Kryptographische Angriffe

https://iuk.one/1012-1025

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock,Germany
clemens.cap@uni-rostock.de

Version 1

Ziele

Gutes Verteidigen setzt voraus, wie ein Angreifer denken zu können.

Arten von Angriffen

1. **Art: Angriffe auf kryptographische Algorithmen:**
   - Bsp: Verfahren wird geknackt — unwahrscheinlich, speziell bei "alten" Verfahren.
   - Bsp: Verfahren ist kaputt — kann sein, vgl. NSA Manipulation des NIST Standards
2. **Art: Angriffe auf kryptographische Protokolle:**
   - Bsp: Deterministisches Verfahren erlaubt das Erstellen eines Codebuchs.
3. **Art: Angriffe auf Sicherheitsannahmen:**
   - Bsp: Jemand bringt den Quantencomputer zum Laufen.
   - Bsp: Jemand verliert seinen privaten Schlüssel.
   - Bsp: Die Implementierung erlaubt Seitenkanal, den Modell nicht enthielt
4. **Art: Zugriff auf die noch nicht verschlüsselte Information:**
   - Bsp: VoIP Telefonat nicht abhören, sondern mit Raummikrophon abgreifen.
   - Bsp: Chat Nachricht über Hintertüre im Tastatur-Treiber auslesen.
   - Das werden die erfolgreichen Angriffe der nächsten 20 Jahre sein!

1. Replay und Co.

Ziele: Eine Klasse von Angriffen, die von fehlender Veränderung lebt.

Übersicht

Replay Attacke:
Angreifer sendet ein Paket nochmal. Blinder Angriff ohne Verständnis der Semantik.

Codebuch Attacke:
Angreifer erstellt ein Codebuch zur Übersetzung Plaintext — Chiffretext.

Korrelations-Attacke:
Angreifer nutzt deterministischer Zusammenhänge aus.

Replay Attacke (1)

Situation: Mallory hört bei einer Kommunikation von Alice und Bob zu.

Am Montag:

Bob: Alice, was kostet denn ein iPhone bei euch heute?
Alice: Wart mal, ich sende Dir das verschlüsselt.
Alice: 0xAE23 0xBBFC 0x3435

Am Dienstag:

Bob: Alice, was kostet denn der neue Tesla heute?
Mallory: Speist 0xAE23 0xBBFC 0x3435 als Antwort ein.
Bob: Bestellt einen Tesla und wundert sich über die hohe Rechnung.

Eine **Replay-Attacke** besteht aus dem erneuten Senden
eines früher einmal gesendeten Datenpakets.

Replay Attacke (2)

Abwehr von Replay Attacken:
Zusätzliche Information unfälschbar und untrennbar einarbeiten (prepend, append, inject).

Möglichkeiten:

- **Nonce:** Number used **once**, Zufallswert, der nur einmal verwendet wird.
- **Zeitstempel:** Aktuelle Uhrzeit.
- **Sequenznummer:** Wird mit den Paketen immer hochgezählt.
- **Verkettung:** Einbinden von Informationen des vorangegangenen Pakets.
  Bsp: CBC **C**ipher **B**lock **C**haining Mode
- **Sitzungs-Id:** Etabliere eigene Session-Id von kurzer zeitlicher Gültigkeit.
- **Schlüssel:** Etabliere eigenen symmetrischen Schlüssel kurzer zeitlicher Gültigkeit.

Codebuch Attacke

Ähnlich wie Replay Attacke.

Angreifer führt hier ein Codebuch in der Form:

Chiffretext	**Plaintext**
0x3457 0xA3B4	Nein
0x3229 0x1121	Ja

Verteidigung: Randomisierung.

2. Differentielle Attacken

Ziele: Eine Klasse von Angriffen, die Zusammenhänge der Veränderung in Plaintext und Ciphertext untersucht.

Chosen Plain Text Attacke

Situation:

- Alice arbeitet in der Buchhaltung und sendet immer wieder Schecks mit dem Text "Betrag von X an Y auszahlen" an die Bank.
- Alice verschlüsselt diese Schecks mit dem RSA Algorithmus.
- Mallory schneidet das alles mit.
- Alice verliert ihre Verschlüsselungskarte (die sie nicht PIN-gesichert hat).

Attacke: Mallory verschlüsselt nun (choosen plain text):

- "Betrag von 1001 an Bob auszahlen"
- "Betrag von 1002 an Bob auszahlen"
- "Betrag von 1003 an Bob auszahlen" – AHA ! Das ergibt den Chiffretext!

Mallory weiß nun, was Bob verdient.

Verteidigung: Randomisieren, probabilistische Verschlüsselung.

Ciphertext Indistinguishability

Beachte: Anforderung der Randomisierung wäre formal bereits hier erfüllt:

Plain	**Ich habe gewonnen**	**Ich habe verloren**
Cipher 1	AS123123	ATsdf
Cipher 2	BS123123	BTsdf
Cipher 3	CS123123	CTsdf

Daher: Offensichtlich reicht "Randomisierung" alleine nicht aus!

Idee: Ununterscheidbarkeit von Ciphertexten (Ciphertext Indistinguishability):
Gegeben 2 Plaintexte und ein Ciphertext soll der Angreifer
nicht raten können, zu welchem Plaintext der Ciphertext gehört.

Lösung: OAEP: **O**ptimal **A**symmetric **E**ncryption **P**adding

Chosen Ciphertext Attacke

Beobachtung: Systeme mit Random Padding prüfen nach Entschlüsselung ob das Random Padding im Plaintext auch durchgeführt wurde.
Wenn nicht: Entsprechende Fehlermeldung.
Systeme geben über Fehlermeldungen Zusatzinfo ab.

Daraus kann ein Angriff konstruiert werden:

Angreifer kann immer wieder bestimmte, ausgewählte Ciphertexte entschlüsseln lassen bzw. die dazugehörigen Fehlermeldungen erhalten.

Diese Informationen nutzt er, um einen bestimmten Ciphertext zu entschlüsseln (zu dem er das System nicht befragen darf.)

3. Man in the Middle

Ziele: Wir verstehen die Mechanismen des MITM Angriffs und warum er so gefährlich ist.

Ausgangslage Man in the Middle (MITM)

Situation: Alice sendet an Bob *ohne* Verschlüsselung:

$$Alice \xrightarrow{Hello} iPhone \xrightarrow{Hello} \xrightarrow{Hello} \xrightarrow{Hello} Mac \xrightarrow{Hello} Bob$$

Situation: Alice sendet an Bob *mit* Verschlüsselung:

$$Alice \xrightarrow{Hello} iPhone \xrightarrow{0x1347} \xrightarrow{0x1347} \xrightarrow{0x1347} Mac \xrightarrow{Hello} Bob$$

Beobachtung: Eines Tages passiert das Folgende:

$$Alice \xrightarrow{Hello} iPhone \xrightarrow{0x8899} \xrightarrow{????} \xrightarrow{0xAC} Mac \xrightarrow{Hi} Bob$$

1. Alice sieht: Ihr Endgerät versendet offenbar verschlüsselt.
2. Bob sieht: Sein Endgerät empfängt offenbar verschlüsselt.
3. Weder Alice noch Bob sehen aus ihrer *lokalen* Perspektive daß der gesendete Chiffre- & Klartext *verschieden* ist vom empfangenen.

Erklärung der MITM

Charakteristika einer **M**an **i**n **t**he **m**iddle (MITM) Attacke

- Der Sender verschlüsselt (unwissend) an die Angreiferin Mallory.
- Die Angreiferin Mallory
  - entschlüsselt den Text
  - liest den Text oder verändert ihn sogar
  - verschlüsselt danach an den ursprünglichen Empfänger.
- Weder Sender noch Empfänger bemerken den Fehler.

Ursache:	Falsche Zuordnung öffentlicher Schlüssel. Der Sender benutzt den öffentlichen Schlüssel des Angreifers, statt des öffentlichen Schlüssels des Empfängers
Hier:	Angriff auf die Verschlüsselung.
Generell:	Auch Angriff auf Prüfung einer Unterschrift denkbar.

3 Verteidigungs-Strategien gegen eine MITM

Lösung: Mechanismen zur Sicherstellung der korrekten Schlüssel-Nutzung.

Zentralisiertes Vertrauen: Zertifikats-Infrastruktur, public key infrastructure PKI

- Als vertrauenswürdig angesehenen Institutionen bestätigen Schlüssel-Korrektheit.
- Problem: Single point of failure ist immer gefährlich.
- Problem: Fälle bekannt, in denen das Vertrauen systematisch mißbraucht wird.

Dezentralisiertes Vertrauen: Web of Trust, WoT

- Dezentrales Netz bestätigt Schlüssel-Korrektheit.
  Bsp: Viele Leute, denen viele Leute vertrauen, denen viele Leute vertrauen, denen ich vertraue bestätigen die Korrektheit des Schlüssels.
- Problem: Ohne Fachausbildung wird Schlüsselbestätigung oft falsch gehandhabt.

Separat-Kanal: Benutze zweiten, unabhängigen Kanal zur Überprüfung.

- Bsp: Alice ruft Bob an und bittet um Fingerprint / Hash-Wert seines Schlüssels.
  Unwahrscheinlich, daß zwei Kanäle vom Angreifer manipuliert sind.
- Problem: Separat-Kanal oft nicht verfügbar oder als unbequem erachtet.

Zertifikate und das Bootstrapping Problem von Identität

Zertifikate sind Dokumente, die folgende 3 Dinge enthalten

1. eine eindeutigen Aussage über die Identität einer Person oder Entität
2. den öffentlichen Schlüssel dieser Person oder Entität
3. eine digitale Unterschrift auf diese beiden Bestandteile.

Frage: Wie prüft man diese digitale Unterschrift?

Antwort: Mit dem zugehörigen öffentlichen Schlüssel!

Problem: Woher weiß ich, daß dieser öffentliche Schlüssel der richtige ist?

Public Key Infrastructure: Etablieren von Identität

Etablieren von Identität:

- Trent ist eine per Definition vertrauenswürdige Institution.
- Trent betreibt eine Certificate Authority (CA, Trust Center).
- Bob trifft Trent und legt einen Lichtbildausweis vor.
- Trent produziert und unterschreibt das folgende Dokument digital:

Zertifikat für Bob, unterschrieben durch Trent

```
Der öffentliche Schlüssel von Bob Digitalis, geboren am 2. 2. 2022 in
Berlin, Reisepaß Nummer 1234-5678-90 und email bob@berlinmail.de ist E893
3437 ...
```

Hinweis (1)

Achtung!

Vertrauen auf Basis von Annahmen ist ein **grundsätzlicher Fehler** in der Sicherheit.

Die menschliche **Geschichte** lehrt:

- Angenommenes Vertrauen **kann** mißbraucht werden.
- Angenommenes Vertrauen **wird regelmäßig** mißbraucht.

Achtung!

Ein besserer Ansatz ist: Vertrauen auf Basis **grundsätzlicher und individueller Möglichkeiten der regelmäßigen Überprüfung**.

Hinweis (2)

Manche Kryptographen sagen zur Zertifikats-Infrastruktur statt "Trust Center" auch "**Schlüsselfertigungszentrale**" um herauszuarbeiten, daß bei Nutzung einer PKI der einzelne Nutzer **blindlings den Behauptungen der CA glaubt**.

Das in der **Namensgebung** "Vertrauen", "Zertifikat", "Authority" transportierte **Framing** von Sicherheit ist eine konzeptuelle **Lüge**, die in der Praxis aber ausgesprochen bequem ist – wie jede an Dritte delegierte Eigenverantwortung.

Die gute Nachricht: Protokolle für **überprüfbares Vertrauen** sind möglich und **entstehen gerade in unserer Zeit** in der Kryptographie.

Beispiele: Blockchain, Zero Knowledge Proof, Self Certifying Storage, Private Information Retrieval usw.

Public Key Infrastructure: Nutzen

Nutzen eines Zertifikats:

- Alice möchte mit Bob kommunizieren.
- Sie braucht dazu den öffentlichen Schlüssel von Bob.
- Sie bittet Bob um sein Zertifikat.
- Sie prüft die Unterschrift von Trent auf dem Zertifikat.
- Sie nutzt den öffentlichen Schlüssel von Bob.

Bootstrapping Problem (1)

Problem: Wie kommt Alice an den öffentlichen Schlüssel von Trent?

Öffentliche Registratur:

- Problem: Warum sollte Alice der Registratur vertrauen?
- Lösung: Kraft Annahme.
- Aber: Es sind Fälle des Mißbrauchs und der Schlamperei bekannt.
  Es sind Fälle der Zusammenarbeit von Registraturen
  mit Geheimdiensten, IT- und Überwachungs-Unternehmen bekannt.

Digitale Schlüsselspeicher: Vom Hersteller ins Betriebssystem eincodiert.

- Problem: Warum sollte Alice dem Hersteller des Betriebssystems vertrauen?
- Problem: Hat Update oder Virus den Schlüsselspeicher manipuliert?
- Problem: Hat Alice den Schlüsselspeicher versehentlich ruiniert?

Bootstrapping Problem (2)

Key Pinning: Wurde vom Hersteller ins Binary des Programms geschrieben.

- Problem: Bei Problem mit einem Schlüssel schwer austauschbar.
- Problem: Warum sollte Alice dem Hersteller vertrauen?

Rekursiv: Durch ein weiteres Zertifikat.

- Problem: Wie prüft Alice dieses weitere Zertifikat? Endlose Rekursion?
- Lösung: Durch ein sogenanntes Wurzel-Zertifikat *root certificate* das durch eine der anderen Methoden abgesichert ist.

Reality Check (1)

Ist MITM **wirklich** so ein Problem?

Szenario 1: **Industrielle und politische Spionage**

- Geheimdienst eines Landes bittet befreundete CA um den privaten Schlüssel.
- Geheimdienst kann Zertifikate ausstellen.
- Geheimdienst kann nun überall mitlesen.
- Öfter als "Räuberpistole" belächelt.
- Heute gelten mehrere Fälle als zweifelsfrei etabliert.

Szenario 2: **RSA SecurId Hack**

- Server des Herstellers gehackt.
- Pressemeldung: "Alles sicher. Weitergehen. Hier gibt es nichts zu sehen".
- Einbruch bei Lockheed Martin, Hersteller Tarnkappenbomber.
- Jetzt: 40 Millionen Devices weltweit werden ausgetauscht.

Reality Check (2)

Szenario 3: **Erfolgreiche Angriffe**

- Cracker bricht bei Zertifizierungsstelle ein und stiehlt private key.
- Cracker stellt sich Zertifikate aus, die ihm gestatten sich auszuweisen als: google.com, update.microsoft.com, mossad.gov.il, skype.com, cia.gov uvm. und stellt den Beweis dafür auf pastebin ein.

Szenario 4: **Deep Packet Inspection Firewalls**

- Hersteller der Firewall erzeugt ein spezielles Zertifikat.
- Besitzer der Infrastruktur installiert das auf den Browsern seiner PCs.
- Der manipulierte Browser verhält sich, wie es der Nutzer erwartet, aber Firewall macht MITM Angriff, Besitzer der Infrastruktur kann mitlesen & -schreiben.

Szenario 5: **Staatliche Überwachung**

- Bei DE-Mail, 3G & 4G können Behörden Verschlüsselung letztlich umgehen.

4. Integrität des Endgeräts

Ziele: Wir verstehen die hohe Vulnerabilität des Endgeräts gegen Eingriffe und Modifikationen.

Grundsätzliches Schema

In Software:

- Funktionieren oft auch remote (Schadsoftware)
- Sind leicht zu plazieren
- Urheber kann sich gut verbergen

In Hardware:

- Erfordern Präsenz vor Ort.
- Skalieren schlecht für Massenangriff, da Aufwand des Plazierens.
- Urheber leichter aufzufinden.

Daher: Wegen großer Bandbreite an Möglichkeiten sehr schwer zu vermeiden.

Hardware-Keylogger

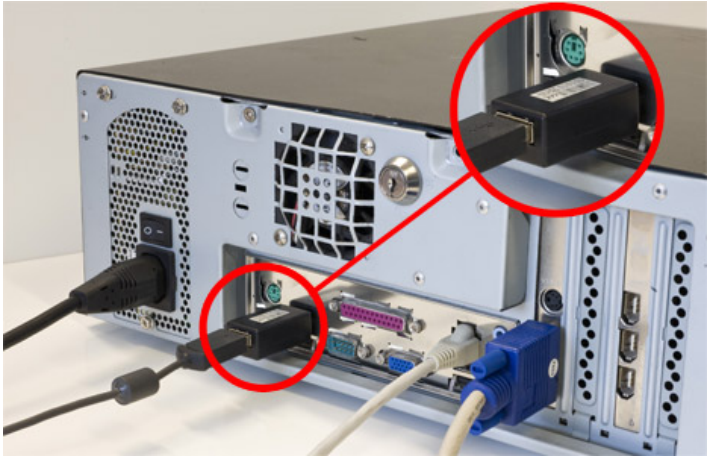

Abb. 1: Hardware Key Logger, der Tastatureingaben und somit auch Paßwort-Eingaben mitschneidet und dann per Wifi an den Angreifer überträgt. © Rechte siehe Anhang.

Cold Boot Attacke in der Theorie

Problem:

- Private Schlüssel befinden sich nach der Eingabe durch den Benutzer im RAM.
- Kann man den Schlüssel nach der Eingabe aus dem RAM auslesen?

Vorgehensweise:

- Laufenden Computer öffnen.
- Speicherchips kühlen und aus dem Gerät entfernen.
- Speicherchips in anderes System umstecken.
- Dank der Kühlung behalten die Chips die Inhalte noch einige Sekunden.
- Speicher auslesen und Schlüssel suchen.
- Für Schlüsselsuche gibt es open source Software.

Cold Boot Attacke in der Praxis

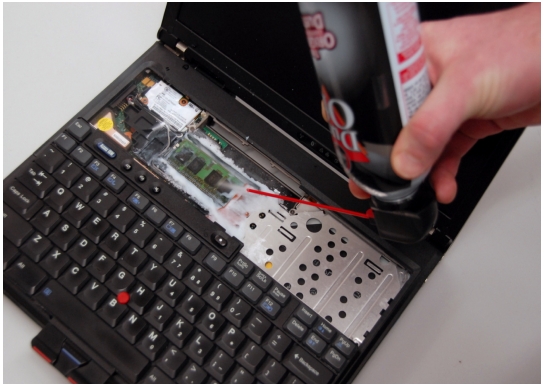

Abb. 2: Kühlung der Speicherchips. © Rechte siehe Anhang.

Abb. 3: Gekühlte Speicherchips. © Rechte siehe Anhang.

Seitenkanal-Angriffe

Definition

Seitenkanal-Angriffe nutzen Informationen, die aus der physikalischen Implementierung eines Systems gewonnen werden können.

Private Schlüssel können rekonstruiert werden aus:

Timing Attacke: Aus Zeit zur Verschlüsselung bestimmter ausgewählter Plain Texte.

Power Attacke: Aus dem Stromverbrauch während der Verschlüsselung.

Akustische Cryptanalyse: Aus den Tönen, welche die CPU beim Arbeiten abgibt.

Bellcore (Fault Injection) Attacke: Aus teilweisen Fehlfunktionen der CPU durch Erhitzen. Bei RSA ist so die Bestimmung des Schlüssels möglich.

5. Umgebung des Endgeräts

Ziele: Wir erkennen, daß Verschlüsselung auch leicht umgangen werden kann, indem man einfach die Umgebung der Informations-Erzeugung angreift.

Angriff auf die Umgebung des Endgeräts

Eigenschaften:

- Erfordern meist physische Präsenz in der Nähe.
- Skalieren schlecht für Massenangriff, da teuer und auffällig.
- Können oft auf einen Urheber zurückgeführt werden.

Daher:

- Geringe Wahrscheinlichkeit, außer Opfer ist in Risikogruppe.
- Abwehr erfordert breites physikalisches Know How.

Tempest

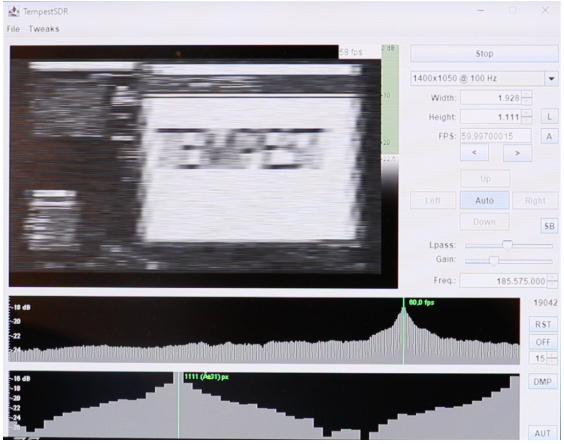

Abb. 4: Tempest-Angriff: Aus den elektromagnetischen Abstrahlungen eines Monitors kann der Bildschirminhalt rekonstruiert werden.

Abhören mit passivem Funktransponder

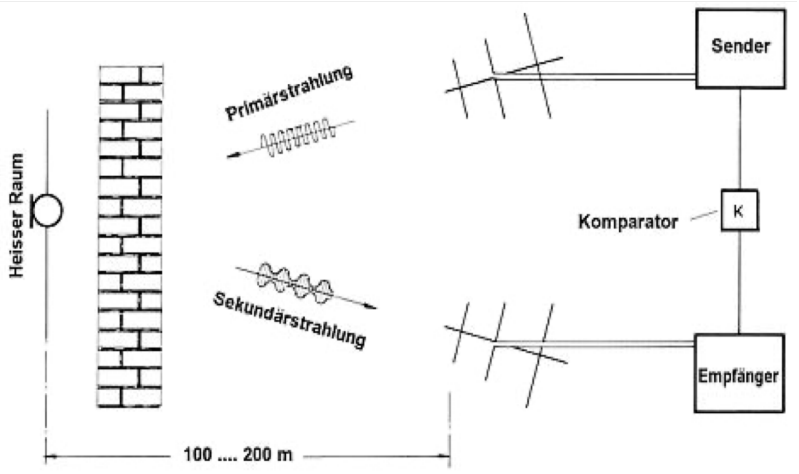

Abb. 5: Mechanismus eines passiven Funktransponders

Abhören mit passivem Funktransponder

Abb. 6: Siegel der USA, 1945 Geschenk der UDSSR an den US Botschafter in Moskau.

Abb. 7: Das Siegel enthielt eine Metallkonstruktion, die bei enstprechender Funkbestrahlung den Strahl modulierte und das Abhören des Raumes ermöglichte.

Abhören mit Laserstrahl

Abb. 8: Die Reflexion des Laserstrahls wird durch die Vibrationen der Scheibe moduliert.

Abb. 9: Ausrüstung zum Abhören.

Abhören mit optischem Mikrophon

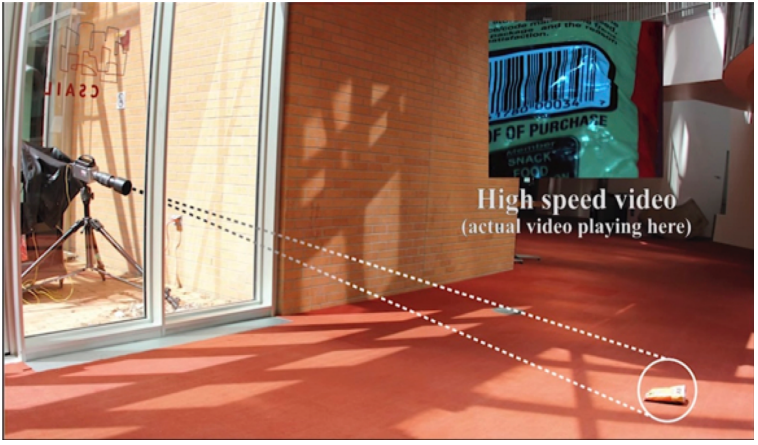

Abb. 10: Eine Video-Camera nimmt die Vibrationen eines Blattes Papier auf und hört damit einen Raum ab. http://people.csail.mit.edu/mrub/VisualMic/ und http://youtu.be/FKXOucXB4a8 https://www.youtube.com/watch?v=eUzB0L0mSCI.

Hinweis

Ein Kryptosystem, bei dem

- der Algorithmus proprietär ist
- die Implementierung proprietär ist
- die komplette Betriebsumgebung nicht völlig trusted ist
- die Hardware nicht völlig trusted ist
- die Software nicht auditiert / open source ist
- die Umgebung des Geräts nicht sicher ist

ist nicht vertrauenswürdig.

Anhang

Übersicht

Verzeichnis aller Abbildungen (1/2)

Rechtsnachweise

Abb. 1 Quelle: http://www.kingston.ac.uk/it-security/includes/img/static/usb-logger.jpg, Nutzung nach CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=55384824.

Abb. 2 Quelle: https://citp.princeton.edu/research/memory/.

Abb. 3 Quelle: https://citp.princeton.edu/research/memory/.

Abb. 4 Quelle: https://deralchemist.wordpress.com/2020/09/04/tempestsdr-monitore-ausspionieren/.

Abb. 6 Quelle: https://commons.wikimedia.org/w/index.php?curid=596734, Nutzung nach CC BY-SA 3.0.

Abb. 7 Quelle: https://commons.wikimedia.org/w/index.php?curid=596727, Austin Mills, IMG-0214, Nutzung nach CC BY-SA 2.0.

Rechtliche Hinweise

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das Zitatrecht in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Zitierweise dieses Dokuments

Wenn Sie Inhalte aus diesem Werk nutzen oder darauf verweisen wollen,
zitieren Sie es bitte wie folgt:

Clemens H. Cap: Kryptographische Angriffe. Electronic document. https://iuk.one/1012-1025
30. 1. 2021.

Bibtex Information: https://iuk.one/1012-1025.bib

```
@misc{doc:1012-1025,
   author       = {Clemens H. Cap},
   title        = {Kryptographische Angriffe},
   year         = {2021},
   month        = {1},
   howpublished = {Electronic document},
   url          = {https://iuk.one/1012-1025}
}
```

Typographic Information:
Typeset on January 30, 2021
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

Verzeichnis aller Folien

Legende:
Fortsetzungsseite
Seite ohne Überschrift
Bildseite