Paroolivaba elu: kuidas teeb pisike füüsiline FIDO2 võti sisselogimise turvalisemaks?

1 nädal tagasi - 02.11.2026 Autor: AM

Üllatus-üllatus, ka mõned uued arvutid ei sisalda sõrmejäljelugejat ega Windows Hello turvakaamerat. Alati parooli tippida on aga jube tüütu. Kuid sisseehitatud biomeetria asemel on olemas veel üks võimalus - palju turvalisem ja häkkimiskindlam.

Ajal, mil küberpätid on relvastatud võimsa tehisaruga, mis meisterdab mõne minutiga nii usutavaid õngitsuslehti, et ka kogenud arvutikasutaja trükib oma parooli ja SMS-koodi pahaaimamatult valesse kohta, tuleb meelde tuletada üks juba mõnda aega kasutusel olnud militaartasemel turvavahend - füüsiline turvavõti, mis sisaldab endas salajast võtit, mida niisama lahti ei murra. Lahenduseks on pisike mälupulka meenutav FIDO2 turvavõti võtmekimbus. See töötab nii lihtsalt puudutades kui ka sõrmejäljelugejana - saadaval on erinevaid vidinaid.

Tavalise autentimise probleemi juurpõhjus peitub selles, mida krüptograafid nimetavad „*shared secrets*“ (jagatud saladused). Olgu selleks kui tahes pikk parool, SMS-iga saabuv kood või autentimisäpi numbririda - see on info, mida teavad nii sinu seade kui ka server. Kõike, mida jagatakse, saab aga tee peal vahelt lõigata, varastada või sinult lihtsalt osava jutuga välja meelitada.

Yubico ülemaailmse autentimisaruande järgi valitseb inimeste arusaamade ja tegelikkuse vahel endiselt hirmutav kuristik. Märkimisväärne hulk töötajaid usub siiani sinisilmselt, et tavaline kasutajanimi koos parooliga või SMS-kood on kõige turvalisemad viisid sisselogimiseks.

Kuidas siis FIDO2 õngitsejad tühjade kätega jätab?

Siin tulebki mängu avatud standard FIDO2 (*Fast IDentity Online 2*), mille on välja töötanud FIDO Alliance koos suurte tehnoloogiahiidudega nagu Microsoft, Google, Apple ja Yubico.

Selle asemel, et küsida sinult järjekordset saladust, kasutab FIDO2 avaliku võtme krüptograafiat ja pääsuvõtmeid (*passkeys*).

Kui registreerid end mõnes teenuses, loob sinu seade unikaalse võtmepaari: avaliku ja privaatse võtme. Avalik võti saadetakse teenusepakkuja serverisse, kuid privaatne võti jääb luku taha sinu isiklikku seadmesse ega lahku sealt kunagi.

FIDO2 turvavõti käitub nagu vanaaegne pitsatsõrmus: server saadab sulle sisselogimisel unikaalse kontrollülesande, sinu võti vajutab sellele oma krüptograafilise pitseri ja saadab tagasi. Pitsatsõrmust ennast sa kellelegi ei anna ning võltsitud veebilehele see pitserit ei vajuta, sest võti kontrollib alati üle, kas tegu on ikka õige veebiaadressiga.

Mille vahel valida: kas nutiseade või eraldi riistvara?

FIDO2 maailmas jagunevad autentimisvahendid laias laastus kaheks.

Esimesed on platvormipõhised ehk sinu sülearvutisse või nutitelefoni sisse ehitatud lahendused, nagu Windows Hello, Apple’i Face ID ja Touch ID või Androidi sõrmejäljelugeja. Need on küll mugavad ja alati käepärast, kuid seotud konkreetse seadmega või sünkroonitud pilveteenuse kaudu, mis jätab teoreetilise ründepinna pilvepakkuja turvalisusele.

Teine ja kõige kindlam kategooria on rändavad (*roaming*) ehk välisteks seadmeteks ehitatud füüsilised FIDO2 turvavõtmed (näiteks YubiKey, Thalese või Kensingtoni mudelid). Need ühenduvad arvuti või telefoniga USB-A, USB-C, NFC või Bluetoothi kaudu.

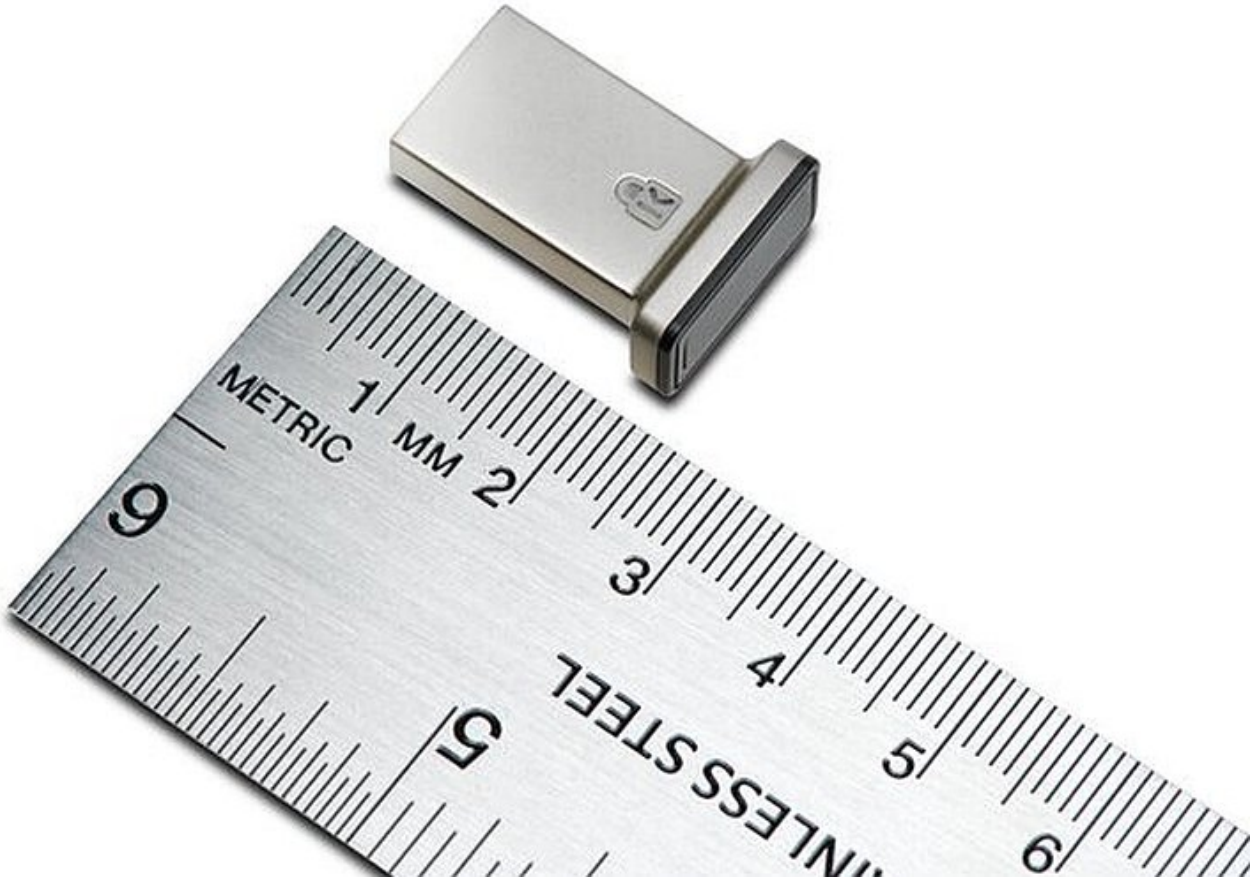
Füüsilise võtme suurim eelis on täielik eraldatus. Privaatvõtmed asuvad turvavõtme spetsiaalsel turvakiibil, mis on täielikult isoleeritud arvuti või telefoni operatsioonisüsteemist. Isegi kui sinu sülearvutis luusib ringi pahavara ja on kogu arvuti hõivanud, ei pääse see võtme sees olevale infole ligi. Lisaks on füüsiline võti asendamatu olukordades, kus inimesed jagavad ühte tööarvutit (näiteks haiglates, kõnekeskustes või kassasüsteemides) või töötavad turvatsoonides ja tootmishoonetes, kuhu isikliku nutitelefoni kaasavõtmine on keelatud.

Puudutus ja NFC *vs.* sõrmejäljelugejaga võti: kumb on mõistlikum?

Kui lähed mõnda poodi füüsilist FIDO2 võtit valima, seisad peagi teelahkmel: kas võtta soodsama hinnaga võti, mida tuleb sisselogimisel lihtsalt sõrmega puudutada (või telefoniga NFC kaudu viibata), või kallim biomeetriline võti, millel on peal päris oma sõrmejäljelugeja?

Tavaline puudutusega ja NFC-ga võti (näiteks YubiKey 5 seeria või soodsam Security Key seeria) kontrollib puudutusega vaid seda, et sa oled füüsiliselt arvuti taga, mitte aga ei ürita keegi kaugelt sinu seadmesse sisse tungida. Et keegi võõras sinu kaotatud võtmega kontodele sisse ei saaks, kaitstakse võtit FIDO2 puhul PIN-koodiga, mida tuleb sisestada sisselogimisel. Selle lahenduse suureks plussiks on töökindlus, soodsam hind ja NFC tugi – saad sama võtit mugavalt vastu telefoni tagakülge toksata ja ka mobiiliäppidesse niimoodi turvaliselt sisse logida.

Sõrmejäljetuvastusega võti (nagu YubiKey Bio seeria või Kensington VeriMark IT) asendab PIN-koodi trükkimise biomeetriaga. Näiteks Kensingtoni võti kasutab *Match-in-Sensor* tehnoloogiat, mis loeb sõrmejälge 360 kraadi ulatuses otse pisikesel sensoril ega lase krüpteerimata biomeetrilistel andmetel kunagi võtmest väljuda. See on kiire ja mugav: paned näpu peale ja oledki sees, ilma et peaksid ühtegi koodi meeles pidama või klaviatuuril toksima.



Samas on sõrmejäljevõtmetel omad konksud, millest müügibrošüürid vaikivad. Paljudel biomeetrilistel USB-võtmetel puudub NFC-võimekus, sest sõrmejäljesensor vajab tööks rohkem voolu, kui telefoni NFC-väli suudab alati stabiilselt pakkuda. Seega on neid tülikam kasutada nutitelefoniga. Lisaks võib esineda ootamatuid ühilduvusprobleeme: näiteks mainitud Kensington VeriMark IT ei toeta Windowsi ARM-protsessoritega arvuteid ning nõuab uuemates Windows 11 versioonides Microsofti täiustatud sisselogimisturbe (ESS – *Enhanced Sign-In Security*) väljalülitamist, et üldse toimida. Samuti tuleb arvestada, et kui sõrm on märg või vigastatud, küsib võti tagavaraks ikkagi PIN-koodi, kuid turvalisus on endiselt tagatud ka siis.

Varundamise tähtsus: kahe võtme reegel

FIDO2 turvavõtmega kaasneb üks karm reaalsus: kuna paroolid ja jagatud saladused kaovad, muutub iganenuks ka harjumuspärane nupp „Unustasin parooli“. Kui sul on ainult üks füüsiline võti ja sa selle ära kaotad, oled oma kontodest ilma.

Seetõttu kehtib turvavõtmete maailmas raudne reegel: registreeri alati vähemalt kaks sõltumatut autentimisvahendit. Kõige kindlam strateegia on osta korraga kaks võtit – üks ripub igapäevaselt võtmekimbus (või istub YubiKey Nano või Kensington VeriMark IT kujul püsivalt masina USB-pesas) ning teine ootab

turvaliselt kodus sahtlipõhjas või seifis. Muu, pisut soodsam variant on kasutada igapäevaselt füüsilist võtit, kuid registreerida samale kontole tagavaraks ka oma arvuti Windows Hello või Maci Touch ID.

Oluline on muidugi teada sedagi, et FIDO2 ei ole hõbekuul kõigi maailma hädade vastu. See hoiab küll ära paroolide õngitsemise ja vaheltlõikamise sisselogimise hetkel, kuid ei kaitse sind siis, kui ründaja kaaperdab sinu sessiooni pärast seda, kui oled ukse juba lukust lahti keeranud.

FIDO2 puudutusega ja NFC-ga turvavõti

PLUSSID

- Täielik kaitse parooliõngitsuse ja vahendajarünnete (MiTM - *Man-in-the-Middle*) vastu
- NFC tugi võimaldab mugavat kasutamist nii sülearvutis kui ka nutitelefonis
- Väga vastupidav korpus ja soodsam hind
- Toetab sageli ka vanemaid protokolle (PIV, Smart Card, OTP) hübriidsüsteemide jaoks

MIINUSED

- Paroolivabal sisselogimisel tuleb lisaks puudutusele sisestada klaviatuurilt sessiooni alustuseks ka PIN-kood
- Võtme kaotamisel ja varuvõtme puudumisel on kontode taastamine keeruline

FIDO2 sõrmejäljelugejaga (biomeetriline) turvavõti

PLUSSID

- Mugav ja kiire sisselogimine: puudutus ja isikutuvastus toimuvad ühe liigutusega ilma PIN-koodi trükkimata
- Sõrmejäljeandmed on isoleeritud võtme turvakiibil ega jõua kunagi arvutisse
- Välistab olukorra, kus keegi piilub üle õla sinu turvavõtme PIN-koodi

MIINUSED

- Tunduvalt kallim hind (sageli 60 euro ringis ja enamgi)
- Tavaliselt puudub NFC tugi, mis piirab kasutamist nutitelefonidega
- Võimalikud ühilduvuspiirangud (nt osal mudelitel puudub tugi Windows ARM-seadmetele või Windows 11 ESS-turbele)
- Määrdunud või märja sõrme korral tuleb ikkagi kasutada varu-PIN-koodi

Tehnilised andmed ja võrdlus

	Puudutusega ja NFC-ga FIDO2 võti	Sõrmejäljelugejaga FIDO2 võti
Standardid:	FIDO2 / WebAuthn (CTAP2), FIDO U2F (CTAP1)	FIDO2 / WebAuthn (CTAP2), FIDO U2F (CTAP1)
Lisaprotokollid (olenevalt mudelist):	PIV / Smart Card, OATH OTP, OpenPGP	Tavaliselt ainult FIDO2 või FIDO2 + PIV (Multi-protocol)
Kasutaja tuvastamine:	Füüsiline puudutus + PIN-kood	360° sõrmejäljesensor (varuvariandina PIN-kood)
Ühenduvus:	USB-A või USB-C, NFC (mõnel ka Bluetooth)	USB-A või USB-C (NFC tugi enamasti puudub)
Biomeetria täpsus (nt VeriMark IT):	Puudub	Valekeeldumise määr (FRR) 2%, valelubamise määr (FAR) 0,001%
Turvastandardid:	Kuni NIST AAL3, FIPS 140-2 / 140-3	Kuni NIST AAL3, FIPS 140-2 / 140-3 (tootjal lisaks ISO/IEC 27001, GDPR/BIPA vastavus)
Eripärad ja piirangud:	Töötab tõrgeteta peaaegu kõigis kaasaegsetes seadmetes	Võib vajada Windows 11 ESS-i keelamist; ARM-tugi võib puududa
Orienteeruv hinnaklass:	35–55 eurot	60–95 eurot

- Lahendused

- Tarkvara
- Turvalisus

Pilt

Tab
Caps
Shift
Ctrl