpa-simple-power-analysis-spa-works/
https://www.utimaco.com/de/loesungen/branchen
https://en.wikipedia.org/wiki/Hardware_security_module

Vielen Dank für eure Aufmerksamkeit

Gibt es noch Fragen ?

FH Aachen

www.fh-aachen.de

Mick Dahlhaus & Daniel Bachmann