

Was ist Kryptographie und wie geht das?



ag-link.xyz

14. Mai 2019

- 1 Threat modelling
- 2 Passwörter
- 3 Smartphone
- 4 Laptop

Threat Model: Definition

- A way of thinking about the sorts of protection you want for your data so you can decide which potential threats you are going to take seriously.
- It's impossible to protect against every kind of trick or adversary, so you should concentrate on which people might want your data, what they might want from it, and how they might get it.
- Coming up with a set of possible threats you plan to protect against is called threat modeling or assessing your risks.

Threat Model a.k.a Security Plan

- A way of thinking about the sorts of protection you want for your data so you can decide which potential threats you are going to take seriously.
- It's impossible to protect against every kind of trick or adversary, so you should concentrate on which people might want your data, what they might want from it, and how they might get it.
- Coming up with a set of possible threats you plan to protect against is called threat modeling or assessing your risks.

Threat Model a.k.a Security Plan

- A way of thinking about the sorts of protection you want for your data so you can decide which potential threats you are going to take seriously.
- It's impossible to protect against every kind of trick or adversary, so you should concentrate on which people might want your data, what they might want from it, and how they might get it.
- Coming up with a set of possible threats you plan to protect against is called threat modeling or assessing your risks.

- 1 Was möchte ich schützen?
- 2 Vor wem möchte ich es schützen?
- 3 Wie gravierend sind die Konsequenzen, falls ich scheitere?
- 4 Wie wahrscheinlich muss ich die Dinge tatsächlich schützen?
- 5 Wie aufwändig ist es, die Dinge zu schützen?

Was möchte ich schützen?

- Sensible Informationen
- Metadaten
- Personenbezogene Daten
- Geräte
- ...

Todo: List of Assets

- Welche Daten halte ich vor?
- Wo liegen diese Daten?
- Wer hat Zugang dazu?
- Was hindert andere am Zugriff?

Was möchte ich schützen?

- Sensible Informationen
- Metadaten
- Personenbezogene Daten
- Geräte
- ...

Todo: List of Assets

- Welche Daten halte ich vor?
- Wo liegen diese Daten?
- Wer hat Zugang dazu?
- Was hindert andere am Zugriff?

Vor wem möchte ich meine Daten schützen

- Polizei
- Regierungen
- Unternehmen
- Politische Gegner:innen
- Diebstahl
- Brand
- ...

Todo: List of Adversaries

- Angreifer
- Jene, die Deine Daten gerne hätten.

Vor wem möchte ich meine Daten schützen

- Polizei
- Regierungen
- Unternehmen
- Politische Gegner:innen
- Diebstahl
- Brand
- ...

Todo: List of Adversaries

- Angreifer
- Jene, die Deine Daten gerne hätten.

Wie gravierend sind die Konsequenzen, falls ich scheitere?

- Ich werde getrackt
- Ich werde aufgespürt
- Ich werde erpresst
- Ich verliere Daten
- Ich verliere Geräte

Todo: List of Consequences

- Was kann mit meinen Daten angestellt werden?
- Was kann mit meiner Hardware passieren?

Wie gravierend sind die Konsequenzen, falls ich scheitere?

- Ich werde getrackt
- Ich werde aufgespürt
- Ich werde erpresst
- Ich verliere Daten
- Ich verliere Geräte

Todo: List of Consequences

- Was kann mit meinen Daten angestellt werden?
- Was kann mit meiner Hardware passieren?

Wie wahrscheinlich muss ich die Dinge tatsächlich schützen?

- Hausdurchsuchungen
- Polizeigesetze
- Digitale Durchsuchungen
- Diebstahl

Todo: List of Threats

- Welche Gefahren sind ernst zu nehmen?
- Welche sind sehr unwahrscheinlich oder harmlos?
- Welche sind unvermeidbar oder nicht abwehrbar?

Wie wahrscheinlich muss ich die Dinge tatsächlich schützen?

- Hausdurchsuchungen
- Polizeigesetze
- Digitale Durchsuchungen
- Diebstahl

Todo: List of Threats

- Welche Gefahren sind ernst zu nehmen?
- Welche sind sehr unwahrscheinlich oder harmlos?
- Welche sind unvermeidbar oder nicht abwehrbar?

Öffentlichkeit

„Zwiebelfreunde“-Durchsuchungen: Wenn Zeugen wie Straftäter behandelt werden

Ein Spendenaufruf auf der Vereinswebseite reicht, um die bayerische Polizei bei Tagesanbruch durch die Wohnungstür marschieren zu lassen. Anlass für die Aktion war eine eher fadenscheinige Verbindung zu einem strittigen Demo-Aufruf. Wir sprachen nach dem Einsatz mit den Betroffenen vom Verein „Zwiebelfreunde“, die sich zu Unrecht kriminalisiert sehen.

04.07.2018 um 10:28 Uhr - Alexander Fanta - 123 Ergänzungen

MOTHERBOARD



Image: Shutterstock. Remix: Jason Koebler

SURVEILLANCE | By Joseph Cox | Jan 8 2019, 6:08pm

I Gave a Bounty Hunter \$300. Then He Located Our Phone

T-Mobile, Sprint, and AT&T are selling access to their customers' location data, and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country.

Wie aufwändig ist es, die Dinge zu schützen?

- Vollverschlüsselung der Festplatte
- Verschlüsselte Kommunikation
- Starke, einzigartige Passwörter
- Alternatives BIOS
- Start-Systemzustand signieren

Optionen

- Welche Optionen stehen zur Verfügung, um konkrete Gefahren abzuwehren?
- Finanzielle Bedingungen
- Technische Bedingungen, Know-How
- soziale Zwänge

Wie aufwändig ist es, die Dinge zu schützen?

- Vollverschlüsselung der Festplatte
- Verschlüsselte Kommunikation
- Starke, einzigartige Passwörter
- Alternatives BIOS
- Start-Systemzustand signieren

Optionen

- Welche Optionen stehen zur Verfügung, um konkrete Gefahren abzuwehren?
- Finanzielle Bedingungen
- Technische Bedingungen, Know-How
- soziale Zwänge

Wie aufwändig ist es, die Dinge zu schützen?

- Vollverschlüsselung der Festplatte
- Verschlüsselte Kommunikation
- Starke, einzigartige Passwörter
- Alternatives BIOS
- Start-Systemzustand signieren

Optionen

- Welche Optionen stehen zur Verfügung, um konkrete Gefahren abzuwehren?
- Finanzielle Bedingungen
- Technische Bedingungen, Know-How
- soziale Zwänge

Wikipedia:

- The Intel Management Engine (ME) [...] is an autonomous subsystem that has been **incorporated in virtually all of Intel's processor chipsets since 2008.**
- It is a part of Intel Active Management Technology, which allows system administrators to **perform tasks on the machine remotely.**
- The Intel Management Engine **always runs as long as the motherboard is receiving power, even when the computer is turned off.**
- The IME is an attractive target for hackers, since it **has top level access to all devices and completely bypasses the operating system**

Was sind Passwörter?

- Passwörter sind Geheimnisse
 - Wie geht ihr mit euren Geheimnissen um?
- Passwörter werden überall eingesetzt
 - Anmeldungen bei Onlinedienst
 - Verschlüsselung von Kommunikation, Dateien und Geräten

- Passwörter müssen **sicher** sein!

- Schwache Passwörter genutzt
 - „password“- häufigstes Passwort weltweit
 - „p@ssw0rd“- simple Ersetzungen
 - „passwordpasswordpassword“- 3fach hält besser
 - „katzenfutter“- steht im Wörterbuch
 - „johannes96“- persönliche Infos als Passwort
- Passwörter mehrfach verwendet
 - Nutzerdatenbank gestohlen (Adobe, MySpace, Patreon)
 - Pishing
- <https://haveibeenpwned.com/>

- Seid ihr betroffen?
- **Schwache Passwörter genutzt**
 - Durch starke, einfach zu merkende Passwörter ersetzen!
- Passwörter mehrfach verwendet
 - Passwortmanager einsetzen, damit ihr euch nicht eure vielen, starken Passwörter merken müsst!

Was macht ein Passwort stark?

- Passwortlänge (Wie viele Zeichen?)
- Zeichenraum (Welche Zeichen sind möglich?)
 - 0-9 = 10
 - a-z & A-Z = 52
 - Sonderzeichen und Erweitertes ASCII
- Zeichenraum^{Passwortlänge} = mögliche Passwörter
 - Zeichenraum (0-9), Passwortlänge (4 - 8)
 - $10^4 = 10000 \Rightarrow 10^8 = 100000000$
 - Zeichenraum (0-9a-zA-Z), Passwortlänge (4 - 8)
 - $62^4 = 14776336 \Rightarrow 62^8 = 2.183401056 \times 10^{14}$
- Passwortlänge ist wichtiger als Zeichenraum!

Wie gehen Angreifer vor?

- Bruteforce: „12345“
 - Wörterbuch: „GanzGanzSicheresPasswort“
 - Maskenangriff/Regelbasiert: „johannes96“
 - Sprachstruktur: „IchbinJohannes“
-
- Ziel ist die Masse der Nutzer mit schwachen Passwörtern
 - Angriffe durch Geheimdienste?

Wie bekommt man sichere Passwörter?

- Zufällig generieren
 - „'uVm7**h(Dp!AV.&zjKHf,Tvs';2Kp“
- Passwortmanager das Generieren übernehmen lassen
- Wer kann sich so ein Passwort merken?

Was hat Ihr Passwort mit Pizza zu tun?

Denken Sie sich einen Satz aus, der mindestens eine Zahl enthält, zum Beispiel:

„**A**m liebsten esse ich **P**izza mit vier **Z**utaten und extra **K**äse!“



Merken Sie sich nun den ersten Buchstaben eines jeden Wortes und Sie erhalten ein starkes und sicheres Passwort.

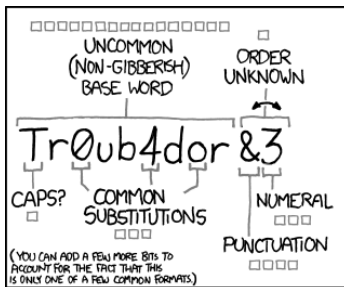
AleiPm4Z+eK!



Tip:
Nutzen Sie Passwort-Manager!
Das sind Apps oder Software-Programme,
die alle Ihre Passwörter und die zugehörigen
Benutzernamen sicher verwalten. Sie brauchen
sich dann nur ein sicheres Masterpasswort für
den Passwort-Manager merken.

Wie bekommt man sichere Passwörter?

- Längere Sätze verkürzen
 - „Am 4.5. hab ich bei einer Crypto-Party mitgemacht und jetzt kann die NSA mich mal!“
 - „A4.5.hibeC-PmujkdNSAmm!“
- Schon eher merkbar, aber immer noch kompliziert!



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

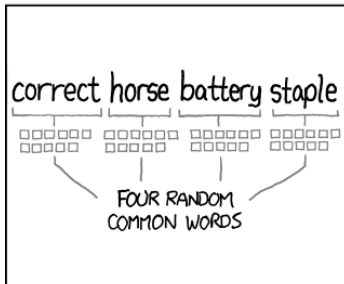
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O'S WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

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.

Wie bekommt man starke Passwörter?

- Worte auswürfeln und aneinanderreihen
 - „Ich bereitete diesen Vortrag vor und lag dabei am Meer, da kam jemand vorbei, gab mir einen Handschlag, trug dabei eine Guccijacke und da hatten wir ne tolle Freundschaft.“
 - „vortrag*meer*handschlag*guccijacke*freundschaft“
- Länger, aber du hast es dir jetzt schon gemerkt, oder?

Wie sicher muss mein Passwort sein?

Desired password entropy H	Arabic numerals	Case sensitive alphanumeric	All ASCII printable characters	All extended ASCII printable characters	Diceware word list
8 bits (1 byte)	3	2	2	2	1 word
32 bits (4 bytes)	10	6	5	5	3 words
40 bits (5 bytes)	13	7	7	6	4 words
64 bits (8 bytes)	20	11	10	9	5 words
80 bits (10 bytes)	25	14	13	11	7 words
96 bits (12 bytes)	29	17	15	13	8 words
128 bits (16 bytes)	39	22	20	17	10 words
160 bits (20 bytes)	49	27	25	21	13 words
192 bits (24 bytes)	58	33	30	25	15 words
224 bits (28 bytes)	68	38	35	29	18 words
256 bits (32 bytes)	78	43	39	33	20 words

- Lieblingstier, Lieblingsessen, 2. Vorname deiner Mutter?
- Dienen dazu, deine Identität zu „bestätigen“
- Niemals echte, öffentlich zugängliche oder „errätbare“ Antworten geben
- Stattdessen zufällig generierte Antworten!

- Passwörter sind Geheimnisse
 - Fingerabdruck, Gesicht, Iris, etc. sind nicht geheim
 - Risiko: Speichern von Merkmalen auf Gerät oder zentral in Datenbank
- Weiterführende Infos: Starbug CCC Talks

- Seid ihr betroffen?
- Schwache Passwörter genutzt
 - Durch starke, einfach zu merkende Passwörter ersetzen!
- **Passwörter mehrfach verwendet**
 - Passwortmanager einsetzen, damit ihr euch nicht eure vielen, starken Passwörter merken müsst!

Was sind Passwortmanager?

- Anwendung, die eure Passwörter für euch generiert, verwaltet, speichert (& auch eingibt)
- merken müsst ihr euch nur ein starkes Master-Passwort
- Für jeden Dienst wird ein zufälliges, starkes Passwort generiert
- Integration in Browser via Add-ons

Was spricht gegen Passwortmanager?

- Single Point of Failure
 - Risiko: Masterpasswort und Passwortdatenbank gestohlen
- Angreifer haben ein erfolgversprechendes Ziel
- Sicherheitslücken existieren. Immer.
 - Open-Source statt Closed-Source

- Neben eurem Master-Passwort wird ein 2. Faktor als zusätzlicher Schlüssel genutzt \Rightarrow zusätzliche Sicherheit
 - Schlüsseldatei auf Gerät
 - Verifizierungscode per SMS
 - One-Time-Passwort auf 2. Gerät (Google Authenticator)
 - YubiKey
- Wenn ihr 2FA benutzt, dann ist darf eure 2. „Schlüssel“ nicht neben dem 1. Schlüssel liegen

- Ihr braucht also eigentlich nur Passwörter für:
 - Festplattenverschlüsselung
 - Login in Benutzeraccount (Ubuntu)
 - Master-Passwort für Passwortmanager
 - Email-Account

Wie geht ihr mit euren 4 Passwörtern um?

- Optimal: Auswendig lernen
- Auch noch gut: Aufschreiben, aber dann sicher verwahren!
- Threat-Model beachten:
 - Wohnt ihr allein?
 - Wo (auch außerhalb der Wohnung) könnt ihr Dinge sicher lagern?
 - Hausdurchsuchung?

- Manuell? Sicher, aber echt unpraktisch!
- Dann wohl automatisch über „die Cloud“, aber wie?
- LastPass, 1Password, etc.
 - Single Point of Failure
 - Ziel von Angriffen
 - Angriffe waren bisher öfter erfolgreich
- **Dann wohl selber machen!**
- Oder: Firefox Sync / Lockbox!

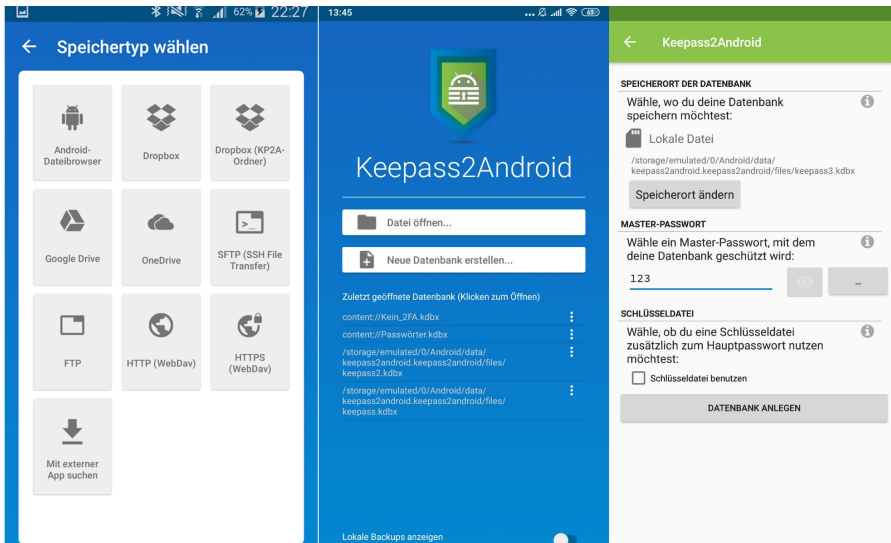
Was ist zu beachten?










- Backup euren Passwort-Datenbank erstellen und auf USB, SD-Karte etc. lagern
- Social engineering, Datenverlust und Sicherheitslücken bei Diensten sind der Regelfall
- Passwortmanager bringen nichts, wenn Spyware auf dem Gerät läuft
- Passwörter können gegen euch verwendet werden. Was passiert bei Verhaftung/Hausdurchsuchung/Grenzüberschreitung?







- Starke Passwörter sind zentral für digitale Selbstverteidigung
- Benutzt Passwortmanager für alles außer eure 4 Passwörter
- Passwortlänge ist wichtiger als Zeichenraum
- Passwörter regelmäßig wechseln (aber richtig!)
- Passwörter sind kein Garant für Sicherheit


- plattformübergreifend (Windows/Mac/Linux)
- aktive Entwicklung
- Homepage: <https://keepassxc.org>
- Installation bei Ubuntu über Software-Store oder
- „sudo apt install keepassxc“


- aktive Entwicklung
- Homepage: <https://github.com/PhilippC/keepass2android>
- Installation über Playstore






-  **eMail**
Gruppe - 0 Einträge >
-  **General**
Gruppe - 0 Einträge >
-  **Homebanking**
Gruppe - 0 Einträge >
-  **Internet**
Gruppe - 9 Einträge >
-  **Network**
Gruppe - 0 Einträge >
-  **Windows**
Gruppe - 0 Einträge >
-  **Sample Entry**
User Name >
-  **Sample Entry #2**
Michael321 >
-  **Zeit test**
Hans >


	Benutzername	⋮
	User Name	
	URL	⋮
	http://keepass.info/	
	Kennwort	⋮
	
	Kommentare	⋮
	Notes	
	Erstellt	
	07.05.2013 06:28	
	Letzte Änderung	
	07.05.2013 06:28	


Name 


Benutzername  **User Name**


password   


.....

Webadresse  <http://keepass.info/>

Notiz  **Notes**

 ZUSÄTZLICHES FELD HINZUFÜGEN

 DATEIANHANG HINZUFÜGEN...

 tag1, tag2



- Da Passwortdatenbank verschlüsselt ist, können auch kommerzielle Clouddienste genutzt werden (Dropbox, Google Drive, etc.)
- Für zusätzliche Sicherheit kann eine eigene Nextcloud betrieben werden
- Client auf euren Geräten



← Speichertyp wählen



Android-
Dateibrowser



Dropbox



Dropbox (KP2A-
Ordner)



Google Drive



OneDrive



SFTP (SSH File
Transfer)



FTP



HTTP (WebDav)



HTTPS
(WebDav)



Keepass2Android



Datei öffnen...



Neue Datenbank erstellen...

Zuletzt geöffnete Datenbank (Klicken zum Öffnen)

content://Kein_2FA.kdbx

content://Passwörter.kdbx

/storage/emulated/0/Android/data/
keepass2android.keepass2android/files/
keepass2.kdbx

/storage/emulated/0/Android/data/
keepass2android.keepass2android/files/

Was kann mit meinem Handy passieren?

- Dauerndes Mikrophon
- Dauernde Kamera
- Alle Chats & alle Mails
- Gesamter Browserverlauf
- Dauerndes Standorttracking
-
- ...

Wie können wir angegriffen werden ?

aktiver Angriff

- Direkter Angriff aufs Gerät
- Auffälliger
- Wenn erfolgreich kompletter Zugriff auf alles

passiver Angriff

- Belauschen der Funkkommunikation des Geräts
- Schwerer zu bemerken
- Weniger Informationen können abgegriffen werden

Wie sieht ein aktiver Angriff auf ein Handy aus?

Wie kann es funktionieren?

- Hacking des Gerätes
- Physischer Zwang (Pozilei/nette Leute an der Grenze)

Folgen:

- Kompletter Kontrollverlust über das Gerät
- Möglicherweise dauerhafter Verlust
- Kompletter Verlust aller Daten auf dem Gerät

Wie sieht ein passiver Angriff auf ein Handy aus?

- IMSI-Catcher
- Mitschneiden des Internet-Traffics
- Bluetooth-Catcher
- Mitschneiden an zentralen Knotenpunkten

- Vor aktiven Angriffen:
 - Verschlüsseln des Gerätes
 - Aussageverweigerung von Passwörtern (Selbstbelastung)
 - System aktuell halten
 - möglicherweise alternatives Betriebssystem installieren
- Vor passiven Angriffen:
 - ⇒ Verschlüsselt Kommunizieren: sichere Messenger benutzen

Was ist denn ein sicherer Messenger?

	WhatsApp	Telegram	Signal	Wire
verschlüsselt	ja	nein	sehr gut	sehr gut
Metadatenschutz	nein	nein	ja	ja
Privacy default	ja	nein	ja	ja
5-Eyes Server	ja	nein	nein	nein
Open Source	nein	jein	ja	ja
Perfekt Secrecy	ja	nein	ja	ja
Usablility	5/5	5/5	3/5	4/5
auf dem Handy?	ja	ja	ja	ja
auf dem PC?	jein	ja	jein	ja

Was kann meinem Laptop passieren?

- Dauerndes Mikrophon
- Dauernde Kamera
- Alle Chats & alle Mails
- Gesamter Browserverlauf
- ...

Was kann mit meinem Laptop passieren?

Was kann meinem Laptop passieren?

- Dauerndes Mikrophon
- Dauernde Kamera
- Alle Chats & alle Mails
- Gesamter Browserverlauf
- ...

Was kann mein Laptop

- Zugang zum Darknet
- IP-Adresse verschleiern
- verschlüsselte Kommunikation
- eigene Kontrolle über das Gerät

Welche Bedrohungen habe ich?

Quasi die selben wie für Smartphones.

- Mehr als beim Smartphone
- Alles beginnt mit einer Linux-Installation
 - Festplattenverschlüsselung
 - verschlüsselte Mail
 - verschlüsselter Messenger
 - custom UEFI
 - reproduzierbar Builds
 - Epoxy in den USB-Ports
 - ...

Oh No, Linux ist doch das mit der schwarzen Commandline

Nicht mehr.

Ubuntu ist für den Start zu empfehlen und user-friendly.

HIER BEISPIELINSTALLATION EINFÜGEN

The End