A TUDOMÁNY, AZ OKTATÁS ÉS A KÖZGYŰJTEMÉNYI KISZOLGÁLÁS ÚJ INFORMATIKAI SZINERGIÁI

NETWORKSHOP 2026
35. Országos Informatikai Konferencia

2026. március 31–április 2.
Debreceni Egyetem, Debrecen

Szerkesztette: Tick József, Kokas Károly, Holl András

HUNGARNET Egyesület
Budapest, 2026

HUN-REN
Magyar Kutatási Hálózat

NETWORKSHOP

Szerkesztette: Tick József, Kokas Károly, Holl András

Tipográfia és tördelés: Vas Viktória
Korrektúra: Danyi Melinda
Angol nyelvi lektor: Lukács Katalin

Networkshop 2026 konferencia előadásainak közleményei
Debreceni Egyetem, Debrecen
2026. március 31–április 2.

ISBN 978-615-6792-29-7
DOI: https://doi.org/10.31915/NWS.2026

Kiadja a HUNGARNET Egyesület
az MTA Könyvtár és Információs Központ közreműködésével
Budapest
2026

Borítókép: freepik.com

DOI: 10.31915/NWS.2026.20

“EGY JELSZÓ MIND FÖLÖTT”, AVAGY KI VAGYOK ÉN? VAN-E, VÉD-E IGAZÁN A NEM JELSZAVAS AUTENTIKÁCIÓ?

ONE PASSWORD TO RULE THEM ALL: OR, WHO AM I?

DOES PASSWORDLESS AUTHENTICATION REALLY EXIST, AND DOES IT TRULY PROTECT?

Pfeiffer Szilárd
mailbox@pfeifferszilard.hu

Balsai Péter
balsai.peter@mithrandir.hu

Absztrakt

A vezető techcégek kommunikációjában ma megszokott kijelentés, hogy a jelszó elavult módszer. Egyetértenek abban, hogy birtokalapú és/vagy biometrikus megoldásokkal kell alkalmazni. A „jelszómentesség” sokszor csak illúzió, a termékeladást segítő marketing-üzenet. Felvetjük, hogy a jelszavak teljes mellőzése hamis dogma, hiszen a biokulcsok és hardvertokenek gyakran megjegyezhető kódokra (PIN, recovery code) támaszkodnak. A CIA-háromszög, a Parkeri hatszög és a Kerckhoffs-elvek használatával mutatjuk be a részletek ismertetése nélkül, hogy a biometria és a birtokalapú megoldások számos biztonsági elvet sértenek/sérthetnek. Azt is bemutatjuk, hogy a jelszó nyújtotta entrópia modern aszimmetrikus protokollokkal (pl.: OPAQUE) ötvözve magasabb szintű kriptográfiai biztonságot nyújtanak az alapvető elvek betartása mellett. Érintjük a szabad, nyílt forráskódú szoftverek szerepét a technológiai szuverenitás és az auditálhatóság megőrzésében.

A valódi kérdés tehát nem az, hogy alkalmazzuk-e a jelszavakat, hanem az, hogy mennyire közvetlen módon alkalmazzuk őket. Kitérünk arra a tapasztalatunkra, hogy az azonosítás és jogosultságvizsgálat a való világból kerül át a digitális térbe, és egyre inkább a digitális térbeli azonosítás határozza meg kilétünket. Így a nemzetállamok jogi és magánszemély-azonosítási monopóliuma a nagy techcégek és partnereik kezébe csúszik át.

Kulcsszavak: autentikáció, jelszó, jelszómentesség, biometria, technológiai szuverenitás, opaque protokoll, digitális identitás, CIA-háromszög, Parkeri hatszög, Kerckhoffs-elv

Abstract

In the messaging of leading tech companies, it is now a commonplace claim that the password is an obsolete method. They agree that it should be used with possession-based and/or biometric solutions. „Passwordlessness" is often only an illusion – a marketing message that helps sell products. We argue that abandoning passwords entirely is a false dogma, since biometric keys and hardware tokens frequently rely on memorable codes (PIN, recovery code). Using the CIA triad, the Parkerian hexad, and Kerckhoffs's principles, we show – without detailing the specifics – that biometric and possession-based solutions violate, or may violate, a number of security principles. We also present that the entropy provided by a password, combined with modern asymmetric protocols (e.g., OPAQUE), delivers a higher level of cryptographic security while respecting the fundamental principles. We touch on the role of free and open-source software in preserving technological sovereignty and auditability.

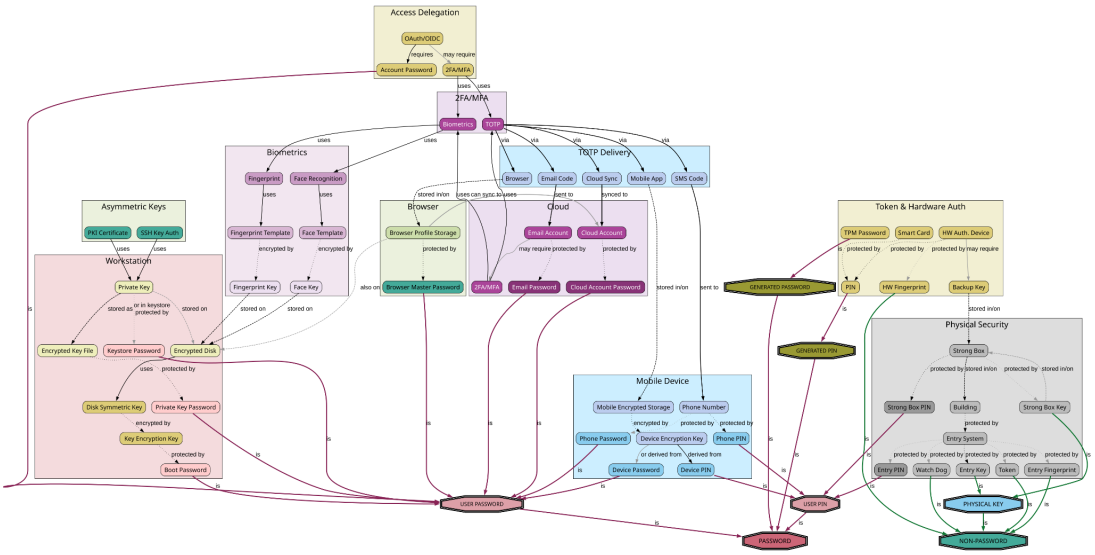
The real question, therefore, is not whether we use passwords, but how directly we use them.

We also reflect on our experience that identification and authorization are moving from the physical world into the digital space, and that digital-space identification increasingly determines who we are. As a result, the nation-states' monopoly on legal and individual identification is slipping into the hands of the large tech companies and their partners.

Keywords: authentication, password, passwordless, biometrics, technological sovereignty, opaque protocol, digital identity, CIA triad, Parkerian hexad, Kerckhoffs's principle

1. Bevezetés

Az 1. ábra megmutatja, hogy milyen gyakran jutunk – egy vagy több lépésben – jelszavakhoz a különböző azonosítási technológiák során.



1. ábra: Autentikációs eljárások visszavezethetősége jelszavakra

1.1. A jelszó széleskörű használata

A birtokalapú biztonsági tokenek és eszközök gyakran PIN-kóddal (azaz jelszóval) védettek. A mobilos biometria hasznos, ám nem ritkán csak kényelmi funkció. Meghibásodás esetén viszont a PIN-kód vagy a valamilyen minta (bit-sor) lesz a tartalékmechanizmus. Egy központi azonosítószolgáltató (identity provider) megoldás is legtöbbször jelszóra, illetve valamilyen visszaállító eljárásra támaszkodik. Léteznek ugyan jelszó nélkül használható, biometriával védett hardveres eszközök (pl.: YubiKey Bio [1]), ám kompromittálódás vagy eszközvesztés esetén a visszaállító kódok (recovery keys) tárolása újfent jelszavakhoz vezet (pl.: széf kód).

A jelszómentes hitelesítés (passwordless authentication) terjedésével ráadásul új kritikus biztonsági kérdés merül fel: a külső hardver, szoftver, internetkapcsolat (azonosítószolgáltató) és/vagy dedikált online szolgáltatók iránti fundamentális igény. Ezeket az infrastrukturális elemeket gyakran az Európai Unió és annak joghatóságán kívül fejlesztik (pl.: Microsoft), gyártják (pl.: RSA Security), illetve üzemeltetik (pl.: Amazon, Google). Ez az ellátási lánc a kritikus infrastruktúráinkat (pl.: közigazgatási rendszerek) olyan adatvédelmi és szuverenitási problémákkal terheli meg, amelyek a jelszó (tudás) esetében nem lennének jelen.

2. A személyazonosítás nagyvonalú története

Az azonosítás nem új keletű, csak az informatika túl fiatal.

Kőkorban és az őskorban az arc- és hangfelismerés, a ruházat, az ékszerek, a csoporthoz tartozást jelző testfestés és a (heg)tetoválások segítették a felismerést.

Ókor és középkor ehhez hozzátette a gyűrűket, címereket, okleveleket [2], pecséteket és egyházi nyilvántartásokat, az előkelőknek a festményeket.

Újkorban kötelező lett az egyházi/állami anyakönyv (hazánkban: 1895) és elterjedtek a hivatalos azonosító okmányok, amik tartalmaztak alapvető adatokat (név, születési idő, "apja neve").

A XIX.–XX. században már a fénykép (igazolványkép), ujjlenyomat, vércsoport, de akár még a koponyaalak is szolgált azonosítási célokra. **A közelmúltban** kamera, íriszszkenner, vénaszkenner, ujjlenyomat-olvasó, hanganalizátor, DNS-profilozó stb. is használatosak, melyek közös jellemzője, hogy a fizikai valóságot valamilyen digitális kivonattá kódolva és egyúttal veszteségesen tömörítve, tárolják és vizsgálják.

Fentiek mellett mindig volt jelentőségük a hangoknak, jelszavaknak és jelmondatoknak is, melyek a "valakiságot", illetve egy adott csoporthoz való tartozást igazolták.

3. Az azonosítás mint állami monopólium megszűnésének jelei

Az Apple – és más cégek – a DUNS-számot (Data Universal Numbering System, amit egy vállalkozás [3] kezel) használják [4, 5, 6], ami nagy, többségében amerikai cégek által elfogadott módja a cégek azonosításának. Számukra ez a szám digitális tanúsítványként igazolja a vállalkozás jogi létezését[7]. A nemzetállamok most is adószámot, cégjegyzékszámot stb. használnak. A Google a diákok jogviszonyának igazolására SheerID-t kér [8, 9], amit szintén egy vállalkozás [10] kezel. Mind a DUNS, mind a SheerID csak információforrásként használják az állami adatokat, saját döntéseik alapján. Ez a trend számunkra arra utal, hogy az azonosítás monopóliuma csúszik ki az állami szervezetek kezéből. Az állami monopólium eltűnésének további lendületet ad az eIDAS-2 [11] mobilalapú digitális tárcája, melynek folyományaként az európai és más (nem az USA vagy Kína) államok mind a hardver, mind a szoftver feletti uralmat elvesztik. Az első lépcsőben [12] használt chipkártyás azonosítás, még sok állam, vagy szövetség számára nyújtott valamekkora önállóságot, tekintve, hogy a szükséges biztonsági chipet európai gyártók is képesek gyártani. Ráadásul a nyomtatott, különböző biztonsági elemekkel ellátott azonosítókártyák, a külső eszköz (hardver, szoftver) nélküli ellenőrzésre is lehetőséget adnak. A tisztán elektronikus "mobiltárca" mindkét lehetőséget megszünteti, hiszen nincs valódi európai gyártó, alkalmazásbolt, és ha megsérült, vagy lemerült az eszköz, pl. telefon akkor azonosításra nem használható.

4. Jelszavak

Míg a hagyományos meghatározások a jelszóra elsősorban az emberek közötti használatot (azonosításra) írják le, míg a szerzők a modern számítógépes világban betöltött szerepet hangsúlyozva az alábbi definíciókat adják.

> *Egy bitsorozat a számítógép számára, melyet az ember – a könnyebb megjegyezhetőség érdekében – nyomtatható karakterekkel és az informatikai rendszerek gyengeségei miatt az angol ábécé betűivel, illetve egyéb nyomtatható karakterekkel – például írásjelekkel – ír be.* – Balsai Péter

> *A jelszó nem más, mint egy – kizárólag az emberi megjegyezhetőség érdekében –, szövegesen ábrázolt véletlen érték, amely az autentikációs algoritmusok számára a szükséges entrópiát szolgáltatja.* – Pfeiffer Szilárd

4.1. A jelszó mint entrópiaforrás

Mivel a számítógépek csak álvéletleneket generálnak, a hitelesítés valódi értéke a jelszó magas bemeneti entrópiájában, statisztikai egyediségében rejlik. A jelszó olyan „biológiai entrópia", amit a felhasználó visz be a rendszerbe egy feltörhetetlen kriptográfiai kulcs származtatásához.

Amikor jelszómentes hitelesítésre váltunk, elveszítjük az afeletti kontrollt, melynek szerepe kritikus. A jelszó valódi értéke ugyanis a statisztikai egyediségében rejlik, nem csupán a bitek mennyiségében[1]. A felhasználók többsége prediktálható mintázatokat követ, ami drasztikusan csökkenti a tényleges entrópiát. Ezért fontos említeni (terjedelmi korlátok miatt nem kifejtve) a tipikus jelszóhibákat[13]: évszámok, családtagok, háziállatok nevei, gyakori szavak, kényszeralgoritmusok stb. A jó jelszó jellemzői: egyedi (nem hasonlít másokéra), semleges (a személyhez könnyen nem köthető), több szó / mondat, aminek nem kell komplexnek (pl.: speciális karakter), csak hosszúnak lennie, megjegyezhető. Egy komplett iparági marketing magyarázza mindenkinek, hogy a megfelelő jelszavakat nem lehet megjegyezni, ám ez így ebben a formában nem igaz.

1 A bitmélység (bit depth) a jelszó elméleti keresési terének mérete: egy n hosszú, k elemű ábécéből álló jelszó bitmélysége log2 (kn) bit. Ez az elméleti felső korlát, amely csak akkor valósul meg, ha a jelszó valóban egyenletes eloszlásból származik.

4.2. Lehet jó jelszót használni, megjegyezni

Pszichológia- és a memóriakutatások azt mondják [14], hogy

- A rövid távú memóriában teljesen véletlenszerű karakterekből átlagosan 7 ± 2 elemet lehet megjegyezni[14], és ennek a hosszú távú memóriába kerüléséhez már sok ismétlés kell.[2]
- Gyakori (a személy által használt) szavakat mondattá összefűzve, a rövid távú memória „tömbösítve" szavankénti egységként kezeli azokat, és a hosszú távú memóriába kerüléshez pár olvasás kell [15]. Napi legalább egyszeri használat mellett néhány százalék a felejtés esélye.

Vélelmezzük, hogy a hiedelemmel ellentétben **hosszú és jó jelszavak is lehetnek megjegyezhetők az ember számára.** Egy véletlenszerű, személyes kontextushoz nem kötődő jelmondat a gép számára szükséges magas entrópiát biztosítja. Bár lenne megoldás (OPAQUE [16] – lásd később), ami az offline szótáralapú támadást a gyakorlatban kiküszöbölné, de a kiinduló jelszó minősége még így is döntő jelentőségű. Fenntartással kell kezelni az informatikai marketinget, a társtudományokban van/lehet megoldás, ám **a cégek nem tanítani, hanem eladni akarnak.**

5. Biztonsági elveknek való megfelelés

A CIA triad, Parkeri hexád [17], Kerckhoffs-elv [18], Zero Trust direktíva [19] nem újdonságok, sok éve léteznek. Figyelembevételük, betartásuk – a szerzők folyamatban lévő kutatásának [20] tapasztalatai alapján – nem igazán jellemző. Nem tapasztaljuk, hogy rendszerek vizsgálatára együtt használják ezeket. Ezért gondolatébresztőként megosztjuk a következő táblázatainkat.

5.1. A CIA-triád és Parkeri hexád

	Jelszó	**Birtoklás**	**Biometria**	**OPAQUE**
Bizalmasság	sérti	*sértheti*	sérti	**nem**
Integritás	nem	sérti	sérti	**nem**
Rendelkezésre állás	*sértheti*	sérti	sérti	*sértheti*
Hitelesség	sértheti	sértheti	nem	nem
Birtoklás és kontroll	sérti	sérti	sérti	**nem**
Hasznosság	nem	nem	nem	nem

2 Egy ma egyre kívánatosabb 20 karakteres jelszó pl f5!Tz9#kL2qP0rWv&n1X) ~85–95% eséllyel megtanulhatatlan, és a megtanulni képes 5–15 % is gyorsan és szinte biztosan gyorsan elfelejti.

5.2. Kerckhoffs-elv / módszerek

	Jelszó	**Birtoklás**	**Biometria**	**OPAQUE**
Feltörhetetlenség	*sértheti*	*sértheti*	*sértheti*	**nem**
Nyilvános specifikáció	**nem**	sérti	sérti	**nem**
Megjegyezhetőség / csere	**nem**	sérti	sérti	**nem**
Távíró (hálózat)	**nem**	**nem**	**nem**	**nem**
Hordozhatóság	**nem**	*sértheti*	sérti	**nem**
Egyszerűség	sérti	sérti	sérti	**nem**

5.3. Zero trust direktíva

	Jelszó	**Birtoklás**	**Biometria**	**OPAQUE**
Adatátvitel közben	*sértheti*	*sértheti*	*sértheti*	**nem**
Feldolgozás közben	**nem**	sérti	sérti	**nem**
Tárolás közben	**nem**	sérti	sérti	*sértheti*

6. Az OPAQUE protokoll: Egy jelszó, ezer egyedi kulcs

Részleges választ és javuló megfelelést adna a biztonsági alapelvek előbb mutatott megsértésére az aPAKE (asymmetric Password-Authenticated Key Exchange) protokollok alkalmazása. Ilyen protokoll például az OPAQUE (VOPRF[21] implementációval), ami az alábbi előnyeire való tekintettel sem terjedt el még a gyakorlatban.

1. Zero-Knowledge Proof: A jelszó soha nem utazik a hálózaton. A klienstől a szerverig csak egy vakított (blinded) bizonyíték utazik, a szerver egyedül a hozzáférés érvényességét hagyja jóvá.
2. Cross-site tracking prevenció: A kulcsszármaztatási folyamatba (Key Derivation Function – KDF) az OPAQUE képes bevonni a szerver azonosítóját (Context) is. Ennek eredményeképp ugyanabból a jelszóból a KDF funkciószerverenként eltérő aszimmetrikus kulcspárt fog generálni.
3. Rugalmas paraméterek: a biztonsági szint skálázható, a kulcspár generálásához szükséges számítási-, illetve memóriakapacitás-igény növelésével, miközben a jelszó változatlan.
4. A hardveres tokenekkel ellentétben nem kell új eszközt vásárolni a paraméterek frissítéséhez.

7. Technológiai szuverenitás és a nyílt vagy saját forráskód együtt jár

A Cloud-szinkronizált Passkeyek használata — a fentiekkel szemben — azzal jár, hogy az óriáscégek digitális gyámjaink lesznek. A felhőbe például a következő kritikus adatok kerülhetnek: privát kulcs (end-to-end titkosítva, a mesterjelszó védi), metaadatok (melyik szolgáltatáshoz tartozik, létrehozás időpontja), valamint a credential azonosító. A jelszó-visszaállítási mechanizmusok (pl.: elfelejtett Apple ID jelszó esetén) a „Zero Knowledge" szempontjából vetnek fel kérdéseket. A zárt forráskód, illetve az ellenőrizhető audit hiánya miatt a ténylegesen használt titkosítási, hash és egyéb mechanizmusok nem ellenőrizhetők. A kulcsok fizikai helye pedig joghatósági kérdéseket vet fel: az államok kikényszeríthetik az adatok átadását, lehetnek politikai okok miatt beépített „kém megoldások" is. Az akuttá váló – nem javított – sérülékenységek is a gyártóval szembeni súlyos függőséget hoznak létre

Ezek alapján belátható, hogy a szabad és saját fejlesztésű szoftvereknek kiemelkedő jelentősége lehetne.

8. Konklúzió

A digitális és a valós tér egybeolvadásával a szuverén, megbízható állami azonosítás ma már kritikus, az alapvető infrastruktúra-szolgáltatás része kell(ene) legyen. Az azonosítás a fizikai és digitális tér építőeleme, ennek megfelelő szemléletet és erőforrásokat igényel problémáinak kezelése.

Nem az a kérdés, hogy alkalmazzuk-e a jelszavakat, hanem az, hogy mennyire közvetlen módon történik az alkalmazásuk — és kitől függünk mindeközben. Valóban jobbak-e, jelszómentesek-e a „jelszómentes" megoldások, vagy csupán más, nehezebben kontrollálható kockázatokat vállalunk be egy illúzióért? **A biometria és a hardver tokenek sem mentesek a biztonsági elvekkel kapcsolatos kompromisszumoktól és geopolitikai függőséget is teremthetnek.**

A jelszó legfőbb hátránya a feloldható a modern azonosítási keretrendszerek (OPAQUE) alkalmazásával. Az egyik legbiztonságosabb kulcsgeneráló erő továbbra is a saját emberi tudatunkból fakadó entrópia marad — és ez az egyetlen autentikációs faktor, amelyhez sem külföldi hardver, sem szoftver, sem szolgáltató nem szükséges, **a jelszó a tudatunkból (**most még**) nem olvasható ki.**

[1] “YubiKey Bio Series,” Yubico. Accessed: Jun. 28, 2026. [Online]. Available: https://www.yubico.com/products/yubikey-bio-series/

[2] L. Benedictus, “A brief history of the passport,” *The Guardian*, Nov. 17, 2006. Accessed: Jun. 28, 2026. [Online]. Available: https://www.theguardian.com/travel/2006/nov/17/travelnews

[3] “A D-U-N-S számról.” Accessed: Jun. 28, 2026. [Online]. Available: https://www.dnb.com/hu-hu/smb/duns.html

[4] “DUNS-szám,” Google Ads Súgó. Accessed: Jun. 29, 2026. [Online]. Available: https://support.google.com/google-ads/answer/85961?hl=hu

[5] “KB0756540 - Why is a DUNS number required for me to register?,” SAP Ariba Help Center. Accessed: Jun. 29, 2026. [Online]. Available: https://hc.ariba.com/index.html?sap-ui-language=en#/item/KB0756540

[6] “Company account verification requirements – Windows apps,” Microsoft Learn. Accessed: Jun. 29, 2026. [Online]. Available: https://learn.microsoft.com/en-us/windows/apps/publish/store-business-verification-reqs

[7] G. Teubner, “Global Bukowina: Legal pluralism in the world society,” in *Critical theory and legal autopoiesis*, D. Göbel, Ed., Manchester University Press, 2019. doi: 10.7765/9781526139948.00017.

[8] “Google AI Pro student trial,” Google One Help. Accessed: Jun. 29, 2026. [Online]. Available: https://support.google.com/googleone/community-guide/379602230/google-ai-pro-student-trial?hl=en

[9] “Amazon Music FAQ.” Accessed: Jun. 29, 2026. [Online]. Available: https://verify.sheerid.com/amazon-music-faq/

[10] “Identity Marketing Platform,” SheerID. Accessed: Jun. 28, 2026. [Online]. Available: https://www.sheerid.com/

[11] “AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2024. április 11-i (EU) 2024/1183 RENDELETE a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról - Hatályos Jogszabályok Gyűjteménye,” Hatályos Jogszabályok Gyűjteménye. Accessed: Jun. 29, 2026. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a2401183.eup

[12] “AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2014. július 23-i 910/2014/EU RENDELETE a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről - Hatályos Jogszabályok Gyűjteménye,” Hatályos Jogszabályok Gyűjteménye. Accessed: Jun. 28, 2026. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1400910.eup

[13] “Miért ne becsüljük le a kisbetűs jelszavakat? 3. rész,” Bitport. Accessed: Jun. 28, 2026. [Online]. Available: https://bitport.hu/miert-ne-becsuljuk-le-a-kisbetus-jelszavakat-password-security-3-resz/

[14] G. A. Miller, "Classics in the History of Psychology An internet resource developed by Christopher D. Green York University, Toronto, Ontario (Return to Classics index)." Accessed: Jun. 29, 2026. [Online]. Available: https://psychclassics.yorku.ca/Miller/

[15] C. E. Bonhage, L. Meyer, T. Gruber, A. D. Friederici, and J. L. Mueller, "Oscillatory EEG dynamics underlying automatic chunking during sentence processing," *NeuroImage*, vol. 152, pp. 647–657, 2017, doi: https://doi.org/10.1016/j.neuroimage.2017.03.018.

[16] D. Bourdrez, H. Krawczyk, K. Lewi, and C. A. Wood, "The OPAQUE Augmented Password-Authenticated Key Exchange (aPAKE) Protocol," Internet Engineering Task Force, Request for Comments RFC 9807, 2025. doi: 10.17487/RFC9807.

[17] D. B. Parker, *Fighting computer crime: a new framework for protecting information*. New York: Wiley, 1998.

[18] A. Kerckhoffs, "La Cryptographie Militaire (Seconde partie)".

[19] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[20] S. Pfeiffer, "Assessing IT Solutions Against Security Principles," Szilárd Pfeiffer. Accessed: Jun. 30, 2026. [Online]. Available: https://pfeifferszilard.hu/2026/06/30/assessing-it-solutions-against-security-principles.html

[21] A. Davidson, A. Faz-Hernandez, N. Sullivan, and C. A. Wood, "Oblivious Pseudorandom Functions (OPRFs) Using Prime-Order Groups," Internet Engineering Task Force, Request for Comments RFC 9497, 2023. doi: 10.17487/RFC9497.