

# Forearmed.

## Phishing Attacks and Password Cracking.

---

Prof. Dr. Andreas Aßmuth

Technical University of Applied Sciences  
OTH Amberg-Weiden

Department of Electrical Engineering, Media and  
Computer Science

2021-05-29

Professor of Computer Networks and Mathematics

Dean of Studies

Teaching:

Mathematics, Computer Networks, Cryptography, Coding Theory,  
Information Security

Research:

Applied Cryptography, Information Security, Ethical Hacking

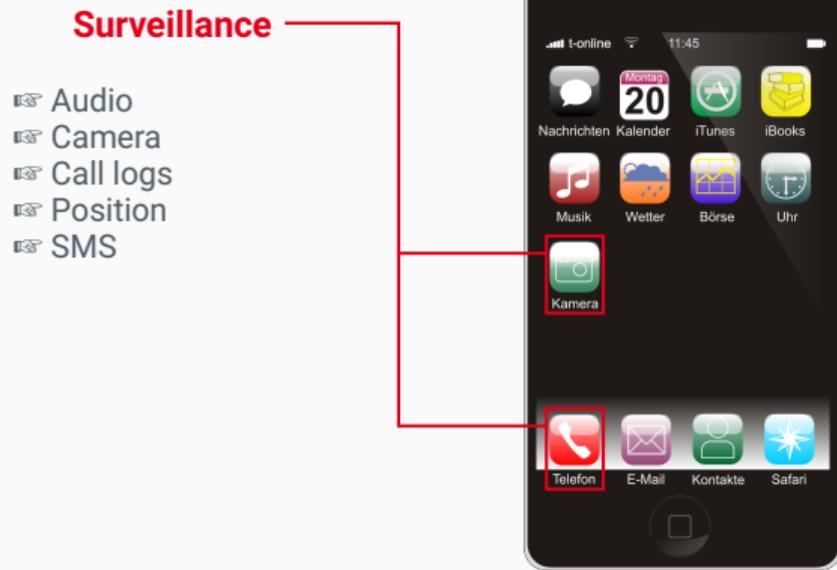
IARIA Fellow



# Anatomy of a Hacked Smartphone



# Anatomy of a Hacked Smartphone



## Surveillance

### Data Theft

- ☞ Account infos
- ☞ Contacts
- ☞ Call logs
- ☞ Theft through apps
- ☞ Device infos (IMEI)



# Anatomy of a Hacked Smartphone

Surveillance

Data Theft



**Money**

- ☞ Premium SMS
- ☞ Theft of TANs
- ☞ Ransomware
- ☞ Fake Antivirus
- ☞ Overpriced calls

# Anatomy of a Hacked Smartphone

Surveillance

Data Theft



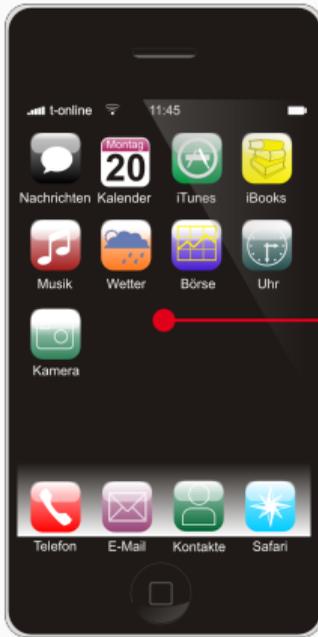
Money

## Faked Identity

- ✉ Re-routing of SMS
- ✉ Sending emails
- ✉ Posts on social media

Surveillance

Data Theft



Money

Faked Identity

**“Zombie Smartphone”**

- ☞ DDoS attacks
- ☞ Clickbait

Cryptographic hash functions must have certain **properties**:

- (i) Fast and easy computation of hashes.

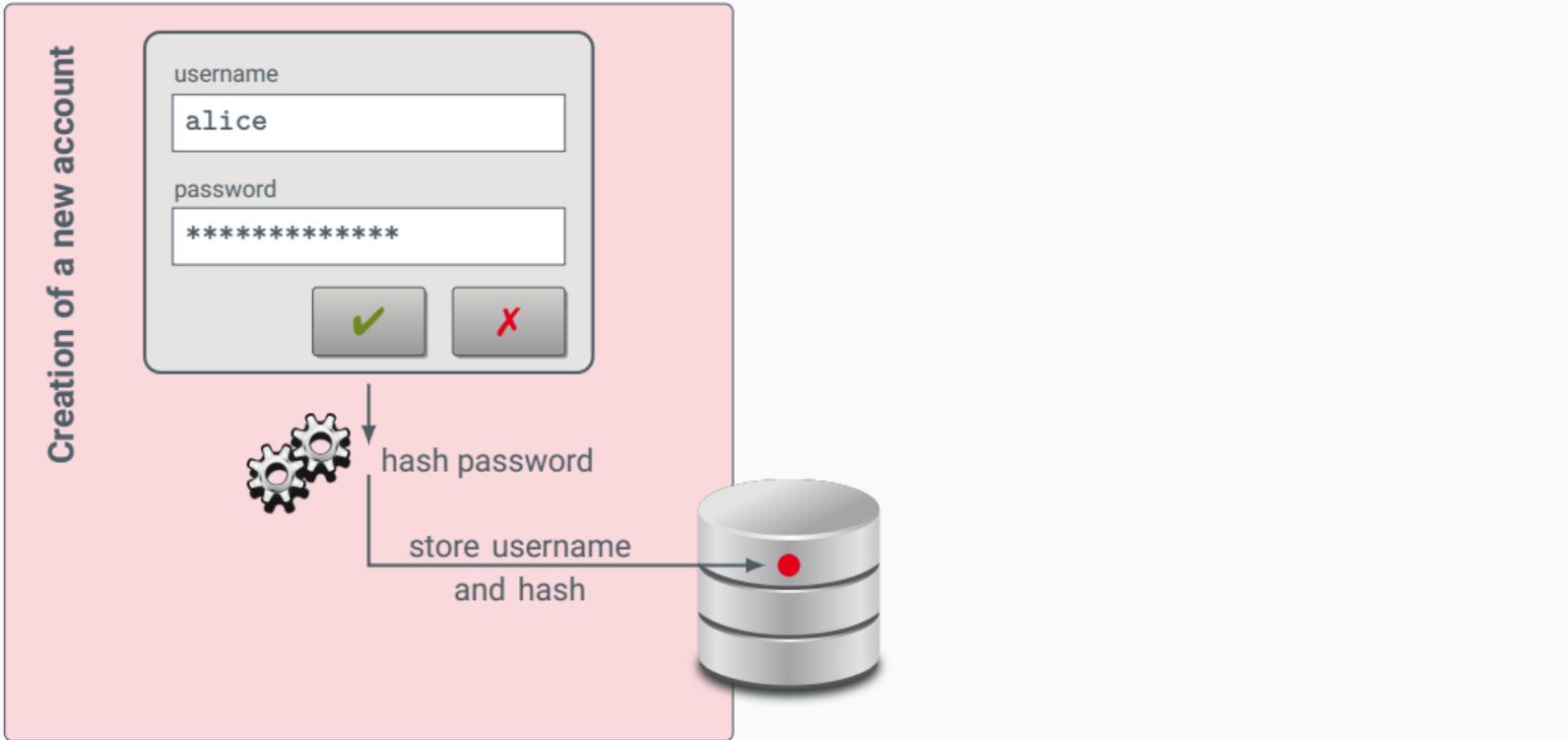
Cryptographic hash functions must have certain **properties**:

- (i) Fast and easy computation of hashes.
- (ii) One-way function: Given a hash, it must be infeasible to find an input that generates exactly that hash.

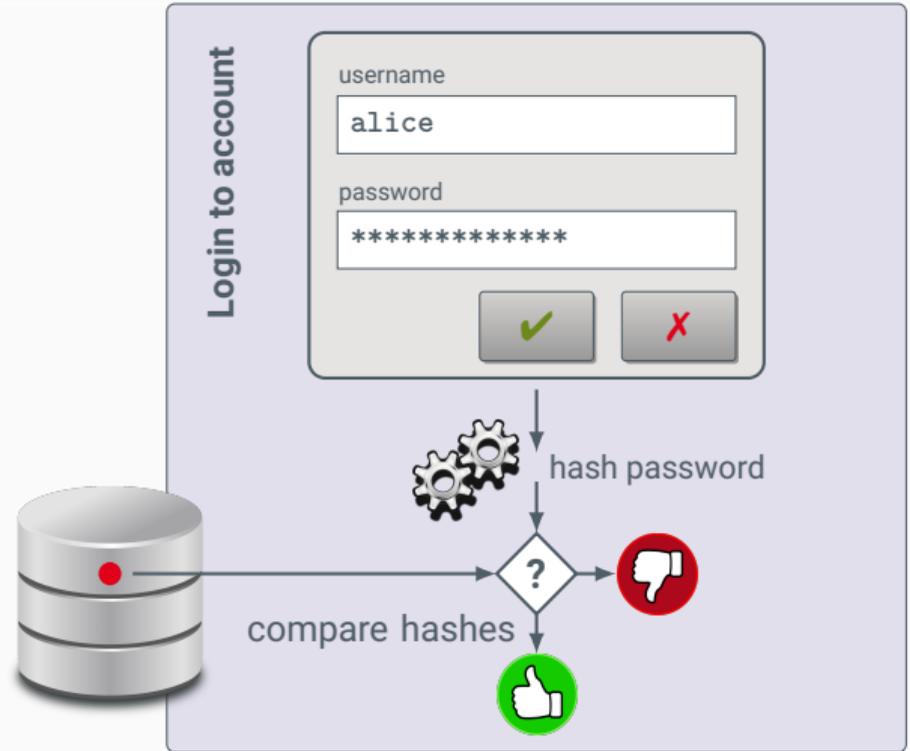
Cryptographic hash functions must have certain **properties**:

- (i) Fast and easy computation of hashes.
- (ii) One-way function: Given a hash, it must be infeasible to find an input that generates exactly that hash.
- (iii) Collision resistance: It must not be possible to find any two inputs that generate the same hash.

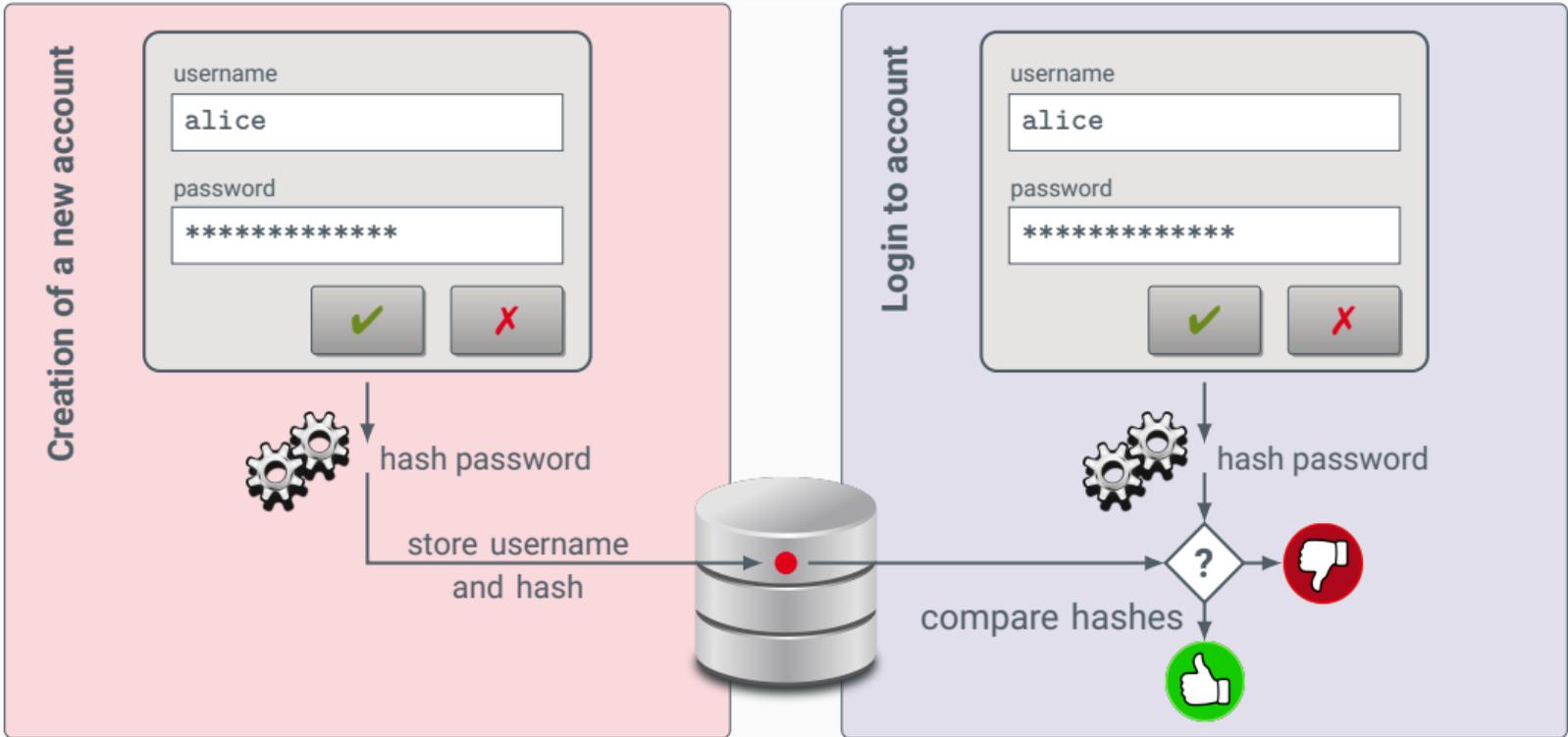
# How Does a Login Procedure Work?

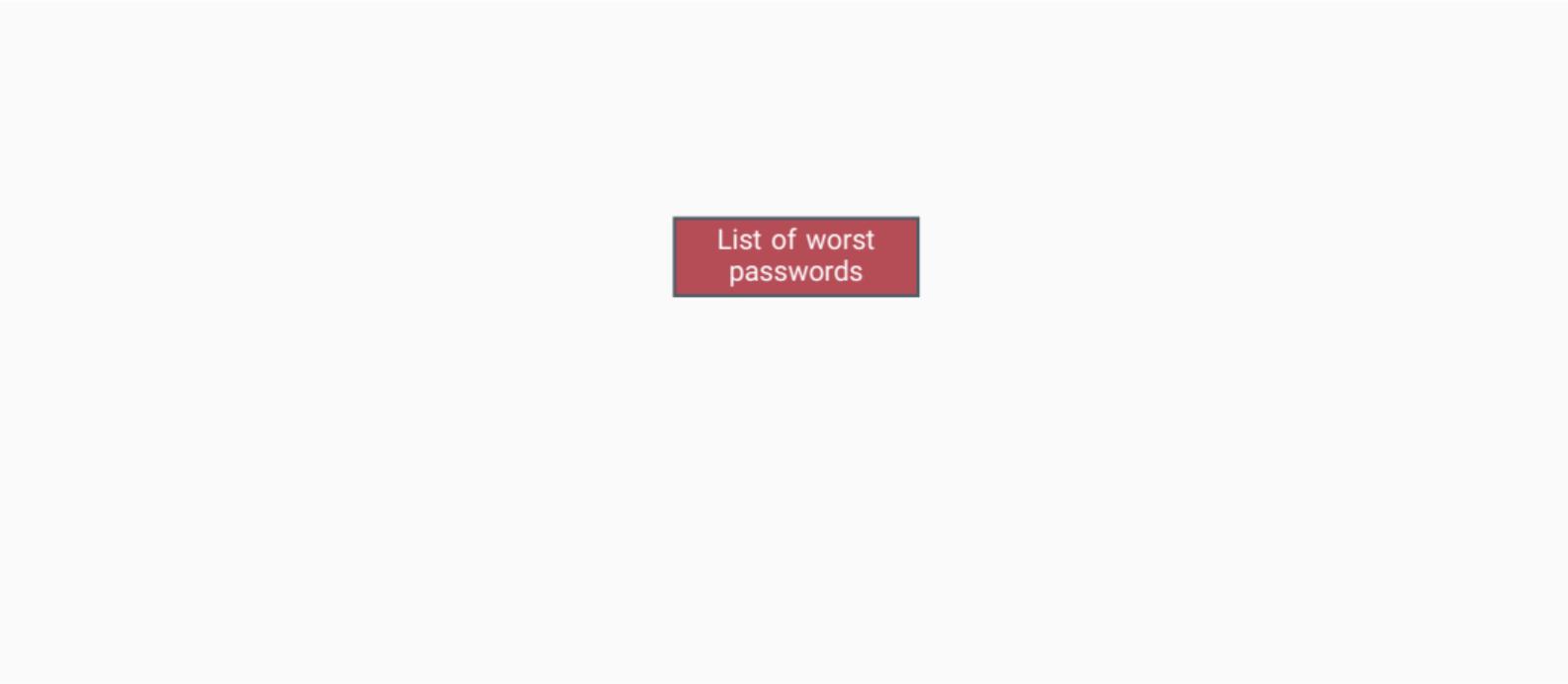


# How Does a Login Procedure Work?



# How Does a Login Procedure Work?





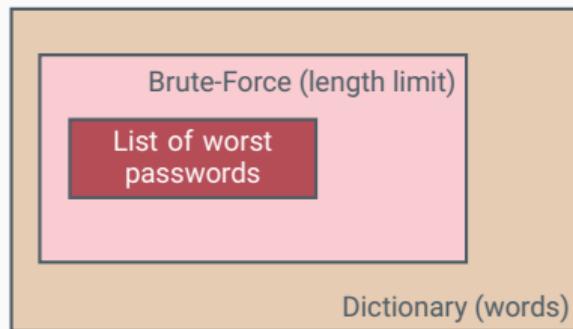
List of worst passwords

Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

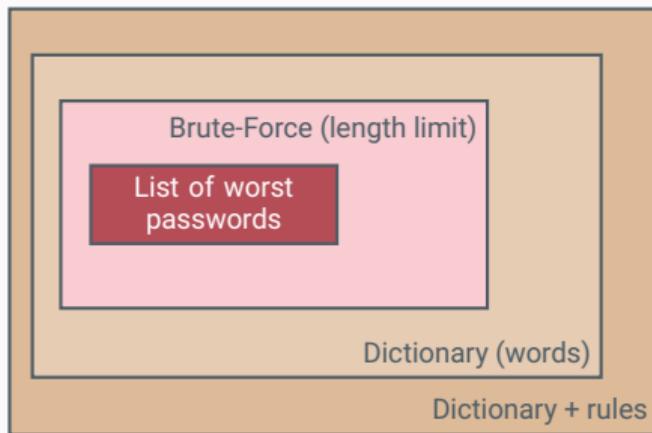
Brute-Force (length limit)

List of worst  
passwords

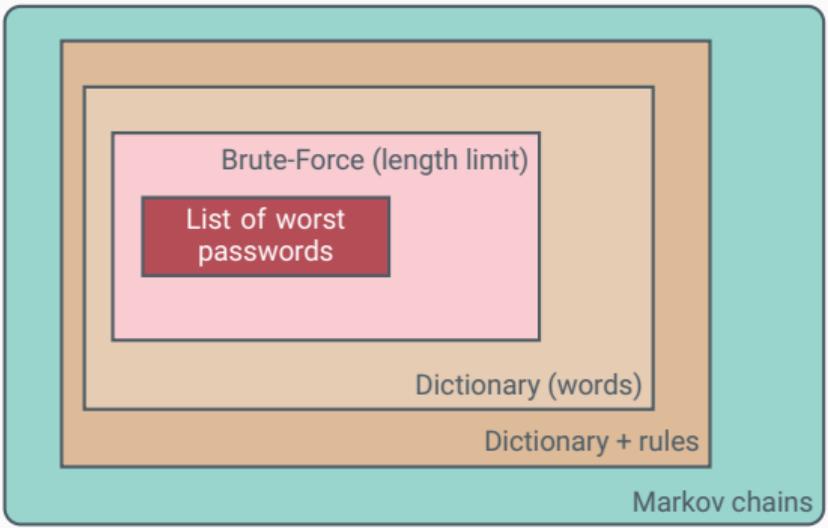
Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.



Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

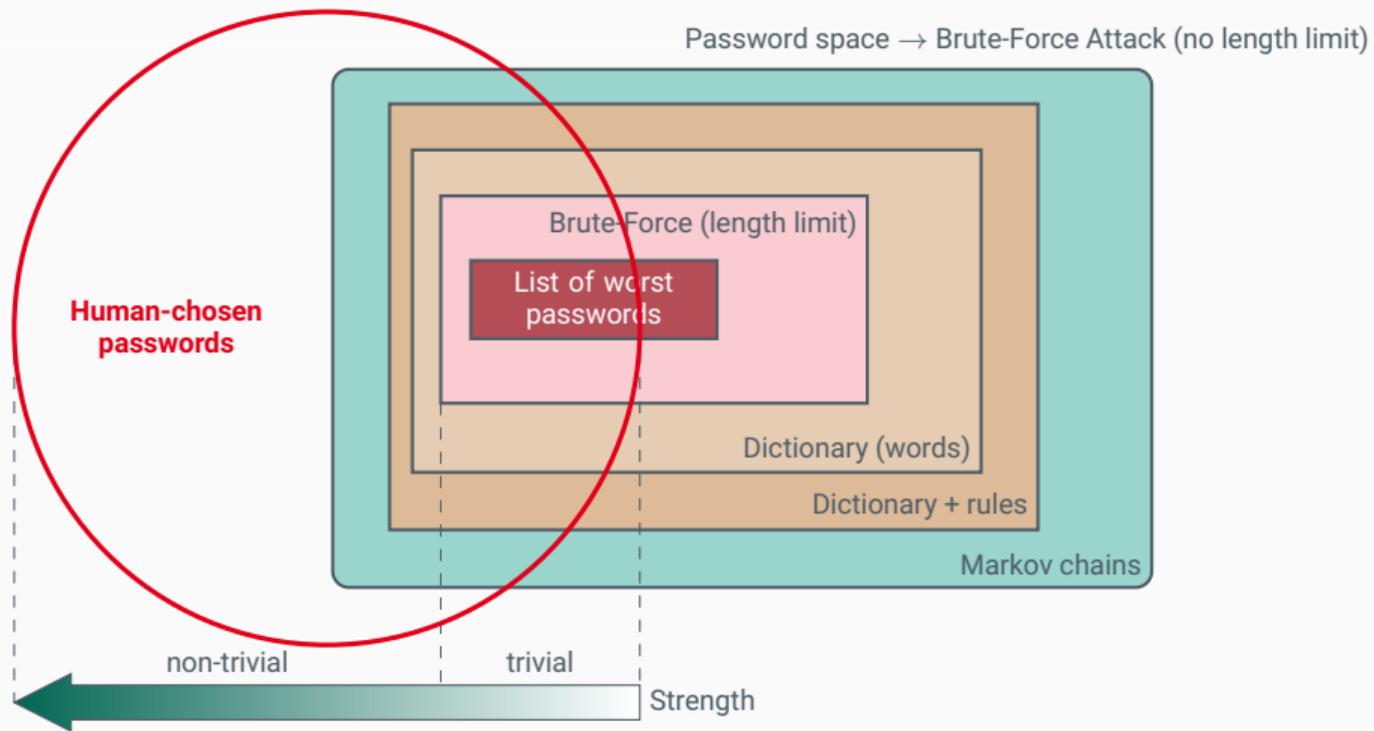


Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.



Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

# Password Cracking Offline Attack



Password space → Brute-Force Attack (no length limit)

Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

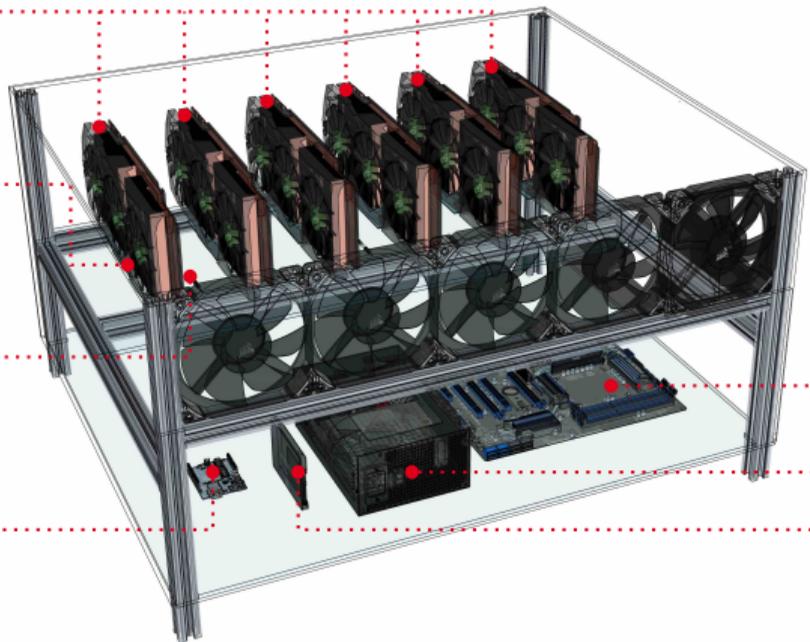
# Grapucino Graphic Processing Unit Cluster in a Box

Graphics Cards  
GeForce GTX 1080

Riser Adapter Boards  
1x → 16x

Temperature Sensors

Fan Control  
Arduino Uno



Mainboard  
Asus Mining Expert

Power Supply  
1600 W

256 GB SSD

Figure created by Tobias Nickl, M.Sc.

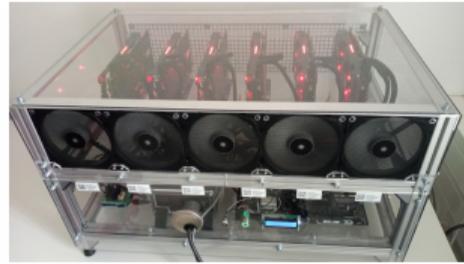
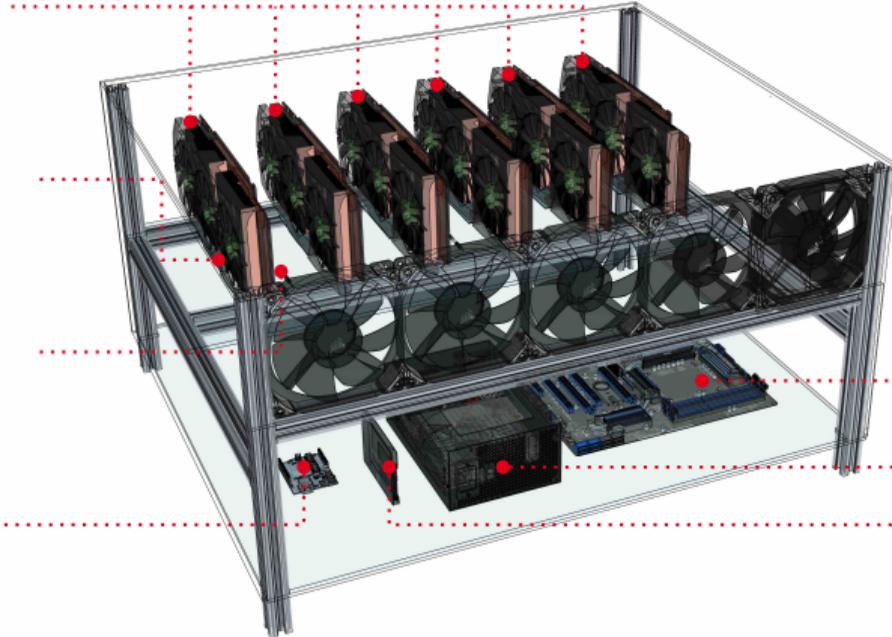
# Grapucino Graphic Processing Unit Cluster in a Box

Graphics Cards  
GeForce GTX 1080

Riser Adapter Boards  
1x → 16x

Temperature Sensors

Fan Control  
Arduino Uno



Power Supply  
1600 W

256 GB SSD

Figure created by Tobias Nickl, M.Sc.

Demonstration

# Secure Passwords Summary

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &amp; 3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS)</p>	<p>~28 BITS OF ENTROPY</p> <p><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOKEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: <b>EASY</b></p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: <b>HARD</b></p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p><math>2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>DIFFICULTY TO GUESS: <b>HARD</b></p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source: Randall Munroe, <https://xkcd.com/936/>

Von Amazon Kundensupport <info@clientsupportpanel.org> ☆  
Betreff: **Ihre Bestellung wurde storniert!**  
An a.assmuth@haw-aw.de ☆



[Meine Bestellung](#) | [Mein Konto](#) | [Amazon.de](#)

**Bestellung storniert**  
Referenz: #471-1086479-5478260

Guten Tag,

aufgrund diverser Widrigkeiten während des Bestellablaufs, wurde Ihr Nutzerkonto zum Schutz vorsorglich gesperrt. Womöglich erfolgte ein unberechtigter Zugang auf Ihr Konto.

Bitte bestätigen Sie sich als primärer Kontoinhaber, um eine erneute Wiederaufnahme der Handlungsfähigkeit des Kontos zu realisieren.

Folgen Sie dazu bitte den Hinweisen am Ende dieser Benachrichtigung.

Zustellung:

**Dienstag, 5. September 2017 -  
Mittwoch, 6. September 2017**

Versandart:

**Standardversand**

Die Bestellung geht an:

**Radoslav Sapisacut  
Packstation 131  
Arnulf-Klett-Platz 2  
Stuttgart, Baden-Württemberg  
70173  
Deutschland**

## Einzelheiten Ihrer Bestellung

Bestellung: #471-1086479-5478260

Aufgegeben am 3. September 2017



Apple iPhone 7 Smartphone (11,9 cm (4,7 Zoll), 128GB  
interner Speicher, iOS 10) matt schwarz  
Zustand: Neu  
Verkauft von: Amazon EU S.a.r.L.

**EUR 729,00**

Zwischensumme:	EUR 590,49
Verpackung und Versand:	EUR 0,00
Zwischensumme ohne USt:	EUR 590,49
Umsatzsteuer:	EUR 138,51
<b>Endbetrag inkl. USt:</b>	<b>EUR 729,00</b>

Die Wiederherstellung der uneingeschränkten Handlungsfähigkeit Ihres Kundenkontos, erfolgt unverzüglich nach erfolgreichem Abschluss des Verifizierungsprozesses.

Verifizierung starten

Bitte achten Sie bei Ihren Angaben auf die korrekte Schreibweise, da eine Wiederherstellung bei erheblicher Abweichung zu den hinterlegten Daten, nur noch über den Postweg möglich ist.

Wir bedauern diese Unannehmlichkeiten,

**Amazon.de**

Von Amazon Kundensupport <info@clientsupportpanel.org> ☆  
Betreff: **Ihre Bestellung wurde storniert!**  
An a.assmuth@haw-aw.de ☆



[Meine Bestellung](#) | [Mein Konto](#) | [Amazon.de](#)

**Bestellung storniert**  
Referenz: #471-1086479-5478260

Guten Tag,

aufgrund diverser Widrigkeiten während des Bestellablaufs, wurde Ihr Nutzerkonto zum Schutz vorsorglich gesperrt. Womöglich erfolgte ein unberechtigter Zugang auf Ihr Konto.

Bitte bestätigen Sie sich als primärer Kontoinhaber, um eine erneute Wiederaufnahme der Handlungsfähigkeit des Kontos zu realisieren.

Folgen Sie dazu bitte den Hinweisen am Ende dieser Benachrichtigung.

Zustellung:

**Dienstag, 5. September 2017 -  
Mittwoch, 6. September 2017**

Versandart:

**Standardversand**

Die Bestellung geht an:

**Radoslav Sapisacut  
Packstation 131  
Arnulf-Klett-Platz 2  
Stuttgart, Baden-Württemberg  
70173  
Deutschland**

## Einzelheiten Ihrer Bestellung

Bestellung: #471-1086479-5478260

Aufgegeben am 3. September 2017



Apple iPhone 7 Smartphone (11,9 cm (4,7 Zoll), 128GB  
interner Speicher, iOS 10) matt schwarz  
Zustand: Neu  
Verkauft von: Amazon EU S.a.r.L.

**EUR 729,00**

Zwischensumme:	EUR 590,49
Verpackung und Versand:	EUR 0,00
Zwischensumme ohne USt:	EUR 590,49
Umsatzsteuer:	EUR 138,51
<b>Endbetrag inkl. USt:</b>	<b>EUR 729,00</b>

Die Wiederherstellung der uneingeschränkten Handlungsfähigkeit Ihres Kundenkontos, erfolgt unverzüglich nach erfolgreichem Abschluss des Verifizierungsprozesses.

 <https://gglks.com/8i43k>

Bitte achten Sie bei Ihren Angaben auf die korrekte Schreibweise, da eine Wiederherstellung bei erheblicher Abweichung zu den hinterlegten Daten, nur noch über den Postweg möglich ist.

Wir bedauern diese Unannehmlichkeiten,

**Amazon.de**

## Phishing Example 2



## Phishing Example 2



The screenshot shows a webmail interface in a Chromium browser window. The title bar reads "Mail-Nachricht Von: Rechenzentrum – OTH Amberg-Weiden <lspg2018100932@ispgaya.pt> - Chromium". The address bar shows "webmail.oth-aw.de". The interface includes standard email actions like "Antwort", "Weiterleiten", and "Verschieben". The email header shows it is from "Rechenzentrum – OTH Amberg-Weiden" dated "Donnerstag, 13. Mai 2021 20.28 Uhr". The subject is "Ihr Postfachspeicher ist überschritten". The main body of the email contains a warning about a mailbox limit and a link to a malicious website: <https://thewhiteroomcreative.com/it-service.oth-aw.de/>. The email is signed off by "Prof. Dr. Schmid, Harald" from "Rechenzentrum – OTH Amberg-Weiden".

Mail-Nachricht Von: Rechenzentrum – OTH Amberg-Weiden <lspg2018100932@ispgaya.pt> - Chromium

webmail.oth-aw.de

✖ ◀ ▶ ↶ Antwort ↷ Antwort an alle ➦ Weiterleiten 📁 Verschieben ✉ Als 'Ungelesen' kennzeichnen

🗑️ Löschen 🖨️ Ansicht drucken 📄 📄

**Mail** Eigenschaften

Von: **Rechenzentrum – OTH Amberg-Weiden** Donnerstag, 13. Mai 2021 20.28 Uhr  
<lspg2018100932@ispgaya.pt>

An: noreply@oth-aw.de

Betreff: **Ihr Postfachspeicher ist überschritten**

Ihr Postfach hat das vom Standardadministrator festgelegte Limit überschritten. Sie können keine neuen oder ausstehenden Nachrichten mehr empfangen. Ignorieren Sie nicht, um zu verhindern, dass Ihr E-Mail-Konto vom Serveradministrator abgemeldet wird. Aktualisieren Sie jetzt, um Ihr Postfachkonto weiter zu verwenden.

[🔒 https://thewhiteroomcreative.com/it-service.oth-aw.de/](https://thewhiteroomcreative.com/it-service.oth-aw.de/)

Mit freundlichen Grüßen,  
---

Prof. Dr. Schmid, Harald  
Rechenzentrum – OTH Amberg-Weiden

New programme against COVID-19

 **GOV UK Notify** <michaelnhs@deeededraz.com>  
Friday, March 6, 2020 at 3:39 AM  
[Show Details](#)

---

 **GOV.UK**

---

**The government has taken urgent steps to list coronavirus as a notifiable disease in law**

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund (rebate)* of 128.34 GBP.

[Access your funds now](#)

The funds can be used to protect yourself against COVID-19(  
<https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona )

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

Singapore Specialist : Corona Virus Safety Measures

---

 Tuesday, 28 January 2020 at 03:51  
[Show Details](#)

---

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

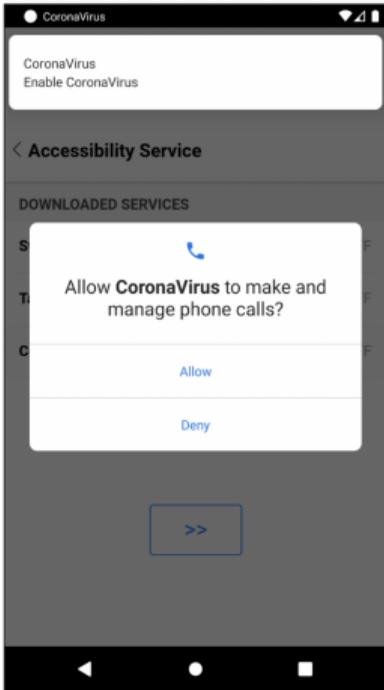
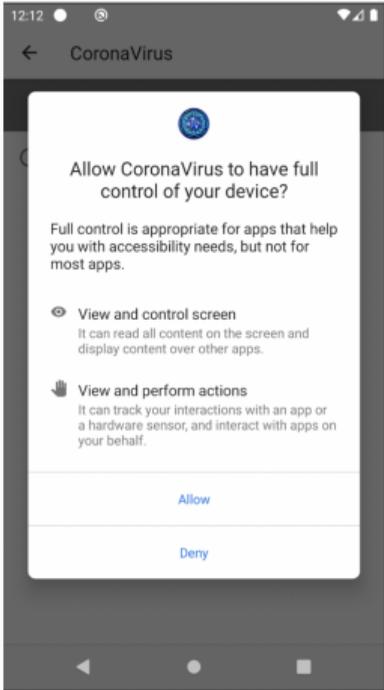
Use the link below to download

[Safety Measures.pdf](#)

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards  
Dr. [Redacted]  
Specialist wuhan-virus-advisory  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

# Malicious COVID-19 Apps



Demonstration

