How (not) to store passwords

Habilitation colloquium

Andreas Unterweger

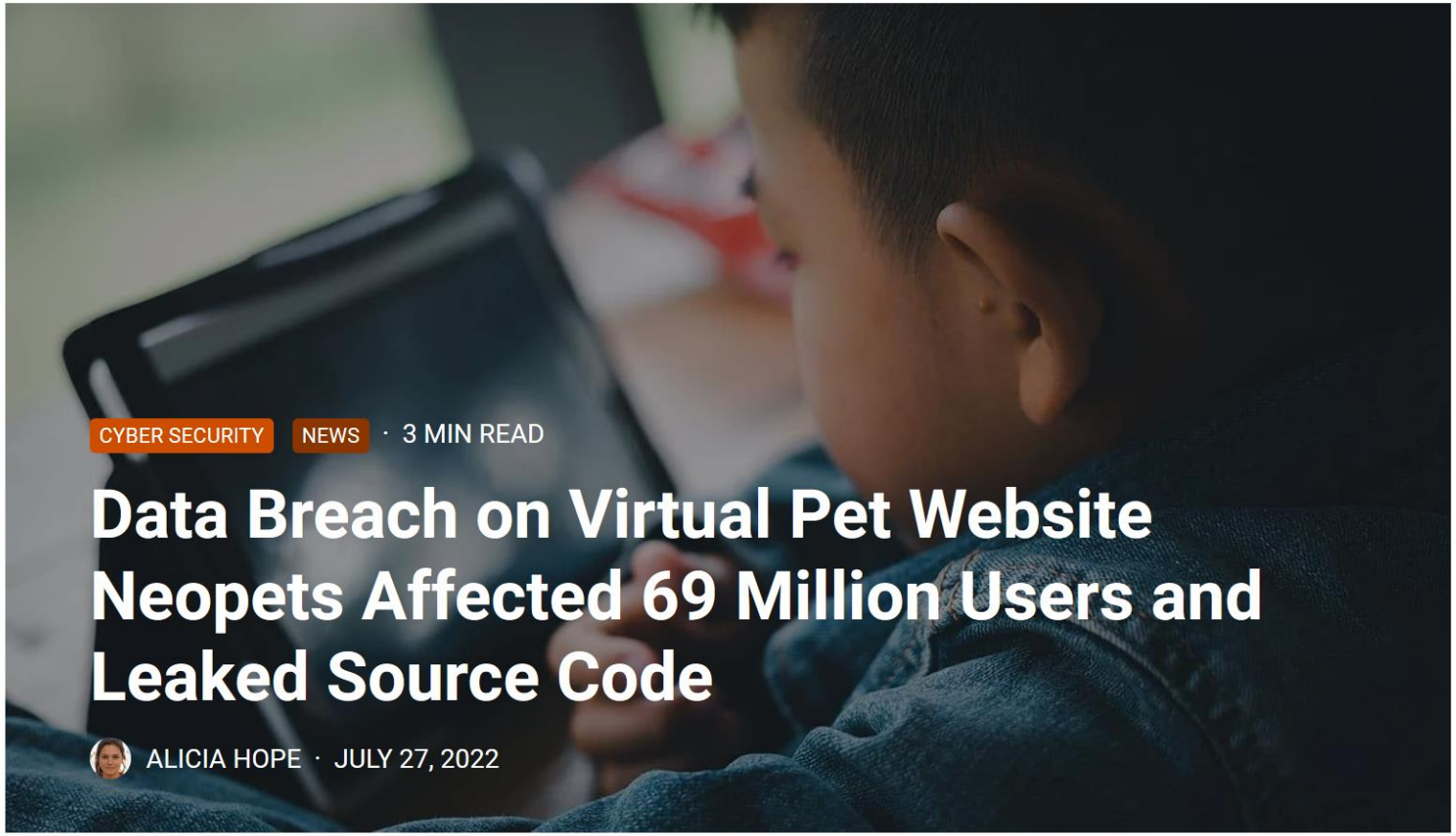
University of Salzburg

Contents

- Recent password-related incidents
- The purpose of (storing) passwords
- Obvious ways not to store passwords
- Improving password storage in three simple steps
- The importance of user passwords
- How to store passwords in 2023

Recent password-related incidents

2022: Neopets

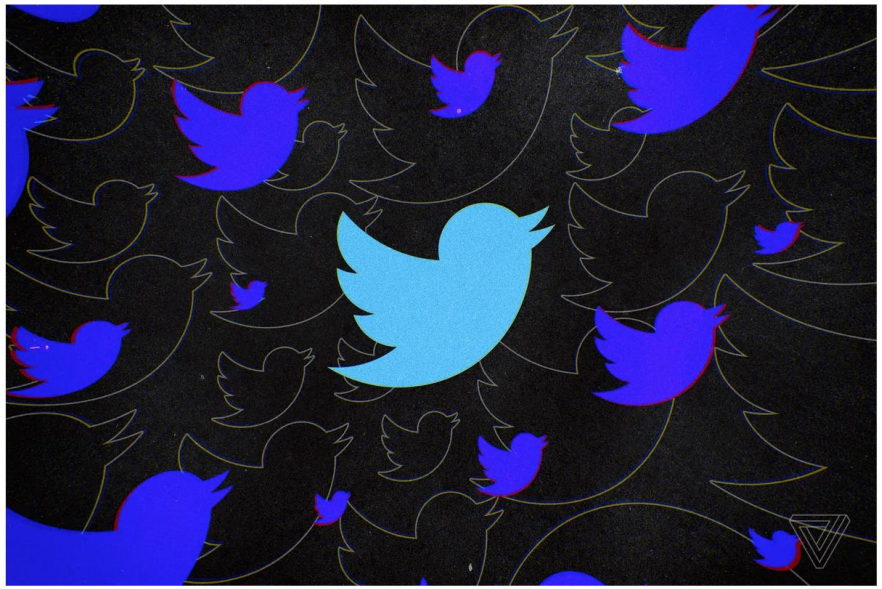


Source: https://www.cpomagazine.com/cyber-security/data-breach-on-virtual-pet-website-neopets-affected-69-million-users-and-leaked-source-code/ (18.2.2023)

2018: Twitter

TECH / TWITTER / MOBILE

Twitter advising all 330 million users to change passwords after bug exposed them in plain text

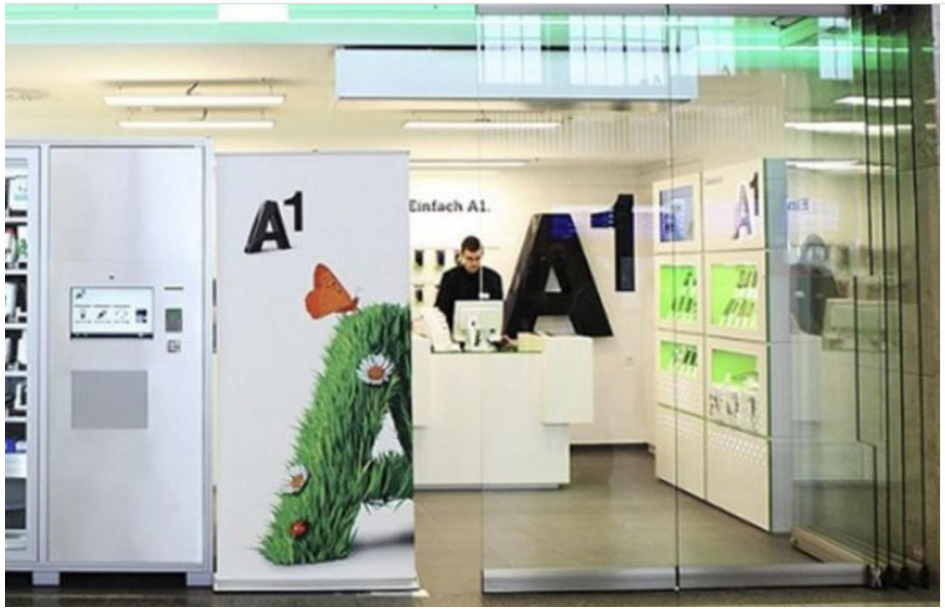


/ There's apparently no evidence of any breach or misuse, but you should change your password anyway

By CHAIM GARTENBERG / @cgartenberg
May 3, 2018, 10:21 PM GMT+2 | 0 Comments

Source: https://www.theverge.com/2018/5/3/17316684/twitter-password-bug-security-flaw-exposed-change-now (18.2.2023)

2018: A1 Telekom Austria



SECURITY

A1 Telekom Austria hacked – user data stored in plain text

5 October 2018 by Nicole Lorenz

4 years ago

Source: https://www.avira.com/en/blog/a1-telekom-austria-hacked-user-data-stored-in-plain-text (18.2.2023)

2018: T-Mobile Austria

MOTHERBOARD
TECH BY VICE

T-Mobile Stores Part of Customers' Passwords In Plaintext, Says It Has 'Amazingly Good' Security

A T-Mobile Austria customer representative made a shocking admission in a Twitter thread.

Source: https://www.vice.com/en/article/7xdeby/t-mobile-stores-part-of-customers-passwords-in-plaintext-says-it-has-amazingly-good-security (18.2.2023)

The purpose of (storing) passwords

Why passwords?

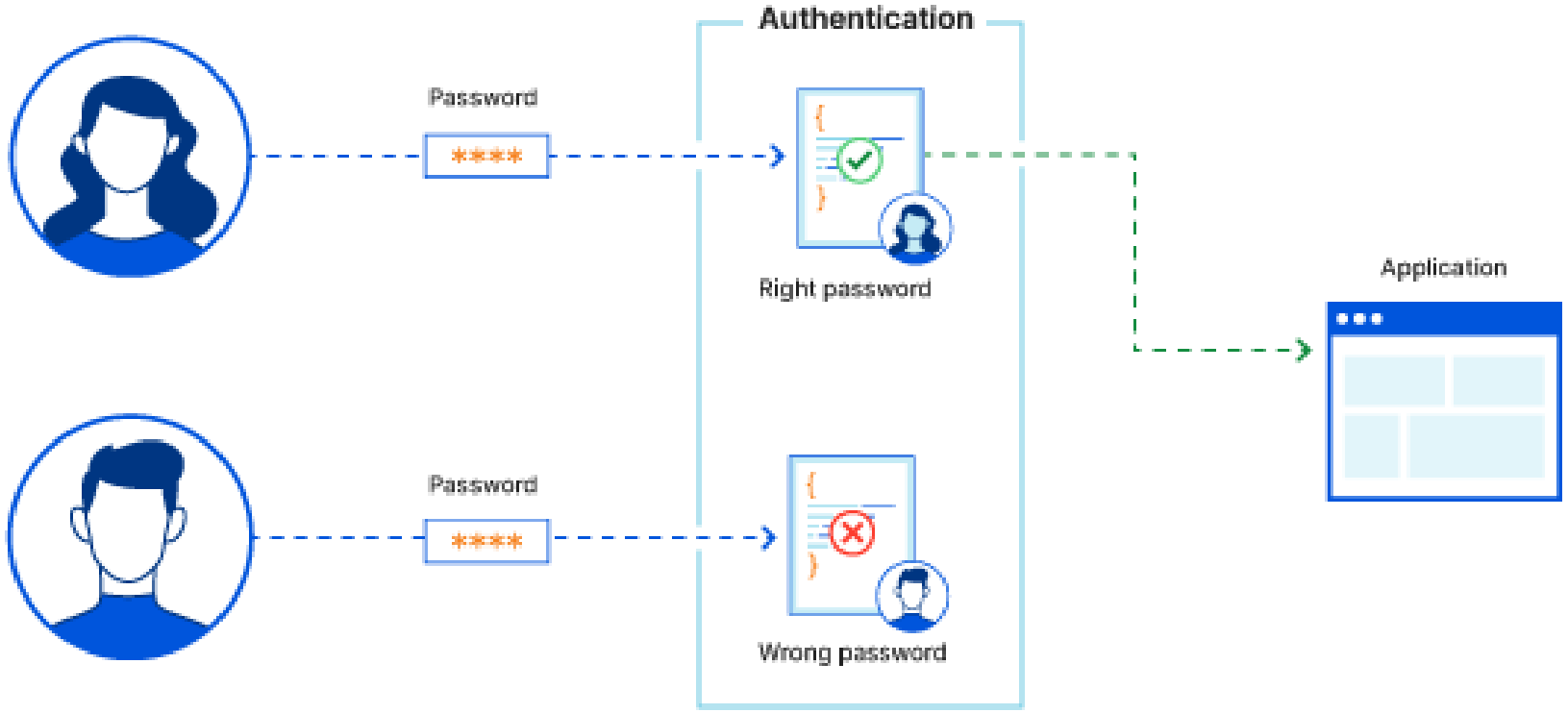


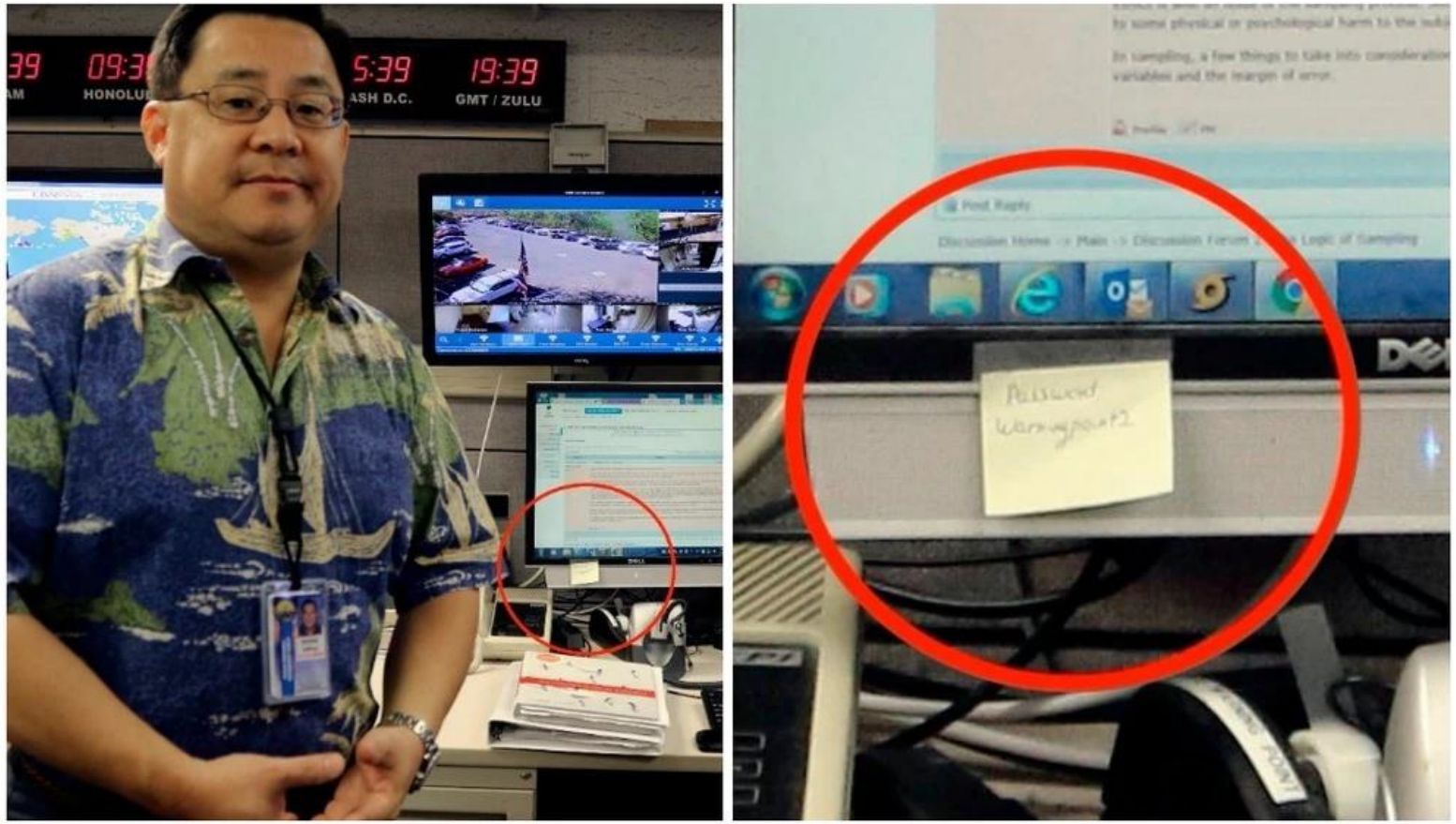
Image source: https://www.cloudflare.com/learning/access-management/what-is-authentication/ (18.2.2023)

Why store passwords?

- Authenticate user
  - Compare entered password with stored password
  - Is it even necessary to store passwords to achieve this?
- Differentiate privileges etc. based on authenticated user
- Examples for widely used user/password „databases“
  - Windows: SAM file and Windows registry
  - Linux: /etc/shadow and /etc/passwd

Obvious ways not to store passwords

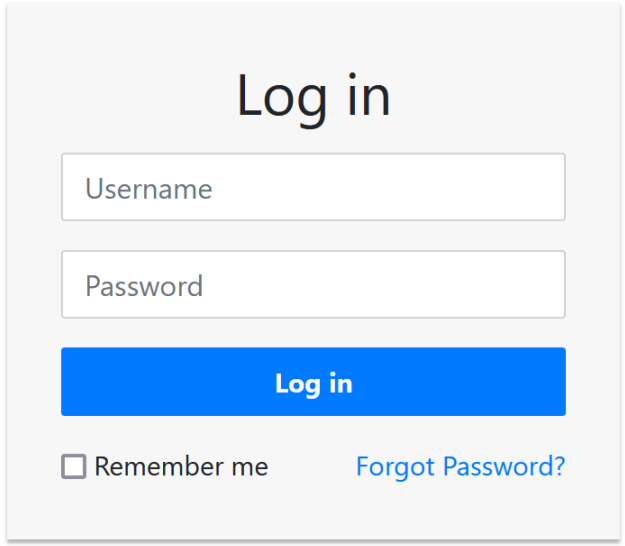
User side – Hawaii's Emergency Management Agency (HEMA), 2018

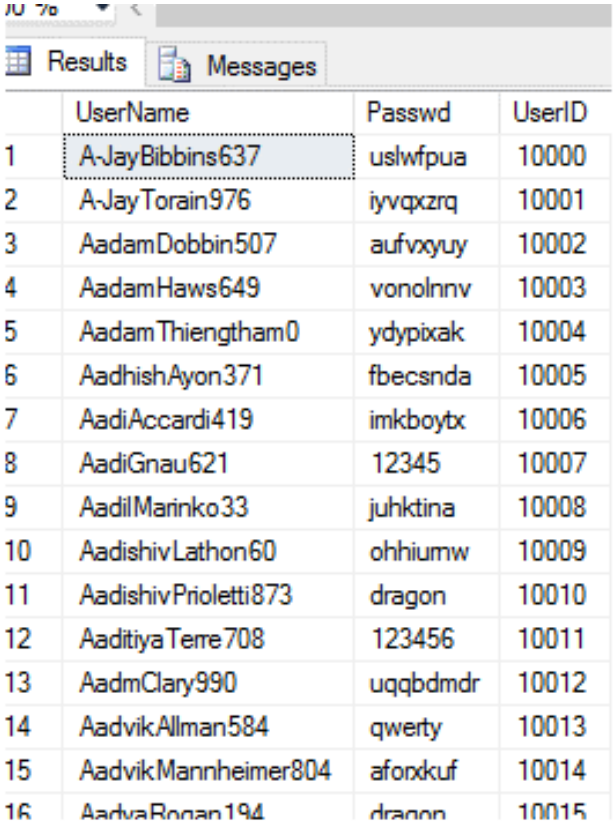


Source: https://www.vice.com/en/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn (18.2.2023)

Service-side password storage

- In plaintext
- Encrypted (still obvious?)
  - Where is the key stored?





	UserName	Passwd	UserID
1	A-JayBibbins637	uslwfpua	10000
2	A-JayTorain976	iyvqxzrq	10001
3	AadamDobbin507	aufvxyuy	10002
4	AadamHaws649	vonolnnv	10003
5	AadamThiengtham0	ydypixak	10004
6	AadhishAyon371	fbecsnda	10005
7	AadiAccardi419	imkboytx	10006
8	AadiGnau621	12345	10007
9	AadilMarinko33	juhktina	10008
10	AadishivLathon60	ohhiumw	10009
11	AadishivPrioletti873	dragon	10010
12	AaditiyaTerre708	123456	10011
13	AadmClary990	uqqbdmdr	10012
14	AadvikAllman584	qwerty	10013
15	AadvikMannheimer804	aforxkuf	10014
16	AadyaRogan194	dragon	10015

Image sources: https://www.mssqltips.com/sqlservertip/4260/storing-passwords-in-sql-server-things-to-know-to-keep-the-data-secure/ (18.2.2023),
https://www.tutorialrepublic.com/snippets/preview.php?topic=bootstrap&file=simple-login-form (18.2.2023)

2018: T-Mobile Austria (revisited)

MOTHERBOARD
TECH BY VICE

T-Mobile Stores Part of Customers' Passwords In Plaintext, Says It Has 'Amazingly Good' Security

A T-Mobile Austria customer representative made a shocking admission in a Twitter thread.

Source: https://www.vice.com/en/article/7xdeby/t-mobile-stores-part-of-customers-passwords-in-plaintext-says-it-has-amazingly-good-security (18.2.2023)

Improving password storage in three simple steps

Hashing I

- Operation that is easy to compute and reproducible

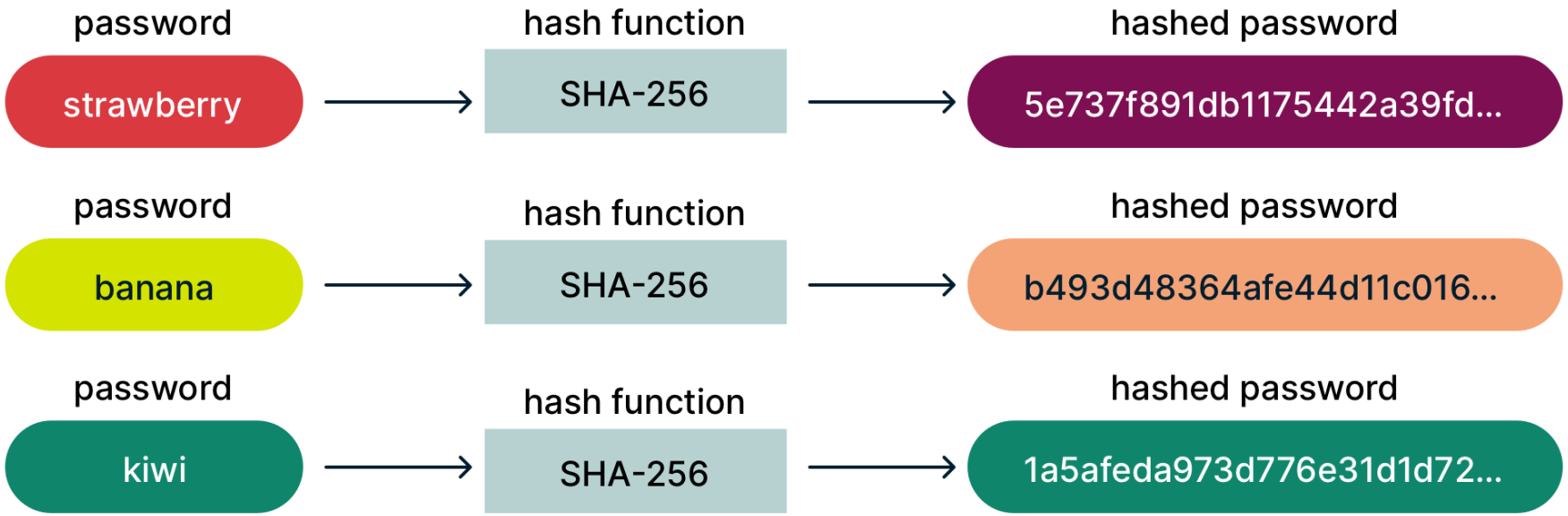


Image source: https://www.expressvpn.com/blog/salt-hash-password-protection/ (18.2.2023)

Hashing II

- Operation that is infeasible to reverse

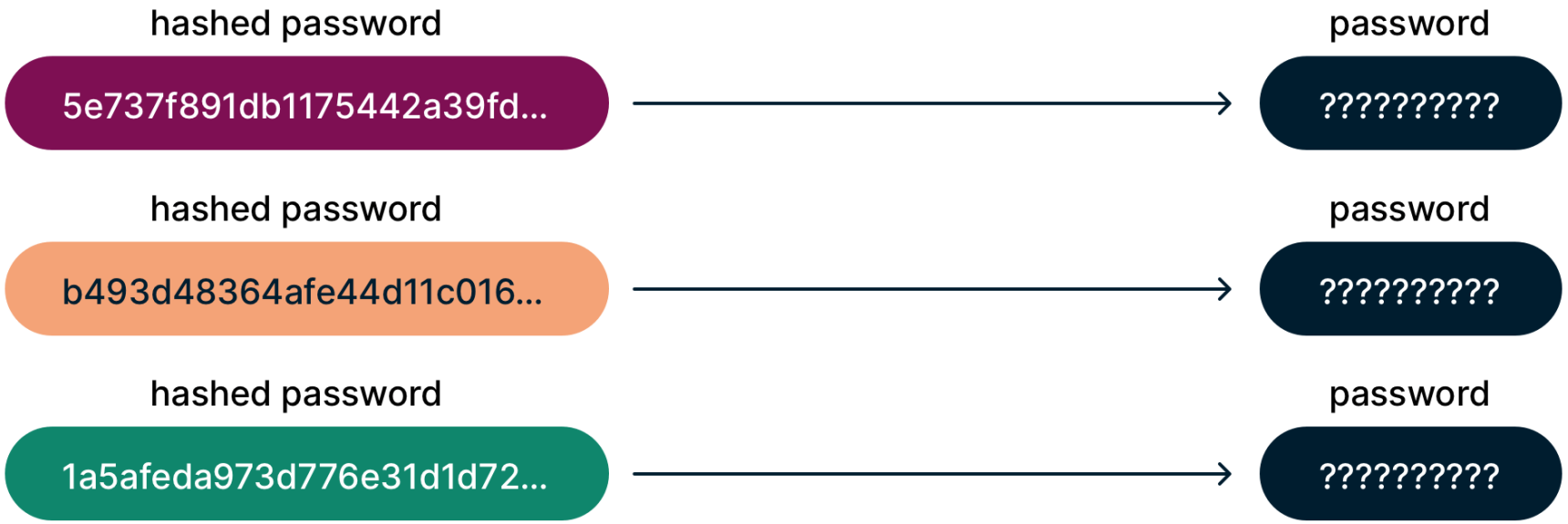


Image source: https://www.expressvpn.com/blog/salt-hash-password-protection/ (18.2.2023)

Improvement 1: Hashing

- Idea: Store a practically irreversible version of the password (hash)
- Authentication: Compare hashes, not passwords

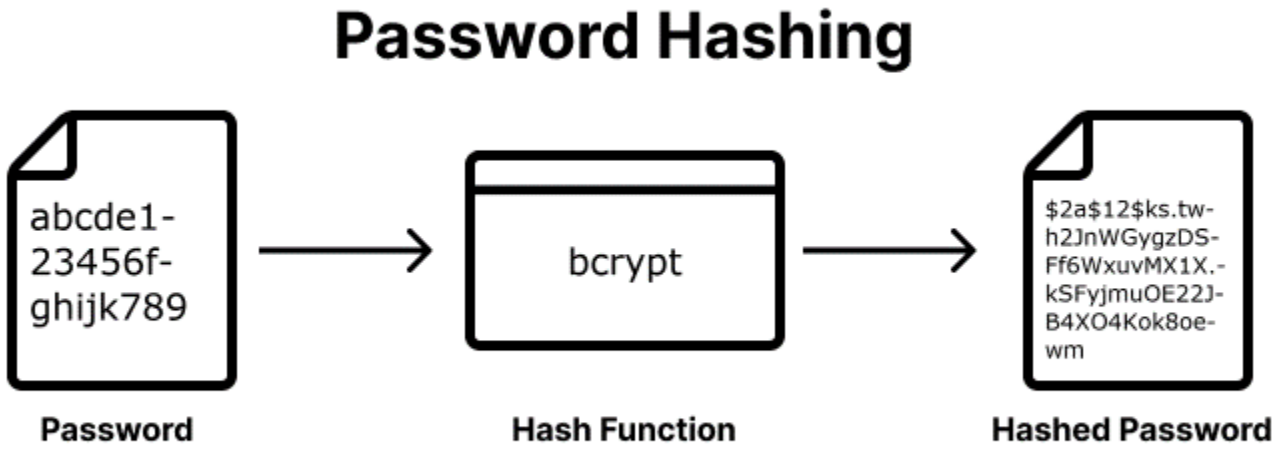


Image source: https://www.authgear.com/post/password-hashing-salting (18.2.2023)

Observation: Same passwords, same hashes

- Identical hashes reveal users with identical passwords
- Identical hashes reduce the effort for an attacker
- How to prevent attackers from knowing who has the same password?

Username	Password Hash (SHA256)
alice	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
bob	308738b8195da46d65c96f4ee3909032e27c818d8a079bccb5a1ef62e8daaa45
charlie	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

Image source: https://medium.com/swlh/introduction-to-salted-hashed-passwords-d19bd6f92480 (18.2.2023)

Salting

- Add text (“salt“) before hashing

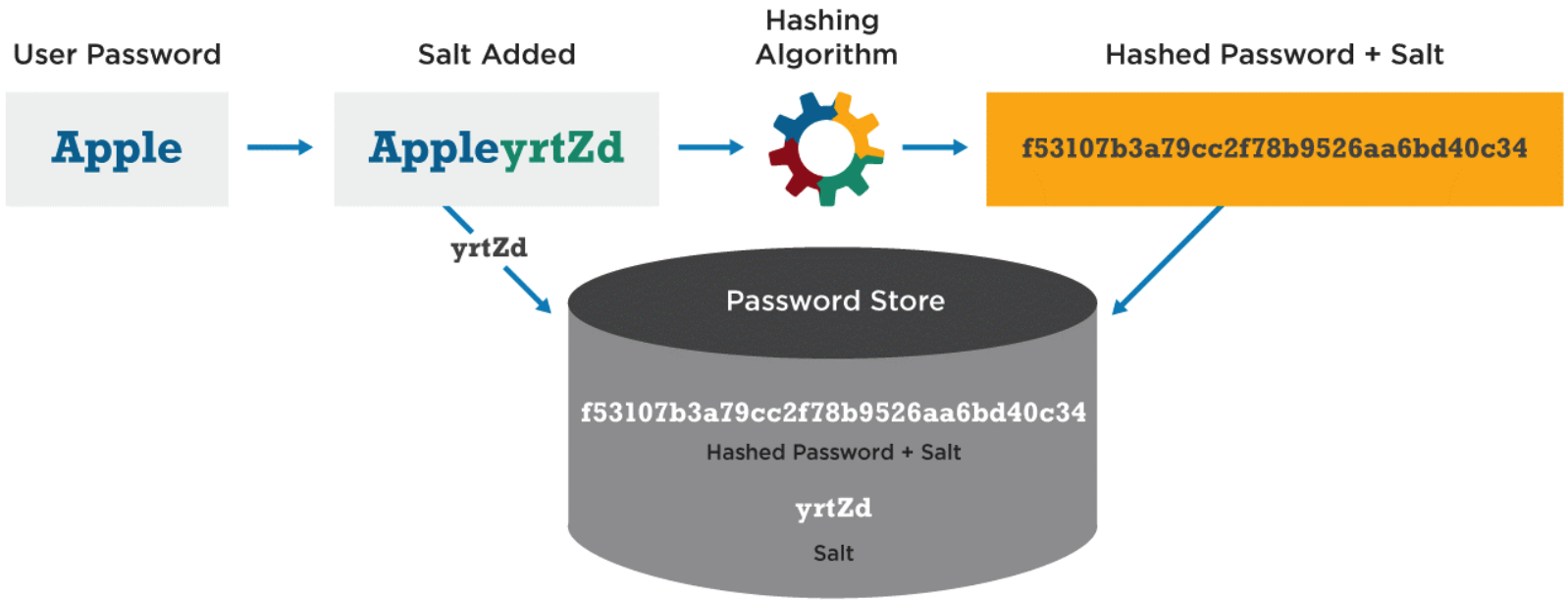


Image source: https://cyberhoot.com/cybrary/password-salting/ (18.2.2023)

Improvement 2: Salting

- Store user-specific salt used for hashing

				
Password	`p4s5w3rdz`	`p4s5w3rdz`	`p4s5w3rdz`	`p4s5w3rdz`
Salt	-	-	`et52ed`	`ye5sf8`
Hash	`f4c31aa`	`f4c31aa`	`lvn49sa`	`z32i6t0`

Image source: https://medium.com/swlh/introduction-to-salted-hashed-passwords-d19bd6f92480 (18.2.2023)

Observation: Hashes are fast to compute

- Hashing is (too) fast → attackers can try out passwords (too) fast
- How to slow attackers down?
- Stretch hashing operation by repeating it on its output
  - Slows down attackers
  - Also slows down legitimate users
  - Security/usability trade-off needed

Improvement 3: Stretching

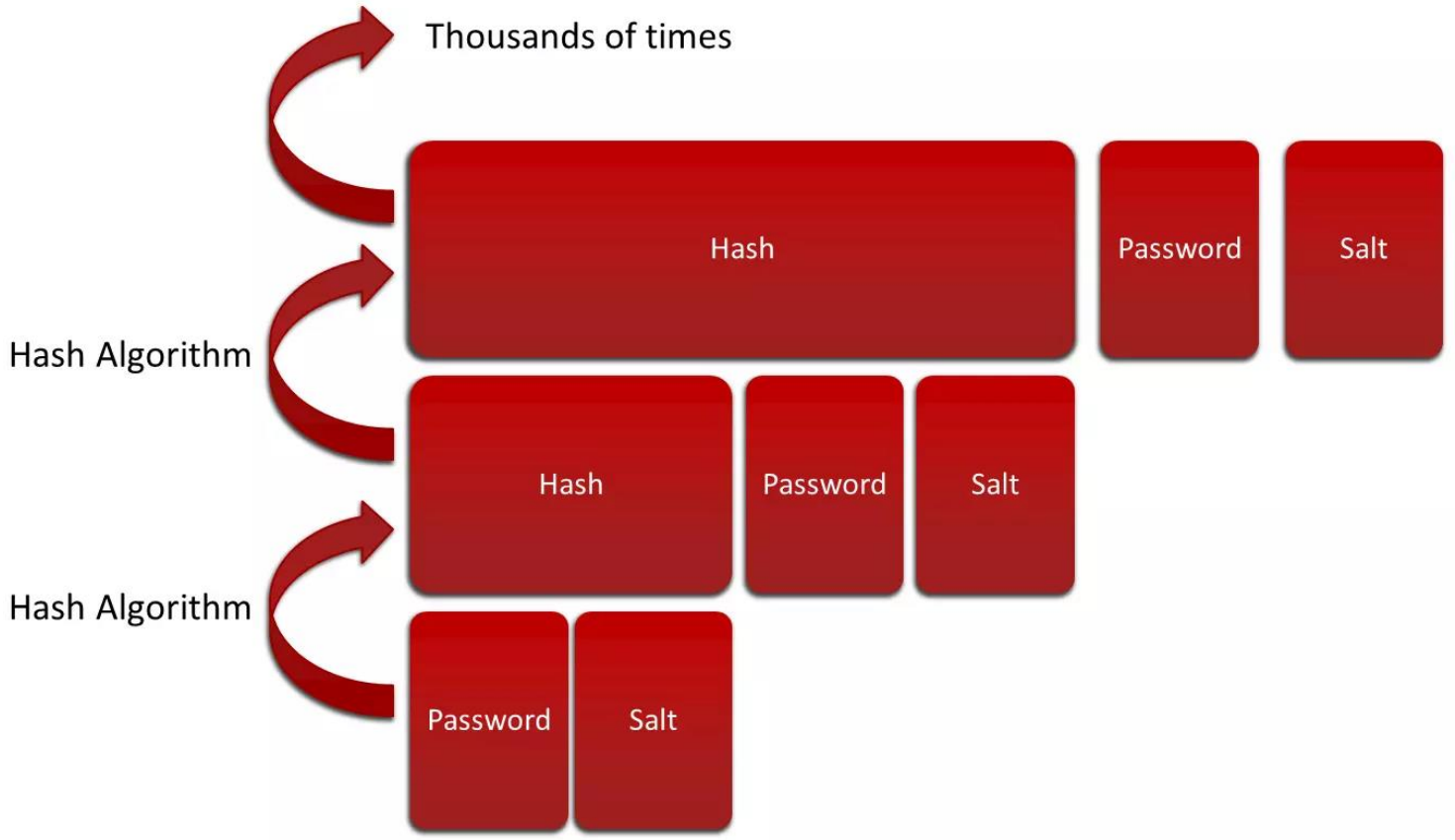


Image source: https://www.sitepoint.com/risks-challenges-password-hashing/ (18.2.2023)

The importance of user passwords

Password hashes: The attacker‘s viewpoint

- Recall: Hashes are infeasible to reverse
- How does an attacker find passwords?
- Try to find a password that produces the same hash
- Types of attack
  - Brute-force
  - Word list/Dictionary
  - More sophisticated attacks (out of scope)

Password recommendations (demo‘d)

- Do not use short passwords
- Do not use simple passwords
- Do not reuse passwords → credential stuffing

- Even hashing, salting, stretching etc. cannot prevent a bad password from being easily retrieved by an attacker

How to store passwords in 2023

How to store passwords (one possibility)

- Service side: Password-Based Key Derivation Function 2 (PBKDF2)
  - Hashing (simplified)
  - Salting
  - Stretching
  - Additional parameters and operations to control output
- User side: Choose password which is
  - Long
  - Complex
  - Unique → Password manager

Further reading

- Katz, Jonathan, and Yehuda Lindell. *Introduction to Modern Cryptography, 3rd ed*. CRC press, 2020.
- Visconti, Andrea, Ondrej Mosnáček, Milan Brož, and Vashek Matyáš. „Examining PBKDF2 security margin—Case study of LUKS.“ *Journal of Information Security and Applications* 46 (2019): 296-306.
- Ur, Blase, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. „Do users‘ perceptions of password security match reality?“ In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 3748-3760. 2016.
- Bauman, Erick, Yafeng Lu, and Zhiqiang Lin. “Half a century of practice: Who is still storing plaintext passwords?” In *Proceedings of the 11th International Conference on Information Security Practice and Experience (ISPEC 2015), Beijing, China, May 5-8*, pp. 253-267. Springer International Publishing, 2015.

Thank you for your attention!

Questions?

Addendum: Why this topic?

Ein Termin für den öffentlichen Vortrag und für die anschließende öffentliche Aussprache (Habilitationskolloquium) mit Ihnen wurde noch nicht fixiert. Sie werden diesbezüglich noch separat per E-Mail kontaktiert. Der Hörsaal (in Itzling) wird Ihnen dann noch rechtzeitig mitgeteilt. Entsprechend der Satzung soll der Vortrag „ein Thema aus dem Fach aber nicht aus der Habilitationsschrift" behandeln. Bitte übermitteln Sie den Titel für Ihren Vortrag bis spätestens 27. Jänner 2023 per E-Mail an isolde.rehrl@plus.ac.at .

Source: Letter from the head of the habilitation commission, dated 25.11.2022, received on 25.11.2022 from isolde.rehrl@plus.ac.at