Understanding the Attacker

https://iuk.one/1033-1006

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

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

Version 1

Know the Attacker

Motives: What does the attacker want to do?

Capabilities: What is the attacker able to do?

Ressources: Which means does the attacker have available?

Overview

1. Motives
2. Capabilities and Ressources
3. Special Scenarios

1. Motives

The motives of an attacker are the starting points of our defense.

1. Motives

2. Capabilities and Ressources

3. Special Scenarios

Financial Gain

Variants:

- Steal information (spying).
- Steal access codes.
- Get services for free.

Response:

- Raise the costs for the attacker.
- A rational attacker is easy to beat.

Psychological Gain

Variants:

- Do damage, do revenge.
- Get attention of the victim.
- Obtain cracker fame.
- Produce chaos and confusion.
- Provoke specific reaction.

Response:

- **Problem 1:** Irrational goals (vandalism) are difficult to counteract.
- **Problem 2:** Inaccessible goals (cracker fame) are difficult to destroy.
- Knowing true motives helps in defense.
- Defense by destroying the goal of the attacker.

No Motive is also a Motive

Variants:

- No plan, just random hacking.
- No plan, just testing a random script.
- Deflecting attention of the defense system.
- Testing and studying the defense system.

Response:

- Must defend against it – even if attacks does not seem reasonable at all.

2. Capabilities and Ressources

2.1. Computational Capabilities

2.2. Network Access

2.3. Physical Access

2.4. Institutional Access

Implementation and size of defense depends on the assumed capabilities of the attacker.

1. Motives
2. **Capabilities and Ressources**
3. Special Scenarios

Computational Capabilities

Relevant for:

- Breaking encryption.
- Forging signatures.
- More advanced cryptographic attacks.

Measured in:

- Key testings per time unit.

RSA Challenges: Which are broken?

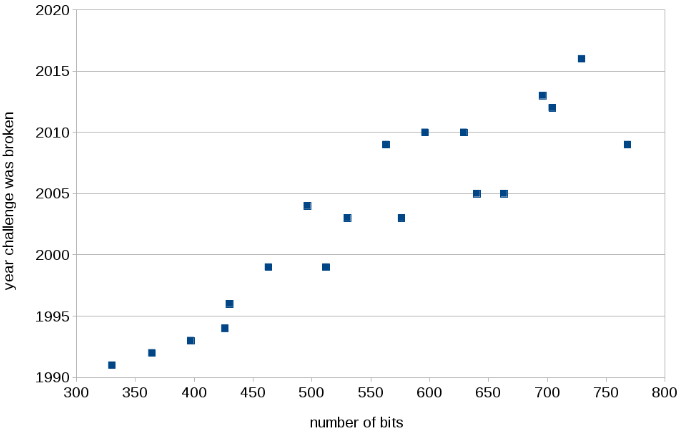


Fig. 1: When were which RSA-challenges broken? © Rechtsnachweis siehe Anhang.

RSA Challenges: Which effort is needed?

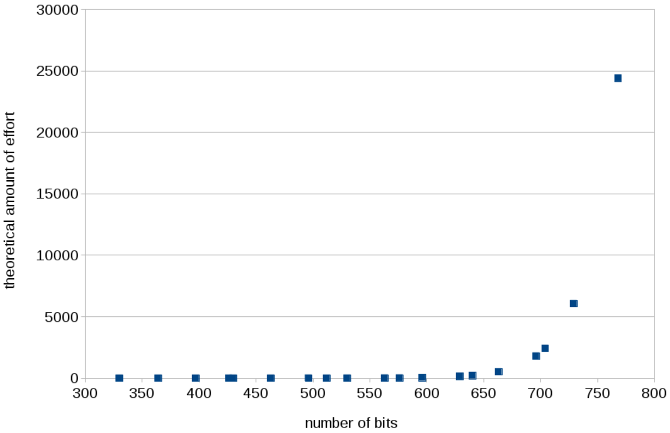


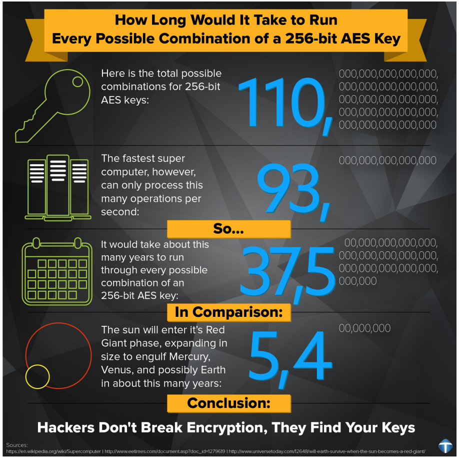
Fig. 2: Scaling of the Efforts Required to Break RSA Challenges © Rechtsnachweis siehe Anhang.

How long do we need to break AES-256?

$n = \log_2(k)$	$k = 2^n$
1	2
2	4
4	16
8	256
16	65536
32	$4.2 \cdot 10^{9}$
56	$7.2 \cdot 10^{16}$
64	$1.8 \cdot 10^{19}$
128	$3.4 \cdot 10^{38}$
192	$6.2 \cdot 10^{57}$
256	$1.1 \cdot 10^{77}$

Tab. 1: Security parameter and size of key space.

Brute Forcing AES-256



How Long Would It Take to Run Every Possible Combination of a 256-bit AES Key

Here is the total possible combinations for 256-bit AES keys:

110,000,000,000,000,000,
000,000,000,000,000,
000,000,000,000,000,
000,000,000,000,000,
000,000,000,000,000

The fastest super computer, however, can only process this many operations per second:

93,000,000,000,000,000

So...

It would take about this many years to run through every possible combination of an 256-bit AES key:

3,75,00,000,000,000,000,
000,000,000,000,000,
000,000,000,000,000,
000,000

In Comparison:

The sun will enter it's Red Giant phase, expanding in size to engulf Mercury, Venus, and possibly Earth in about this many years:

5,400,000,000

Conclusion:

Hackers Don't Break Encryption, They Find Your Keys

Sources:
https://en.wikipedia.org/wiki/Supercomputer | http://www.eetimes.com/document.asp?doc_id=1279619 | http://www.universetoday.com/12648/will-earth-survive-when-the-sun-becomes-a-red-giant/

Fig. 3: Brute Forcing AES-256 © Rechtsnachweis siehe Anhang.

Computationally Secure Model

Definition: Computationally Secure Model

The attacker has a device of a certain computational speed.

Analysis:

- Models the dangers of an attack in current technology.
- **Optimistic** approach
- **Neglects** future hardware development.
  - **Quantitatively:** Faster computers: Moores Law
  - **Qualitatively:** New technology (quantum computer, neuro computer)
- **Security** is based on difficulty of solving a complicated task.
- **Typical statement:** At key length k the method is secure for the next 5 years.

Unconditionally Secure Model

Definition: Unconditionally Secure Model

The attacker has a device of **arbitrary high** computational speed.

Analysis:

- **Pessimistic** approach.
- **Security** is based on statistical effects.
- **Typical statement:** Method is unconditionally secure.

One Time Pad

Plaintext:	$p_1 \ldots p_n$ with $p_j \in \{0, 1\}$
Key:	$k_1 \ldots k_n$
Ciphertext:	$c_1 \ldots c_n$

Encryption:	$c_j = p_j \oplus k_j$
Decryption:	$p_j = c_j \oplus k_j$

Task: Security Parameter of the OTP

Task 1: For a key length of $n = 512$, what is the security parameter of the one time pad?

Task 2: How long does it take to break the One Time Pad? Provide an estimation!

Task 3: Why is that question not really reasonable?

Network Attacks

Forms of Attacks:

- Intercepting Packets (Eavesdropping)
- Suppressing Packets
- Delaying Packets
- Replaying Packets
- Modifying Packets
- Injecting Packets
- Traffic Analysis

Task: Network Attacks

For all of the network attacks5:

Use case:

- How can these capabilities be useful for an attacker?
- Provide a practical use case!
- How would an attacker launch such an attack in practice?

Protection:

- How can we protect ourselves against these attacks?

Overview

Forms:

- Network access.
- Access to hardware.
- Access to premises.

Aspects of Attacks:

- Direct raw damage to the hardware – rather banal.
- **Important form** of attack: Side channel attacks.
- Complete exchange of the functionality of the device.

Side Channel Attack

Side channel attacks gather information on the implementation of a (cryptographic) system and deduce keys or secrets from it.

Electromagnetic Side Channel Attack

Example: Recover private keys.

- Short report in blog, paper

Example: Compromise voter privacy.

- Emanations from a voting machine can detect choice by voter: Video

Example: Changing monitor patterns produce music.

- A monitor is able to play music via particular patterns on the screen: Video

Example: Read keys typed on a keyboard.

- Read keys typed on a remote keyboard: Video (1), (2)

Listening to electromagnetic emanations

Optical Side Channel Attack

Example: Optical Side Channel Attack on Conversations

- Historical example: HAL 9000 lip-reading conversation of pilots discussing to power 'him' down and then prevents this shutdown. Movie clip illustrating the problem
- **Optical** access to a room can reproduce sounds from that room.
- Sound modulates window which modulates a laser reflection.
- Sound modulates movement of objects recorded on a video.

Example: Optical data leakage from air-gapped computer

- Hard drive LED can be used to leak data from an air-gapped computer: 🔗

Acoustical Side Channel Attacks

Example: Acoustical Side Channel Attack on RSA.

- Listening to the sounds of CPU-close capacitors allows to derive RSA private key.
- Overview

Example: Acoustical Side Channel Attack on Keyboard.

- Listening to the sounds of a keyboard allows to reconstruct the typed text.
- Keyboard Acoustic Emanations Revisited

More Side Channel Attacks

Power Attack:

- Deduces information from the power consumption of a chip (cf. acoustic attack).
- Prevent: Isolate power consumption data from attacker (eg. capacitor).

Timing Attack:

- Deduces information from time taken for a cryptographic operation.
- Prevent: Always take a fixed amount of time until delivering a response.

Fault Attack:

- Deduces information from the failure modes of a chip (eg: Belcore attack).
- Prevent: Always check for correct answer before rendering response to user.

Institutional Access

Aspects:

- Knowing people.
- Knowing processes.
- Knowing security policies.

Mechanism:

- Some situations require shortcuts through security procedures.
- Identification / authorization then uses “knowledge” of the institution.
- Institutional access then opens up attack vectors.

Example: Recovery of a Second Factor

Assume: Multifactor authentication.

- Factor 1: Password – with email recovery.
- Factor 2: Mobile phone app, generating a one time password.

Question: How do we do the recovery?

Problem: Recovery must not reduce a 2-factor system to a 1-factor system.

Solution often: Contextual information.

- Call provider, who will ask you for contextual information only you will know.

Examples for contextual information:

- Data on the last bill
- Info on recent transactions
- Special customer number not used otherwise

Access to the institution allows attacker to compromise of this method.

3. Special Scenarios

3.1. Social Engineering

3.2. Insider Attack

3.3. Whistle Blower Attacks

1. Motives

2. Capabilities and Ressources

3. Special Scenarios

Many security breaches are connected with particular combinations of attack capabilities, often revolving around social engineering skills combined with particular other capabilities.

Example: Installing a Program

Attacks:

- Drop a USB stick with label “lay off planning 2021” in the parking area of a company.
- Forget a DVD Rom with an “adult entertainment” labeling in a common access room.
- Send emails with an appealing subject and provide a clickable link or attachment.
- Send SMS with a link “install this app to track your Amazon delivery”.

Example: Access to Restricted Doors

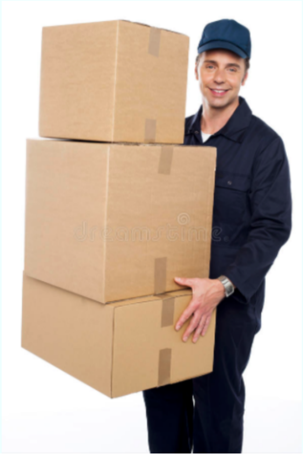


Fig. 4: How to get access through a high-security door.

Task: Security Policy

Assume: You are the only IT specialist in the 20 person regional newspaper.

Task: Design security policies to protect your company against inadvertent installation of a program.

Assume: You run the student PC support hotline of the ITMZ in Konrad-Zuse-Haus.

Task: Design a security concept to prevent unauthorized entry into closed portions of the Konrad-Zuse-Haus.

Teachings

General Approach of Deception:

- Security mechanisms are in place for a reason.
- Security mechanisms may fail in particular situations and then need "exception handling" outside of the rules.
- Deception is the art of leveraging the necessary exception handling into an attack.

Social Engineering

Social engineering is an attack on the psychology of the victim
to trick him into insecure behavior
which he would not show when having the full picture.

Insider Attack

Insider Attack

A malicious attack on a network or computer system by a person with authorized system access.

Problem: Insider information provides big leverage for attacks:

- Attacks are easier to accomplish.
- Damage can be much higher.
- Tracks can be covered easier.

Motivation:

- Do damage as revenge (eg. post termination)
- Steal customer data and IP for competition or to start own company.
- Lazyness: Work-arounds to ease your daily job

Typical Insider Issues

Accumulation: The longer an employee the more privileges.

Documentation: Do we know who has which privilege?

Snooping: For employees it is easy to acquire privileges via inofficial means

- Abuse of the boss position (social engineering).
- Looking over the sholder during password entry.
- Knowing where ownership-connected authentication methods are kept

Legacies: Privileges remain from earlier moments in the life-cycle.

Backdoors: Employees can install methods for later covert re-entry into a system.

Monitoring: Employees have means to downgrade security monitoring.

Task: Insider Attacks

Assume: You are part of a team designing an email app for Android.

Task:

- How do you prevent you small startup company from insider attacks?
- Make a short list of feasible and effective measures!

Example: CEO Fraud

Assume: An employee receives an email.

> Please do the following particularly important money transfer for our company. This is important. I selected you since I trust you. Do not call me, I am on a business trip. Lawyer Alice will call you with the details.

A person of that name calls. The employee hesitates, asks back, receives this email:

> So sad, Mary, that I cannot trust you.
> I have particularly selected you since I thought the company could rely on you.

Question: How should the employee react?

Damages: According to FBI: World-wide damages of the scheme: 3 billion USD.

Whistle Blower

Whistle Blower

Person with access to internal information
who exposes this information, often in violation of contracts and laws,
to turn public attention to supposedly illegal acts.

The two sides:

- Morally charged side of the whistle blower.
- Side of those responsible for preventing information leaks.

The Difficult Position of Whistle Blowing

Situation 1: Necessity of whistle blowers and their protection.

- Society wants to be protected against ethical wrong-doing.
- Particular wrong-doing can only be uncovered with whistle blowers.
- This requires whistle blower protection.

Situation 2: Whistle blowers could undermine opsec.

- Problematic decisions, when taken, must be carried out in accordance to the rules.
- Whistle blowers undermine the operational security of these decisions.

Situation 3: Whistle blowing as necessary last resort.

- When regular protection mechanisms fail, whistle blowers must seek public attention.

Situation 4: Highly difficult situation.

- Whistle blowers must decide themselves, with insufficient legal and moral support.
- Overall legal and ethical evaluation is extremely difficult.

Chelsea / Bradley Manning

Story:

- Had access to classified databases as intelligence analyst in a US army unit.
- Disclosed 750.000 classified military and diplomatic documents to Wikileaks.
- Among them a video of a Baghdad and Afghanistan airstrike.
- Documents revealed numerous supposed war crimes.

> Security staff were working 14 hours a day, 7 days a week.
> People stopped caring after 3 weeks.

Raised Questions:

- Which insight into sad details of military actions should be given to the sovereign of a democratic society?
- Which dangers arise from disclosures of military operational details by ethically motivated whistle blowers?

Edward Snowden

Story:

- Had access document access as former CIA employee and US government contractor.
- Developed a backup system for NSA; had virtually unlimited access to NSA data.
- Disclosed classified information on the NSA global surveillance programs.
- Revelations had high impact on the debate on surveillance.

Raised Questions:

- Where are the limits to a state in surveilling its population?
- Where are the limits to a state in protecting its population from perceived threats?
- Which forms of cyber security measures are required
  for protecting security agencies against insider attacks?
- What are proper means for regulating surveillance institutions?

Julian Assange

Story:

- Unclear role in many interesting whistleblower cases.
- Editor in Chief of Wikileaks
- Provides storage space and redactorial editing (debated) of non-public material

Raised Questions:

- Which information belongs to the general public in a democratic society?
- Which amount of transparency is adequate,
  necessary or detrimental for a democratic society?
- Which duties does a publisher have in protecting sources?

Appendix

Contents of Appendix

Contents of Appendix	
List of Figures	LoF
List of Tables	LoT
List of Rights	©
Terms of Use	§
Citing This Document	→
List of Slides	🗺

List of Figures

List of Tables

List of Rights

Fig. 1	Source: https://www.esat.kuleuven.be/cosic/blog/another-rsa-challenge-broken/
Fig. 2	Source: https://www.esat.kuleuven.be/cosic/blog/another-rsa-challenge-broken/
Fig. 3	Source: https://blog.v-comply.com/256-bit-encryption/

Terms of Use (1)

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.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise Par 60a UrhG ermöglichen.

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.

Use of Logos and Trademark Symbols: The logos and trademark symbols used here are the property of their respective owners. The YouTube logo is used according to brand request 2-9753000030769 granted on November 30, 2020. The GitHub logo is property of GitHub Inc. and is used in accordance to the GitHub logo usage conditions `https://github.com/logos` to link to a GitHub account. The Tweedback logo is property of Tweedback GmbH and here is used in accordance to a cooperation contract.

Terms of Use (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt für mich ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status ich nicht oder nur mit unverhältnismäßig hohem Aufwand abklären kann. Ebenso kann ich den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen lassen, obwohl ich – und in letzter Konsequenz Sie als Leser – ihre Leistungen nutzen.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungssystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungssysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Citing This Document

If you use contents from this document or want to cite it,
please do so in the following manner:

Clemens H. Cap: Understanding the Attacker. Electronic document. https://iuk.one/1033-1006 7. 5. 2021.

Bibtex Information: https://iuk.one/1033-1006.bib

```
@misc{doc:1033-1006,
   author      = {Clemens H. Cap},
   title       = {Understanding the Attacker},
   year        = {2021},
   month       = {5},
   howpublished = {Electronic document},
   url         = {https://iuk.one/1033-1006}
}
```

Typographic Information:
Typeset on May 7, 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

List of Slides

Legend:
⧉ continuation slide
○ slide without title header
▨ image slide