

Graphene-Os

GrapheneOS ist ein mobiles Betriebssystem, welches auf Android basiert. Häufig wird es empfohlen, da es eine Alternative zu vorinstallierten (OEM) Betriebssystemen darstellt, welche gänzlich ohne Google-Services genutzt werden kann. Neben diesem Merkmal, welches die Privatsphäre von Nutzer*innen schützt, bietet GrapheneOS in Kombination mit unterstützten Geräten hochmoderne Sicherheitsfeatures, wegen derer wir die Nutzung an dieser Stelle stark empfehlen.

Einstellungen Empfehlungen

Datenschutz & Sicherheit

Exploit protection

- auto reboot: so niedrig wie möglich, aber für die Anwendenden noch komfortabel! (nach Reboot kommen ohne erstmaliges Entsperren z.B keine Signalnachrichten/anrufe mehr an)
- USB - C Port: hier sollte mindestens "Charging only" gewählt werden. "Charging only when locked" ist nochmal eine Stufe strenger (potentiell besser), führt aber dazu, dass das Handy nicht mehr geladen werden kann, wenn es gleichzeitig benutzt werden muss.
 - Hier könnte es sich empfehlen standardmäßig "Charging only when locked" auszuwählen und im Zweifel direkt zu wissen, wie die Einstellung auf "Charging only" geändert werden kann, wenn dies nötig ist.
- WiFi & Bluetooth automatisch ausschalten: Hier sollte bei Beiden eine noch komfortable Zeitspanne gewählt werden.
- Geräteentsperrung

Geräteentsperrung

- Duress Passwort: Dieses Passwort sorgt dafür, dass wenn es eingegeben wird, das Handy komplett auf Werkseinstellungen zurückgesetzt wird. Das ist sehr praktisch, solltet ihr einmal gegängelt/gezwungen o.ä. werden euer Handy zu entsperren. Das funktioniert übrigens auch, falls ein Angreifer versucht euer Passwort per Brute-Force zu erraten. Voraussetzung ist natürlich, dass auf dem Gerät keine lebensnotwendigen Daten sind, von denen ihr keine Backups habt. Wählt für das Duress Passwort also am besten eins:
 - an das ihr euch im Zweifel sofort erinnert!

- das die Polizei z.B erraten würde
- oder: eins, dass ihr für euer richtiges Passwort niemals wählen würdet.

WiFi

Für sämtliche WiFi's, über die nicht ihr selber die volle Kontrolle habt:

- In die Einstellung der jeweiligen Verbindung (Zahnrad bei WiFi-Name): nicht persistente MAC-Adress-Generierung für diese Verbindung aktivieren.

2FA für Fingerprint

Seit kurzer Zeit gibt es die Möglichkeit einen zweiten Faktor für die Entsperrung per Fingerprint zu nutzen. Das bringt einen enormen Fortschritt im Spannungsfeld zwischen Usability und Security mit sich!

Wo war bisher das Problem?

Im Normalfall ist es ja so, dass biometrische Entsperrmethoden mit äußerster Vorsicht zu genießen sind, aus dem einfachen Grund, dass sie von euch erzwingbar sind. Die Polizei kann im Zweifel euren Finger mit Gewalt auf euer Handy legen und es entsperren.

Das heißt bisher ging die Nutzung der biometrischen Entsperrung immer einher mit der Gefahr überrumpelt und zum Entsperren gezwungen zu werden, bevor das Handy ausgeschaltet werden kann.

Wie schaut die Lösung aus?

Die 2FA Option bietet die Möglichkeit einen mindestens 4-stelligen (empfohlen werden 6Stellen) Zahlen PIN einzurichten, der jedes mal nach dem Fingerprint zusätzlich einzutippen ist, um das Handy zu entsperren.

Dann muss zwar trotzdem noch etwas getippt werden, aber einen z.B 6-stelligen PIN auf dem großen Zahlen-Pad ist viel einfacher und schneller getippt, als eine 7 Wörter lange Passphrase auf der kleinen Tastatur. Außerdem lässt sich der PIN viel entspannter ändern (wenn es sein muss), da man keine große Sorge davor haben muss, jetzt ein neues langes Passwort lernen zu müssen.

Das bedeutet das Handy kann mit einem sehr starken Passwort verschlüsselt werden, ohne dass man nun dieses elendig lange Passwort etliche Male am Tag eintippen muss.

Kann der PIN nicht gebrute-forced werden?

Nur sehr eingeschränkt:

- Die gesamte Fingerprint-Methode ist nur 48h nach der letzten Eingabe des primären (langen) Passworts.

- Es sind maximal $4 * 5$ Fehlversuche erlaubt. Zwischen jedem 5. Fehlversuch gibt es eine 30 sekündige Auszeit. Es gibt also maximal 20 Fehlversuche. [1]

PIN Scrambling

PIN scrambling ist ziemlich nerdig, hat aber durchaus seine Anwendungsfälle:

Anstatt dass die Ziffern immer in numerischer Reihenfolge auf dem Bildschirm angezeigt werden, werden die Ziffern bei der PIN-Eingabe an zufälligen Stellen auf dem Bildschirm angezeigt. Wenn euch also ein Angreifer aus kleiner Entfernung dabei beobachtet hat, wie ihr euren PIN eingegeben habt, in der er nur z.B. die Richtung des Daumens auf dem Bildschirm erkennen konnte, ist der PIN für ihn nicht rekonstruierbar.

PIN scrambling ist auch für die 2FA beim Fingerprint verfügbar.

Version #2

Erstellt: 27 Januar 2025 21:43:00 von ESC-IT Migration Bot

Zuletzt aktualisiert: 11 Februar 2025 13:17:56 von ESC-IT Migration Bot