Spezial System für hohen mobilen und sicheren Einsatz auf Reise, was ist möglich?

Beitrag von „Ghostbuster“ vom 20. Oktober 2023, 16:20

Hallo Community

Ich möchte hiermit ein besonderes Thema neu beginnen und hoffe auf reich Teilnahme und viel Feedback, danke im Vorfeld.

Es geht darum ein System aus mobilem Computer & Telefon in Betriebssymbiose für Reisen und erschwerte Bedingungen ein zu richten.

Grundsätzlich spielt Gewicht, Akkulaufzeit und Leistung sowie Funktionalität in allen Unternehmen eine wichtige Rolle, geknüpft an Datensicherheit und Datenschutz. Und das heist im Umkehrschluss.. selber machen und nicht an die kommerziellen Lösungen halten;) Daher würde ich gerne ein bestehendes MacBook aus älterer Generation mit Opencore ganz speziell an die Bedürfnisse anpassen oder einen modernen Laptop wie z.B. von Lenovo gezielt so einrichten das meine Ansprüche erfüllt werden können.

Erste Frage, hat sich schon mal wer damit beschäftigt ein oder mehrer Geräte für Bedingungen von Reise und Expedition ein zu richten?

Hat wer ggf. Erfahrung mit Drittanbietern von Komplettlösungen oder andere Anregungen zum Thema?

Aktuell habe ich noch ein überholtes MacBook 5,5 das mit OC bis Monterey vollständig unterstützt arbeitet, habe aber noch keine Verschlüsselungen und Bios- Sicherheiten ausprobiert und weis auch nicht in wie weit man das zu machen kann. Wenn hier schon wer mal "Versuche" gemacht hat, würde mich das auch interessieren. Auf jeden Fall soll eine USB-Dongel in Verbindung mit Kennwort/Fingerabdruck etc. nötig sein um das Gerät in den Betrieb zu bringen. Die Speicherung von Passwörtern und die Erstellung muss auch abhängig von den drei Faktoren sein und darf nur auf dem Dengle gespeichert werden. Eine Backup bzw. Recovery Strategie ist natürlich stets von Vorteil;-)

Über eure Anregungen würde ich mich sehr freuen, Grüße.

Beitrag von „apfel-baum“ vom 20. Oktober 2023, 16:24

nen tragmich + tails? https://tails.net/

lg

Beitrag von „Ghostbuster“ vom 20. Oktober 2023, 16:48

> Zitat von apfel-baum
>
> nen tragmich + tails? https://tails.net/
>
> lg

..das schau ich mir direkt mal an, danke.

Bin für alle Anregungen offen, da ich noch keine Entscheidung getroffen habe was ich speziell angehen werde, daher "mit machen" früher oder später müssen wir in diese Richtung denken.. spätestens dann, wenn dir der Laptop geklaut wurde und DU feststellst, WHAT A FUCK

Beitrag von „apfel-baum“ vom 20. Oktober 2023, 16:50

ggf. auch wenns win ist, win + veracrypt container

ledit-

sowie biospasswort setzen, auch was booten und bioslogin angeht- neuere lenovos haben z.b. eine tamperdetection (die merken wenn die unterteilabdeckung ab ist)-und dann ist der tragmich quasi e-schrott, da damit nix mehr anzufangen ist

lg

Beitrag von „Ghostbuster“ vom 20. Oktober 2023, 17:02

Zum Glück bin ich von WIN inzwischen "völlig" gelöst, das rennt.. wenn überhaupt.. dann nur in einer VM;-)

Als ehm. Microsoft Certified Engineer sag ich nur = Zeitverschwendung;-)

Gut das ich mit HP UX groß geworden bin

Ok, zurück zur Sache..

Beitrag von „mhaeuser“ vom 21. Oktober 2023, 09:34

Ganz ehrlich, hol’ dir ein Apple Silicon MacBook und gut ist. Die Idee mit “natürlich ist selber gemacht besser” ist Tagträumerei. Die Arbeit, die es braucht, ein Linux so sicher zu machen wie macOS, will sich niemand antun. Das fängt bei den simpelsten Sachen an wie Dateiauthentifizierung (das Linux-Userland hat nicht mal wirklich ein Konzept davon) und hört bei so etwas wie SIP auf. Aufgrund einer Doppelfunktion als Pseudorandomisierung für’s write levelling ist die SSD-Verschlüsselung auch komplett ohne Leistungseinbußen und hat allgemein keine Nachteile. Die SSD ist natürlich auch kryptographisch a den SoC gebunden, daher nach Ausbau wertlos. Bis du mit Linux, dm-verity, fs-verity und TPM da rankommst, ist das Ding wieder Altmetall. Und mit Hackintosh hast du alle üblichen Nachteile, wie fummliges Secure

Boot, oft kein ordentliches Boot Guard, usw.

Alte Geräte verwenden ist immer so eine Sache. Die neuen Sicherheitskonzepte sind alle sehr speziell und kein Normalsterblicher braucht sie unbedingt, aber du willst doch keine 3(!!)-Faktor-Authentifizierung und dann ist dir egal, dass die Firmware von Schadsoftware befallen sein könnte. Da hilft kein OpenCore und kein selbst machen der Welt, da braucht es Boot Guard oder eben alles ab Apple T2. Zur 3-Faktor-Authentifizierung fallen mir nicht mal Lösungen ein, weil das so eine Niche ist.

Beitrag von „Ghostbuster“ vom 22. Oktober 2023, 11:12

> Zitat von mhaeuser
>
> Ganz ehrlich, hol’ dir ein Apple Silicon MacBook und gut ist.

Danke dir für deine Einschätzung. Tatsächlich überlege ich mir ein neues MacBook Air zu holen, da es mir auch einige Vorteile in der Mobilität gibt, was mit dem alten Schinken nich so einfach möglich ist.

Mit dem M-Chip von Apple habe ich keine Erfahrungen, leider weis ich auch nicht welche "Air's" denn wirklich was taugen.. ich habe schon so einiges gehört, das nicht jeder inzwischen mit den neuen Geräten des Herstellers zufrieden is. Natürlich nur hören-sagen, denn bei mir fehlt die Erfahrung.

Ich behalte den Gedanken mal offen und schau nebenher was denn fürs mittlere Geld an Geräten gerade zur Hand ist;)

Beitrag von „guckux“ vom 24. Oktober 2023, 14:43

Grundsätzlich möchte ich mich mhaeuser anschließen.

Wenn Du wenig bis keine Probleme haben möchtest - nen MacBook Mx... Ausstattung je nach

Portokasse, Leistung haben selbst die "kleinen".

Wenn Du es selbst machen möchtest - Linux wie auch zB *BSD unterstützen auch cryptisierte filesysteme, Das sollte auch ohne Performance Verlust gehen.

Bei Linux wichtig selinux auf enforce zu setzen, die Basis-Installation selbst ist meist schon recht gut. Oder auch OpenBSD...

Den freien gemein ist, daß Du wissen solltest, was Du tust, tun musst und kannst. Das ist dann unter dem sportlichen Ehrgeiz "geil" aber nicht jedermann's Sache.

Im Hinterkopf sollte man sich behalten, daß macOS mittlerweile einen höheren Marktanteil hat als vor "Jahren" und hier auch mehr in den Focus der Hacker rückt.

- einer der Gründe, weshalb bei mir im Heim kein M$ mehr existent ist...

Beitrag von „krokol“ vom 24. Oktober 2023, 16:51

Vieles hängt von den Umständen der Reise und dem intendieren Einsatz ab. Bei Expedition ist vermutlich erst mal die Frage nach den physikalischen Anforderungen - Gewicht, Größe, Robustheit, Staubschutz, ggf. mögliche Betriebs- & Lagertemperatur. Dann ist noch zu klären, wie die Stromversorgung (zuverlässig) funktioniert.

Prinzipiell halte ich ein Mx MacBook Air auch für eine vermutlich brauchbare Wahl: kein Lüfter, keine beweglichen Teile, wenig Möglichkeiten, dass Staub und Sand ins Gehäuse dringen und Schaden anrichten. Zudem sehr lange Akkulaufzeit. Ggf. Ports zusätzlich versiegeln und Folien auf Gehäuse und Bildschirm. Wenn es aber in Gebiete mit besonders hoher Luftfeuchtigkeit geht oder die Geräte (z.B. nachts) besonders tiefen Temperaturen ausgesetzt sind, kann das trotzdem zu Korrosion bzw. zu Akkuschäden führen. Bei einem MBA wäre es gewichtstechnisch evtl. sinnvoll, ein identisch konfiguriertes Ersatzgerät dabei zu haben - Problem ist aber, dass die Daten verschlüsselt auf einem nicht wechselbaren internen Speicher liegen ... also wenn tot, dann erst mal tot. Linux ist gut und schön, aber wenn da jemand erst mal rumbasteln soll, setzt das Know-how und ggf Vorbereitung voraus.

Das führt zur nächsten Anforderung: Gibt es im Fall des Falles vor Ort das Know-how und die

realistische Möglichkeit, etwas zu reparieren bzw. eine verkorkste Installation zu retten? Gibt es eine regelmäßige Online-Datenverbindung? Mit welchem Datendurchsatz, mit welcher Hardware, zu welchen Kosten?

Weiterhin zum Thema "sicher": Was sind die Bedrohungsszenarien? Welche Sorgen treiben dich/das Projekt um? Datensicherheit? Verfügbarkeit und Zuverlässigkeit der Software? Des Betriebssystems? Der Hardware?

Welche zusätzlichen Anforderungen bestehen? Irgendwelche Peripherie, die angebunden werden muss? Irgendwelche Software, die unbedingt genutzt werden muss und das OS vorgibt?

Auch zu bedenken: Alte Notebooks brauchen oft zusätzliche Netzteile - ein weiteres Teil, das kaputt gehen kann und für das man ggf. Ersatz braucht. Aktuelle MBAs werden per USB-C geladen, ein passendes Netzteil gibt es quasi überall und es gibt ultrakompakte, Kabel in fast beliebiger Länge.

Drittanbieter-Lösungen, die ich kenne, beziehen sich zumeist auf die Robustheit (alles im Pelicase verpackt, dicke Hüllen, Folie über Tastatur, um Eindringen von Staub zu verhindern, zum Teil Mini-PC, Display und Tastatur separat statt Notebook), aber wie gesagt, es hängt vieles vom tatsächlichen Einsatz ab. Wer mit dem Rucksack in der Welt unterwegs ist hat andere Anforderungen als eine Expedition in die Wüste mit einem 15köpfigen Team (inkl. einem Techniker) und 6 Fahrzeugen.

Beitrag von „Ghostbuster“ vom 25. Oktober 2023, 09:42

Vielen Dank erstmal, das sind doch einige Anregungen und haben inzwischen einige neue Denkanstöße angeregt.

Nebenher schaue ich mir unterschiedliche OS Varianten an und mache meine ersten Test um zu entscheiden ob ich mich nach der Auswahl der Hardware, für ein Linux oder einen "echten" Mac entscheide.

Weiter habe ich ja noch ein MacBook Pro mit OC und kann hier mal ausprobieren was mir zum Basteln so einfällt;)

Ich bleibe weiter dran und lese mit was noch alles an Anregungen hier eingestellt wird - super!

Beitrag von „mhaeuser“ vom 25. Oktober 2023, 10:09

guckux Bzgl. Verschlüsselung meinte ich nicht “in den meisten Anwendungsfällen nicht spürbar langsamer”, sondern wortwörtlich keine Leistungseinbußen. Das kann eine Softwareverschlüsselung nicht leisten. Die Frage ist, ob das für die eigenen Anwendungsfälle einen Unterschied macht.

SELinux ist auch so eine Sache, da ist nichts mit einfach an und läuft. Bei einigen Standardkonfigurationen kann man einfach mit sudo die Konfigurationsdatei bearbeiten und, wenn nicht, kann man es oft noch einfach mit der GRUB-Konfiguration umgehen. An SIP, das einfach direkt aktiv ist und funktioniert, kommt das bei Weitem nicht ran. Entgegen der endlosen Lobgesänge der FOSS-Armeen kommt Linux im Bereich Endnutzersicherheit im Traum nicht an macOS ran, egal wie viel du da einstellst.

Beitrag von „Ghostbuster“ vom 25. Oktober 2023, 10:29

Hier bei dem MacBook 5,5 Hacki (Catalina bzw. Monterey) habe ich schon einiges probiert, da ich ja das UEFI von OC benötige und somit die Möglichkeit habe einen USB-Stick als Dongle um zu bauen.

Dh. ich habe das EFI nur aufm Stick, nicht mehr lokal. Den Keychain vom Schlüsselbund dort in einen gesicherten verschlüsselten Container gepackt und diesen als Standart angegeben. Zudem synchronisiert meine NAS meine persönlichen Dateien mit dem Stick. Dies ist eine Möglichkeit mir zusätzlich ein externes Medium zum Betrieb des Gerätes ein zu richten, ohne ist dann nur noch das Übliche auf dem System. Wenn jetzt noch FileVault mit OC läuft und ich den Dengle mit dem Masterkey verknüpfen kann, dann ist das zumindest mal eine erfolgreiche

Bastelei;)

Im Moment weis ich nicht ob es das neue MackBook Air 2023 mit Silicon wird oder eines aus den Generationen davor mit Intel- Chip. Bei letzterem habe ich halt mehr Möglichkeiten was Apps angeht.

PS: Diverse Linux- Forks habe ich mir auch schon angeschaut. Die welche ich aufm MackBook zum laufen bekommen habe und andere auf meinem Lenovo. Gibt einige die sich spezialisiert haben auf Minimals und Sicherheit, aber beim dritten Blick war nichts mit bei das mir langfristig keine Sorgen macht. Ich habe wohl weiter macOS im Auge.

Beitrag von „guckux“ vom 25. Oktober 2023, 10:48

mhaeuser

Hm, bei der Verschlüsselung habe ich nichts belegbares - ich weiß nur aus der Vergangenheit, daß in den 90igern für das task-management Linux und *BSD die Hardware des Intels genutzt hatten und somit ein limit von 8192 Prozessen hatten - das war den (Free-)BSDlern zuwenig und sie machten das in Software - keine limits mehr und einiges schneller/agiler (Walnut Creek lief dann zeitweise mit >12,000 FTP-Usern auf nem DualPentium Pro)

RAID ist ein weitere Technologie, welche Software-technisch ebenfalls nicht mehr hinter der Hardware "hinterherhinkt".

Bei den MacBooks unterstelle ich mal, daß die Verschlüsselung über "Co-Protz" realisiert wird (TPM-Chip?) - durchaus vorstellbar für mich, daß es in diesem Falle schneller ist.

SeLinux ist wahrlich recht komplex und nicht trivial im Management (ich habe es nie gelernt).

Beziehst du Dich mit Endnutzersicherheit auf das einfache Management? Ansonsten unterstelle ich, daß man ein UNIX durchaus mehr härten kann als das macOS in der Basis-Auslieferung - wenn man weiß wie und worauf man zu achten hat.

Beitrag von „Arkturus“ vom 25. Oktober 2023, 12:08

> Zitat von Ghostbuster
>
> ....
>
> ....
>
> **.... ein System aus mobilem Computer & Telefon in Betriebssymbiose .....**

> .....
>
> Alles anzeigen

was genau verstehtst Du unter 'Betriebssymbiose' und soll der Mobile Computer gleichzeitig auch das Telefon sein oder nur mit einem Telefon zusammenarbeiten? Ghostbuster

---

Beitrag von „Ghostbuster“ vom 25. Oktober 2023, 14:29

@Arkturus

..zusammen arbeiten reicht. Beim Handy ist mir wichtig das ich meine benötigten Apps einspielen kann und da sowas immer mal gerne entwendet wird, muß das einfach recht sicher sein. Gleichzeitig darf der Verlust oder ein technischer Ausfall nicht zur Katastrophe führen, eine schnelle Widerherstellung aus Backup auf ein neues Gerät muss fix möglich sein.

Gerade bei beiden Geräten ist Akkulaufzeit, Gewicht und Größte sowie Sicherheit gefordert.

Beitrag von „Arkturus“ vom 25. Oktober 2023, 14:50

Also wenn es ums Handy geht, dann erinnere ich mich nur an nervige Android , welche ich bis 2016 privat hatte und dann auf iOS umgestiegen bin. Android dann noch bis Anfang 2022 noch dienstlich nutzen musste.
Ich nutze mit iOS auch iCloud, wie auch mit den Möhren aus der Signatur. Ich schätze es sehr, wenn ich ein neues Gerät aus der Cloud einrichte und nahtlos alle Einstellungen, Passwörter und Daten auf dem neuen Gerät wiederfinde. Ob das mit Android oder diesen Dingsda aus Redmond möglich ist, vermag ich nicht zu beurteilen. Gehört oder gelesen habe ich darüber nichts, was aber nichts bedeutet. Die Zusammenarbeit von iOS mit macOS bedarf wohl keiner besonderen Erklärung in diesem Forum.
Hab keine Vorstellungen, was du während der Expeditionen für Daten erfassen und verarbeiten musst. Ich für meinen Teil schleppe auf Reisen nur noch mein Handy mit. Wenn noch ein Mobiler Computer sein soll, dann hast Du bereits besten Rat dazu erhalten.

Beitrag von „Capos81“ vom 25. Oktober 2023, 15:16

IMSI-Catcher Dan bist du leicht zu hacken das war’s mit der Reise Mobile Handy unsicher

---

Beitrag von „Ghostbuster“ vom 25. Oktober 2023, 15:21

@Capos81

Ja sowas wird mich ja hoffentlich nicht verfolgen;)

Mir geht es in erster Linie um Raub und Verlust durch Beeinflussung Dritter. Natürlich auch Defekt. Vor allem sollen die Daten in den Geräten nicht "so einfach" für andere offenliegen bzw. im Idealfall zu E-Schrott führen.

Beitrag von „mhaeuser“ vom 25. Oktober 2023, 15:25

guckux Was ist denn “einfaches Management”? Linux-Software ist nicht ordentlich signiert, das hinkt selbst Windows Vista hinterher. SELinux so einzurichten, dass man es nicht einfach mit Admin-Berechtigungen wieder abschalten kann, geht glaube ich auch nur “einfach” mit UKI. Selbst dann ist initrd generell nicht signiert. dm-verity ohne Distro-Unterstützung einzurichten ist auch nicht zielführend. Die Sandbox-Konzepte von Snap und Flatpak sind teils mangelhaft und lassen Lücken zum Ausbruch offen. Die hochgelobten Dateisystemberechtigungen werden, wenn sauber angewandt, von Windows in den Schatten gestellt, gerade im Punkt Bedienbarkeit. Mir ist wirklich nichts an UNIX-Konzepten bekannt, das im Bereich Sicherheit etwas taugt.

Beitrag von „Arkturus“ vom 25. Oktober 2023, 16:20

> Zitat von Capos81
>
> IMSI-Catcher Dan bist du leicht zu hacken das war’s mit der Reise Mobile Handy unsicher

was hat das mit Datensicherheit zu tun? Capos81

Beitrag von „Capos81“ vom 25. Oktober 2023, 17:07

Arkturus

Nix ist sicher !!! im Leben das hat es damit Zutun egal was du machst ist hackbar so einfach ist das was sicher ist dein Verstand was du mit deiner Daten machst

---

Beitrag von „Ghostbuster“ vom 25. Oktober 2023, 17:58

Na ja, ohne ab zu driften.. war es trotzdem interessant zu verstehen das heute einige Dinge möglich sind einen als Nutzer aus zu spionieren.

ich habe festgestellt das in den Fetnostländern die Leute sehr schlau geworden sind Diebesgut zu durchleuchten und es dann auch wieder zu verkaufen. Ich möchte einfach zwei- drei Level höher gehen als normal und mir, wenn es passiert, keinen Kopf machen müssen.. genau hier denke ich kann mammoth einiges vorbereiten.

Daher bin ich auch für alles offen, ohne erstmal zu kritisieren, ich versuche für mich dann was zu finden das meine Zwecke erfüllt und das gelingt in erster Linie mal durch Aufklärung und Anregung der Community.

Beitrag von „Arkturus“ vom 25. Oktober 2023, 23:14

Du verwechselt Äpfel mit Birnen Capos81

Aber an der Stelle bin ich ohnehin raus. Kann nichts mehr beitragen zu diesem Thema.

Beitrag von „guckux“ vom 26. Oktober 2023, 00:03

> Zitat von mhaeuser
>
> guckux Was ist denn “einfaches Management”?

Ich meinte damit den Aufwand hintendran, etwas "sicher" zu machen.

Und hier ist macOS mit einem "einfachen" Management versehen, welches einen hohen Grad an Sicherheit bietet - so meine subjektive Meinung...

Wenn ich dergleichen vorhaben würde, würde ich "eh" ein OpenBSD nehmen. Linux ist mir zu "verbreitet" - und die BSDler hatten gewisse Dinge in der Vergangenheit bereits professioneller gelöst.

Beitrag von „Capos81“ vom 26. Oktober 2023, 01:54

Wenn Du die richtigen Aspekte betrachtest wirst Du schnell erkennen dass Äpfel und Birnen mehr gemeinsam haben als Du vielleicht denkst Es ist wichtig sich bewusst zu machen dass Vergleiche nur dann sinnvoll sind wenn sie auf gemeinsamen Merkmalen und dem Kontext basieren Andernfalls kann es zu falschen Schlussfolgerungen und Missverständnissen kommen.

Beitrag von „Arkturus“ vom 26. Oktober 2023, 10:56

Telefonieren mittels Mobilfunk = Äpfel

Datennutzung und -verarbeitung auf dem Smartphone = Birnen

Beitrag von „Capos81“ vom 26. Oktober 2023, 12:19

kannst du mir mal sagen Bitte wie kann man sich von IMSI-Catcher schützen !!!

Warte auf deine Antwort ?

Beitrag von „Arkturus“ vom 26. Oktober 2023, 12:35

Tut mir leid, ich werde das Spiel nicht weiter mitmachen.

Beitrag von „Capos81“ vom 26. Oktober 2023, 12:39

Also weißt du das nicht wie das geht war ja klar das hier ist kein Spiel !

Beitrag von „Arkturus“ vom 26. Oktober 2023, 12:43

Es ist deine Weigerung zu unterscheiden und schiebst anderen die Verantwortung dafür zu.
so, letzte Meinung von mir dazu. Werde nicht mehr antworten.

Beitrag von „Capos81“ vom 26. Oktober 2023, 13:24

Ich selber weiß es wie es geht wollte es wissen ob du es auch kannst wie es aussieht weißt du nicht wie man sich schützen kann von IMSI-Catcher

---

Beitrag von „Ghostbuster“ vom 29. Oktober 2023, 18:38

Hallo und moin zurück

Es hat ein paar Tage gedauert einige unterschiedliche Versionen von Systemen auf diversen Geräten aus zu probieren.

Da es ja um zwei Geräte geht, habe ich für den Moment eine (wichtig: für mich interessante) Lösung gefunden was das Mobilgerät angeht.

Fü die welche interessiert mit lesen, hier meine Entscheidung zum Endgerät Handy.

Google Pixel 4A 5G mit GrapheneOS

Das Gerät läuft nun seit einigen Tagen um täglichen Gebrauch - Der Akku-Verbrauch ist minimal , System ist vollständig verschlüsselt und läßt auch keine forensic tools zu, zumindest nicht welche ich getestet habe. Weiter ist VPN (kostenfrei) eingerichtet und ich verwende eine reine Daten-SIM die ich demnächst noch auf die eSIM umstelle, damit ich den Slot frei habe. Telefonie läuft über Satellite-App.

Als nächstes gehe ich das Thema "Laptop" an, hier stehe ich noch am Anfang. Einige Sachen habe ich getestet, aber eigentlich hat nichts bestanden bwz. mich in Anwendung zu sehr beschränkt. Denke aber die kommenden Tage werde ich die Versuche ausweiten;)

PS: Was das IMSI-Catching angeht, das sollte man erstmal außen vor lassen und bei Interesse mal selber recherchieren. Ich habe dazu einiges von GSMK durchgelesen und andere Publikationen gelesen. Letztendlich hatte es keinen Auswirkung auf meine Entscheidung des zu benutzenden OS auf dem Handy, habe aber mit dem Pixel den Grundstein gelegt mir das genauer am Gerät in Echtzeit an zu schauen und somit auch schon die Schnittstellen geöffnet und einige kleine tools installiert für den Fall das ich da mal ein paar Test machen möchte um mich ggf. etwas zu schützen.