Tipps & Tricks

Sie fragen – wir antworten!

Mehrere FIDO-Sticks zur Linux-Authentifizierung

Im Artikel „Türsteher nach Maß“ (c’t 10/2019) erklären Sie, wie man einen FIDO-Stick verwendet, um U2F für komfortable Linux-Authentifizierung zu verwenden. Ich habe meinen Sicherheitsschlüssel wie beschrieben mit `pamu2fcfg > ~/.config/Yubico/u2f_keys` in der Konfigurationsdatei eingetragen. Jetzt möchte ich einen zusätzlichen FIDO-Stick hinterlegen, um mich wahlweise mit einem der beiden auszuweisen. Wie füge ich den zweiten Sicherheitsstick hinzu?

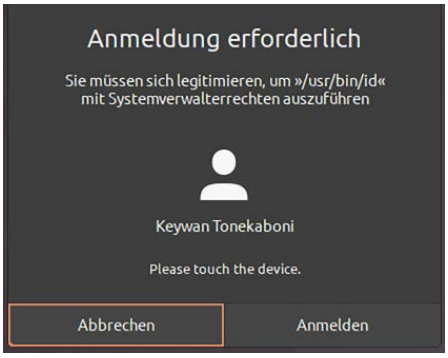
Das U2F-Modul für PAM (Pluggable Authentication Modules) sieht in der Konfigurationsdatei pro Benutzernamen eine Zeile vor. Alle Schlüssel eines Benutzers sind durch Doppelpunkte getrennt. Mit folgendem Befehl hängen Sie weitere Sicherheitsschlüssel an:

```
pamu2fcfg -n >> ~/.config/Yubico/↵
    ↳u2f_keys
```

Die Option `-n` lässt den Benutzernamen weg, wodurch nur die Schlüsselinformationen zur bestehenden Konfiguration hinzugefügt werden. Sind mehrere FIDO-Sticks angeschlossen, erwartet PAM die Authentifizierung mit dem zuerst eingetragenen Schlüssel. Das erkennen Sie, soweit vorhanden, an der blinkenden LED Ihres FIDO-Sticks. *(ktn@ct.de)*

Hinweis auf FIDO-Stick zur Linux-Authentifizierung

Ich habe einen FIDO-Stick eingerichtet, um mich mittels U2F gegenüber meinem Linux-System zu authentifizieren. Manchmal bekomme ich aber nicht mit, dass ich mich authentifizieren soll, da lediglich die LED am Sicherheits-Stick blinkt. Wie kann ich eine grafische Aufforderung einblenden lassen?



Mit der Option `cue` blendet PAM einen Hinweis ein, den Sicherheitsstick zu berühren – wenn auch sehr dezent.

Ergänzen Sie dazu in der PAM-Konfiguration jene Zeilen mit `pam_u2f.so` um die Option `cue`:

```
auth required pam_u2f.so cue
```

Fordert PAM eine Authentifizierung über das U2F-Modul an, wird der Text „Please touch the device“ angezeigt. Das klappte bei uns unter Ubuntu 20.04 sowohl im Terminal (`sudo -k id`) als auch bei grafischen Dialogen. Letztere können Sie mit `pkexec id` testen. *(ktn@ct.de)*

Manueller Fokus für die Webcam unter Linux

Der Autofokus der Webcam stellt unter Linux leider oft auf den falschen Punkt scharf. Mein Gesicht bleibt in Videokonferenzen dann leicht unscharf. Kann man das optimieren?

Die Autofokus-Funktion ist Teil der Webcam-Firmware und damit unabhängig vom Betriebssystem. Unter Linux gibt es aber Konsolentools aus dem v4l2-System, mit denen man den Fokus manuell einstellen kann.

Im ersten Schritt listen Sie dafür die Webcams mit `v4l2-ctl --list-devices` auf. In der Liste erscheinen meist zwei Devices pro Webcam: Das erste von beiden liefert das Bild, das zweite nur Metainformationen. Ein solches Paar sieht beispielsweise wie folgt aus:

```
Microsoft® LifeCam Studio(TM): ↵
            ↳(usb-0000:00:14.0-2.1):
        /dev/video3
        /dev/video4
```

Hier ist `/dev/video3` der Device-Node, der die Bilddaten liefert und bei dem Sie den Fokus einstellen möchten. Was man bei der jeweiligen Webcam einstellen kann, verrät der gleiche Befehl mit der Option `--list-ctrls`:

```
v4l2-ctl -d /dev/video3 --list-ctrls
```

Dass der Fokus dieser Webcam einstellbar ist, erkennen Sie an den folgenden zwei Zeilen in der Ausgabe:

```
focus_absolute 0x009a090a (int)  : ↵
      ↳min=0 max=40 step=1 default=0 ↵
      ↳value=4 flags=inactive
focus_auto 0x009a090c (bool)     : ↵
      ↳default=1 value=1
```

Um den Fokus einzustellen, brauchen Sie zwei Befehle. Zuerst müssen Sie den Autofokus deaktivieren und im zweiten Schritt einen manuellen Wert festlegen. In der Ausgabe des vorherigen Befehls steht der Wertebereich für den Fokus, hier 0 bis 40:

```
v4l2-ctl -d /dev/video3 ↵
        ↳--set-ctrl=focus_auto=0
v4l2-ctl -d /dev/video3 ↵
        ↳--set-ctrl=focus_absolute=12
```

Um die richtige Einstellung zu treffen, brauchen Sie unbedingt ein Vorschaubild in voller Auflösung. Falls die Videokonferenzsoftware keines liefert, bietet sich ein einfacher Webcam-Viewer wie `cheese` an. *(pmk@ct.de)*

Computerattacken mit physischem Zugriff

Immer wieder lese ich Meldungen über Sicherheitslücken, die nur bei physischem Zugriff auf das jeweilige System funktionieren. Sind die wirklich gefährlich? Wer vor Ort auf einen Computer zugreifen kann, kann doch sowieso damit machen, was er möchte.

Angriffe über das Netzwerk wie Phishing und Verschlüsselungstrojaner treffen weitaus mehr Menschen als Attacken, bei denen der Angreifer das jeweilige Gerät in die Finger bekommen muss. Letztere können jedoch bösartige Hacker, Erpresser, Geheimdienste oder Ermittlungsbehörden nutzen, wie einige Beispiele zeigen.

Häufig verweisen Sicherheitsforscher auf sogenannte „Evil Maid"-Attacken. Der Name spielt auf ein vermeintliches oder bestochenes Zimmermädchen (Maid) eines Hotels an, das das unbeaufsichtigte Notebook eines Gastes kurzzeitig entwedet und dann wieder unbemerkt zurücklegt. In der Zwischenzeit installieren Experten ein Hardwaremodul, einen bösartigen Bootloader (Rootkit) oder eine manipulierte Firmware, die Tastatureingaben aufzeichnen. Nachdem der arglose Besitzer sein Notebook wieder eine Weile benutzt hat, wird es abermals gestohlen. Mit den abgeschöpften Daten erlangen die Angreifer nun Zugriff auf das Benutzerkonto oder eine verschlüsselte Festplatte/SSD.

Derart aufwendige Angriffe sind selten, zielen aber auf besonders schützenswerte Daten wie Firmengeheimnisse, wertvolle Forschungsergebnisse, Zugangsdaten für andere Systeme (Spear Phishing) sowie auf missliebige Journalisten oder politisch Verfolgte. Nach dem gleichen Muster könnte auch eine als Servicetechnikerin oder Putzfrau getarnte Angreiferin in wenigen Minuten Spionagesoftware auf einem Desktop-PC installieren, der in einem unverschlossenen Firmenbüro steht. Reparaturbetriebe und Zulieferer sollten ebenfalls keine manipulierte Firmware aufspielen können.

Schutz gegen vor Ort ausgeführte Attacken kann zudem bei eingebetteten Computern (Embedded Systems) wichtig sein, an die ein Angreifer unbeaufsichtigt herankommt. Das gilt etwa für Steuerungsanlagen im öffentlichen Raum (Verkehrsampel, Stromversorgung) oder manche Geldautomaten.

Auch die Firmware von Servern darf sich nicht manipulieren lassen. Sonst ließe sich etwa die durch Secure Boot aufgebaute Kette kryptografischer Zertifikate umgehen. Diese wiederum sichert Funktionen wie Intel Software Guard Extensions (SGX) und AMD Secure Encrypted Virtualization (SEV). SGX richtet Enklaven im RAM ein und SEV verschlüsselt die Speicherbereiche virtueller Maschinen, um diese Daten sogar vor einem Administrator mit Root-Rechten zu verbergen. Das ist für Cloud-Server gedacht, bei denen man dem jeweiligen Anbieter nicht vollständig vertraut. Damit ist nicht unbedingt moralisches Vertrauen gemeint, sondern eine teure und aufwendige Zertifizierung von Rechenzentrum, Servern und Personal nach einschlägigen Sicherheitsvorgaben. *(ciw@ct.de)*

Fragen richten Sie bitte an

hotline@ct.de

c't Magazin

@ctmagazin

Alle bisher in unserer Hotline veröffentlichten Tipps und Tricks finden Sie unter **www.ct.de/hotline.**

Damit Spiele von Google Stadia auf einem Mac in 4K-Auflösung laufen, muss das Chrome-Plug-in Stadia+ installiert sein.

Stadia in 4K auf Mac spielen

Ich besitze einen iMac und würde gerne über die Spielestreaming-Plattform Stadia Spiele in 4K-Auflösung zocken. Trotz ausreichend dimensionierter Internetverbindung funktioniert es aber nur mit Full-HD-Auflösung. Muss ich mich damit zufrieden geben?

Seit März 2020 kann man Videospiele über die Stadia-Plattform auch im Webbrowser Chrome in 4K-Auflösung spielen. Unter Windows funktioniert das standardmäßig, wenn folgende Voraussetzungen erfüllt sind: Man benötigt ein Stadia-Pro-Abo, nutzt Chrome, hat in der Smartphone-App unter „Datennutzung und Leistung" die Option „beste visuelle Qualität" aktiviert und die Internetleitung bietet im Downstream mindestens 35 MBit/s. Diese Voraussetzungen gelten auch für einen Mac. Da Google aber 4K-Spiele mit dem von Apple ab Werk nicht unterstützten VP9-Codec komprimiert, fällt Chrome unter macOS auf einen H.264-Videostream mit 1080p-Auflösung zurück.

Abhilfe schafft das kostenlose Chrome-Plugin Stadia+. Nach der Installation erweitert es das über die Tastenkombination Umschalt+Tab aufrufbare Stadia-Menü in Chrome um den Punkt „Stadia+". Dort wählen Sie den VP9-Codec nebst 4K-Auflösung aus. Im Anschluss müssen Sie den Tab mit dem Videostream erneut laden. Dann aktivieren Sie die Option „Monitor", um im Statusfenster neben der aktuellen Auflösung auch die Latenz zu prüfen. *(des@ct.de)*

Wenig Router-Auswahl für Glasfaseranschlüsse

Für unseren künftigen Glasfaseranschluss im Haus finde ich nur Modelle von AVM. Woran liegt es, dass dieses Unternehmen da ein Monopol zu haben scheint? Gibt es noch andere Hersteller für Router, die sich direkt am AON-Anschluss (Active Optical Network) betreiben lassen? Den Umweg über ein Glasfasermodem möchte ich nicht gehen.

Der Markt für Router mit eigener AON-Schnittstelle ist tatsächlich relativ klein, uns sind derzeit keine anderen Geräte als die von AVM bekannt. Der Endkundenmarkt funktioniert primär über Medienwandler, oft als Glasfasermodem bezeichnet, die Glasfaser- auf Kupfer-Ethernet wandeln und vor handelsübliche Router mit separatem WAN-Anschluss gesetzt werden.

Eine Alternative sind Router mit SFP-Slot. Darin können Sie ein beliebiges kompatibles Modul einstecken, das mit Ihrem Glasfaseranschluss funktioniert. Ein Beispiel wäre das TL-SM321B von TP-Link, das 23 Euro kostet und die Wellenlängen von AON beherrscht. Ob das Modul wirklich funktioniert, sollten Sie jedoch mit Ihrem Netzbetreiber abklären.

Vergleichbare Geräte gibt es beispielsweise von Asus, Netgear, Mikrotik oder Ubiquiti. Allerdings sind diese für Märkte gedacht, in denen Festnetztelefonie entweder keine Rolle mehr spielt oder standardmäßig über VoIP-Telefone abgewickelt wird. Wenn Sie einen Router mit integrierter Telefonanlage suchen, wie er im deutschen Markt typisch ist, werden Sie wieder nur Geräte von AVM finden.

(amo@ct.de)

Ungewollte Netzwerkdrucker

An meinem PC bekomme ich unter Linux immer wieder fremde Netzwerkdrucker angezeigt, die ich nicht eingerichtet habe. Das passiert besonders häufig in Netzen mit Apple-Rechnern. Wenn ich die Drucker entferne, sind sie sofort wieder da. Wie werde ich die ungebetenen Gäste dauerhaft los und woher kommen sie?

Verantwortlich für das Erscheinen der Drucker ist der Netzwerkdienst Avahi. Er sucht automatisch im lokalen Netz nach Geräten und Diensten, darunter auch Drucker. Eine kleine Konfigurationsänderung in der Datei /etc/avahi/avahi-daemon.conf löst das Problem. Fügen Sie dort im Abschnitt `[Server]` die Zeile `enable-dbus=no` ein. Anschließend starten Sie den Avahi-Daemon mittels `sudo systemctl restart avahi-daemon` neu. Danach sollten Sie keine fremden Drucker mehr sehen. Leider führt die Änderung dazu, dass es merklich länger dauert, bis Druckdialoge erscheinen. Alternativ können Sie Avahi auch mittels

```
sudo systemctl disable avahi-daemon
sudo systemctl stop avahi-daemon
```

komplett abschalten. Dann erscheinen die Druckdialoge sofort und die Drucker sind weg. Die Auflösung von Multicast-DNS und das automatische Finden von Netzwerkdiensten funktionieren dann aber möglicherweise nicht mehr zuverlässig.

(mls@ct.de)

F@h-Client nach Ubuntu-Upgrade ohne OpenCL

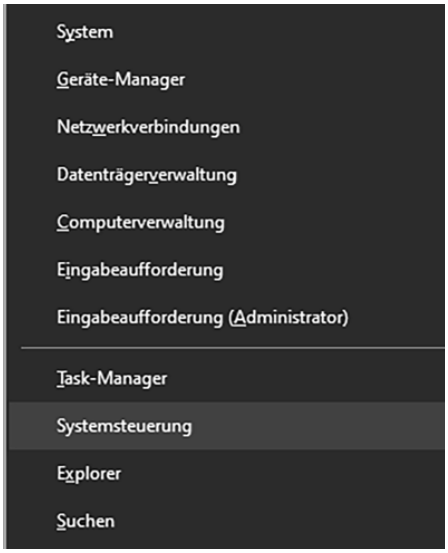
Einmal pro Woche aktualisiere ich bei meiner Ubuntu-Installation per `sudo apt update && sudo apt upgrade` alle Pakete. Nach dem letzten Durchlauf erkennt der Folding@home-Client zwar noch meine Nvidia-Grafikkarte, meckert aber, er könne keine OpenCL-Devices finden. Dabei habe ich nichts am Treiber verändert und auch keinen neuen installiert. Das übliche `sudo ubuntu-drivers devices && sudo ubuntu-drivers autoinstall` hilft auch nicht weiter.

Vermutlich hat das System im Zuge des Upgrades eine neue Kernelversion installiert, zu der der installierte Nvidia-Treiber nicht passt. Dafür reicht schon eine kleine Unstimmigkeit in der Unterversion. Ein `sudo apt upgrade` allein hilft nicht, weil bei Ubuntu unterschiedliche Unterversionen einer Treiberausgabe denselben Paketnamen tragen. So laufen etwa die Treiberversionen 440.64 und 440.100 beide unter dem Paketnamen nvidia-driver-440.

Die Lösung ist simpel: Stellen Sie mit `apt update` sicher, dass Ihre Paketliste auf dem aktuellen Stand ist. Dann führen Sie `sudo apt upgrade nvidia-driver-XXX` aus, wobei sie XXX durch die Nummer des aktuell installierten Nvidia-Treibers ersetzen, und stimmen der Installation neuer Komponenten zu. Anschließend starten Sie den Rechner neu. Wenn Sie dann noch aufräumen wollen, können Sie `sudo apt autoremove` ausführen. *(bkr@ct.de)*

Windows 10: Schneller zur Systemsteuerung

Seit einigen Versionen enthält das kleine Startmenü, welches sich unter Windows 10 beim Drücken von Windows+X öffnet, keinen Link zur Systemsteuerung mehr. Stattdessen ist jetzt einer zu den Einstellungen vorhanden. Doch den finde ich auch im normalen Startmenü und es gibt ja auch noch mit Windows+I eine Tastenkombination dafür. Nur zur Systemsteuerung führt nun kein direkter Weg mehr. Wie komme ich hin?



Mit einer kleinen Änderung lässt sich in Windows 10 die Systemsteuerung wieder direkt übers Windows+X-Menü aufrufen.

Dazu gibt es mehrere Wege. Sie können beispielsweise Windows+R drücken und `control` eintippen. Mit Windows+Pause landen Sie in der Systemsteuerung unter System und klicken dann oben in der Adressleiste wahlweise auf „Systemsteuerung“ oder „Alle Systemsteuerungselemente“. Ersteres führt zur Ansicht „Kategorie“, das andere zur Ansicht „Kleine Symbole“.

Wenn Ihnen das alles auf Dauer zu umständlich ist, ersetzen Sie den Eintrag „Einstellungen“ im Windows+X-Menü wieder durch „Systemsteuerung“. Dazu kopieren Sie aus einer alten Windows-10-Version (vor 1703) aus dem Ordner C:\Benutzer\<Kontoname>\Appdata\Local\Microsoft\Windows\WinX\Group2 die Verknüpfung „Systemsteuerung“ in den gleichnamigen Ordner Ihrer aktuellen Windows-Installation. Die Nachfrage, ob Sie die Datei ersetzen wollen, beantworten Sie mit „Ja“. Falls Sie kein altes Windows 10 haben, finden Sie die Verknüpfung auch unter ct.de/y81g zum Download. *(axv@ct.de)*

Verknüpfung Systemsteuerung:
ct.de/y81g