IMPOSSIBLE TASKS

@sergeybelove

History

2017 – FFmpeg, Imagemagick, Push Notifications VS SMS, Session handling / cookies with hundred of subdomains

2020 - Web-Apps <--> Desktop Apps, promo pages with no server-side and CORS

2023 – Insecure OAuth, blocking bruteforce attacks, cookies and sessions in multidomain env, passwords

HOW TO STORE PASSWORDS

How to store passwords

Generations:

- Plain text
- md4 and similar
- md5()/sha1()/sha256() and so on
- md5(_salt_+$password)
- md5(_salt_+$password+_pepper_)
- md5(_salt_+$password+_pepper_)/2
- sha256(md5(_salt_+$password+_pepper_)/2)

How to store passwords

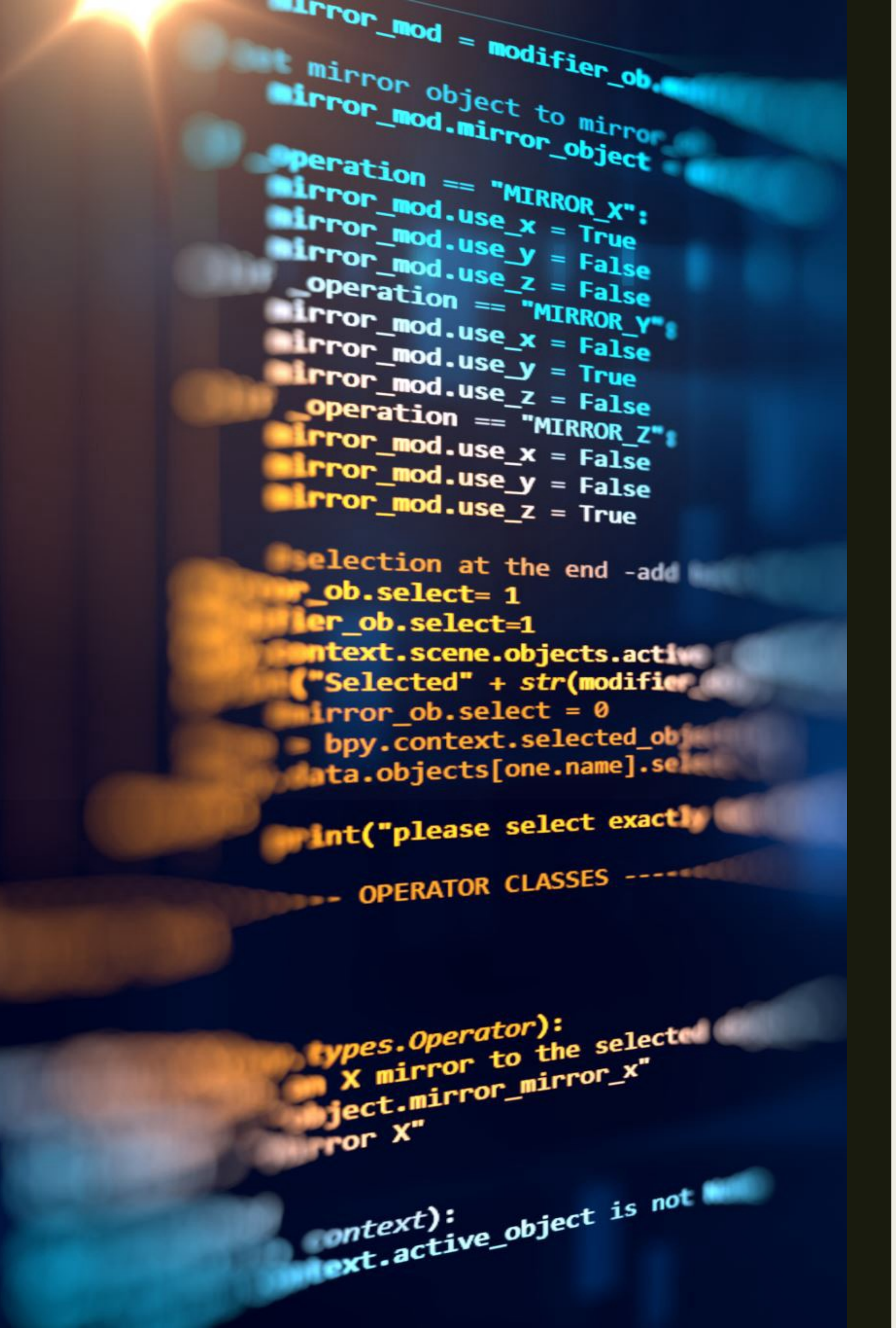
Generations:

- Plain text
- md4 and similar – super easy to bruteforce
- md5()/sha1()/sha256() and so on – brute-forceable
- md5(_salt_+$password) – brute-forceable, but a bit more protection against rainbow tables
- md5(_salt_+$password+_pepper_) – brutable, but a bit more protection against rainbow tables (_salt_) + sql dump without access to application itself (_pepper_)
- md5(_salt_+$password+_pepper_)/2 - ???
- sha256(md5(_salt_+$password+_pepper_)/2) - ??? x2

How to store passwords

Recently, it became better

- Argon2
- BCrypt
- Scrypt

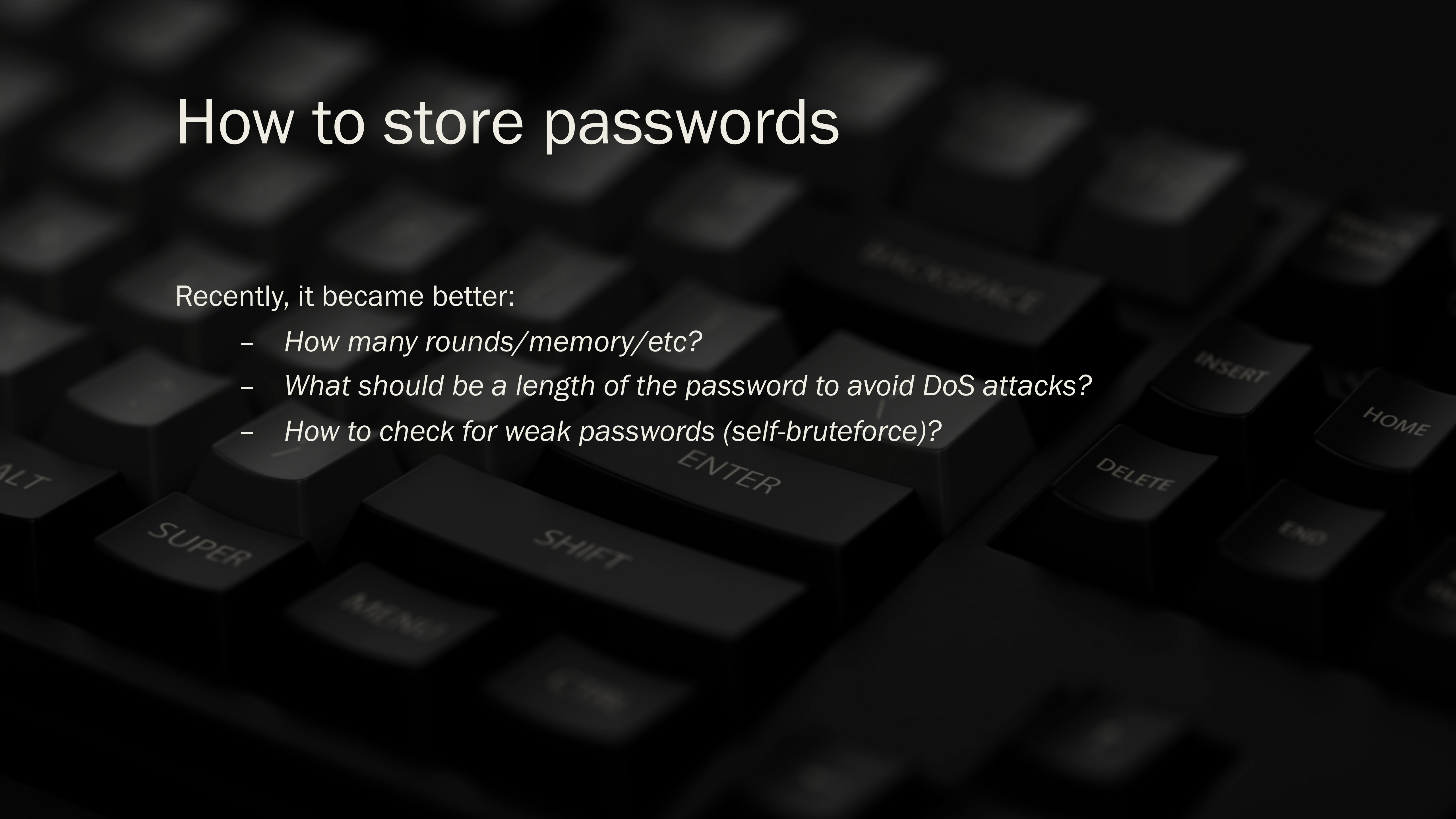


How to store passwords

Recently, it became better

- Argon2 - is a great memory-hard password hashing algorithm, which makes it good for offline key derivation. But it requires more time, which, for web applications is less ideal.
- Bcrypt - can deliver hashing times under 1 second long, but does not include parameters like threads, CPU, or memory hardness.
- Scrypt - is maximally hard against brute force attacks, but not quite as memory hard or time-intensive as Argon2

// https://stytch.com/blog/argon2-vs-bcrypt-vs-scrypt/



How to store passwords

Recently, it became better:

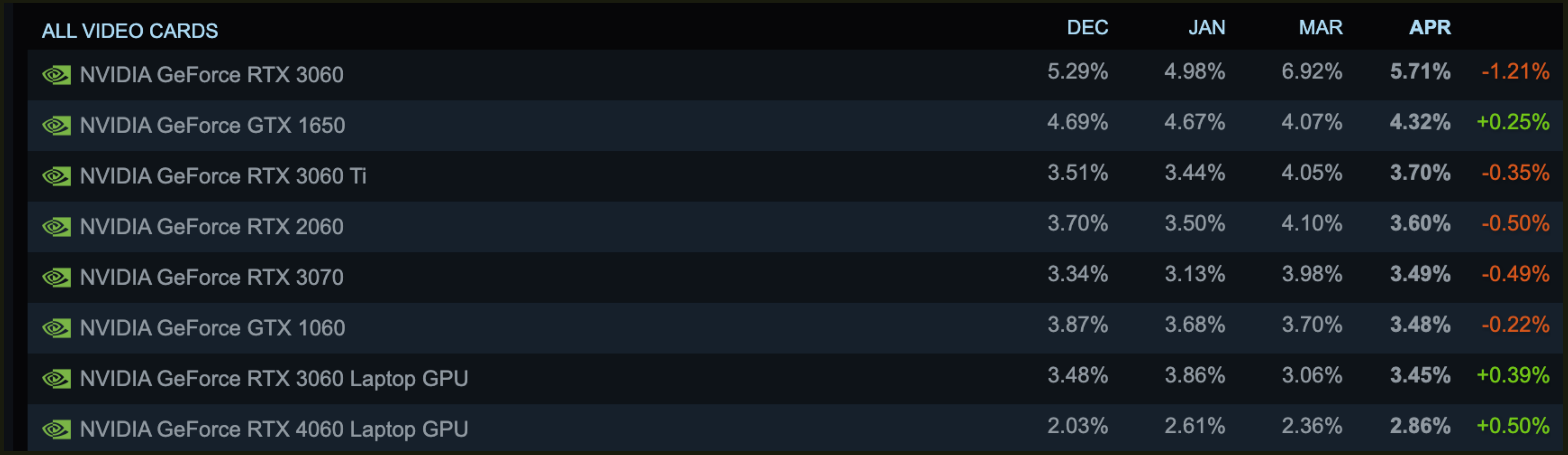
- *How many rounds/memory/etc?*
- *What should be a length of the password to avoid DoS attacks?*
- *How to check for weak passwords (self-bruteforce)?*

How to store passwords
Hardening stage 1/3

How many rounds and length:

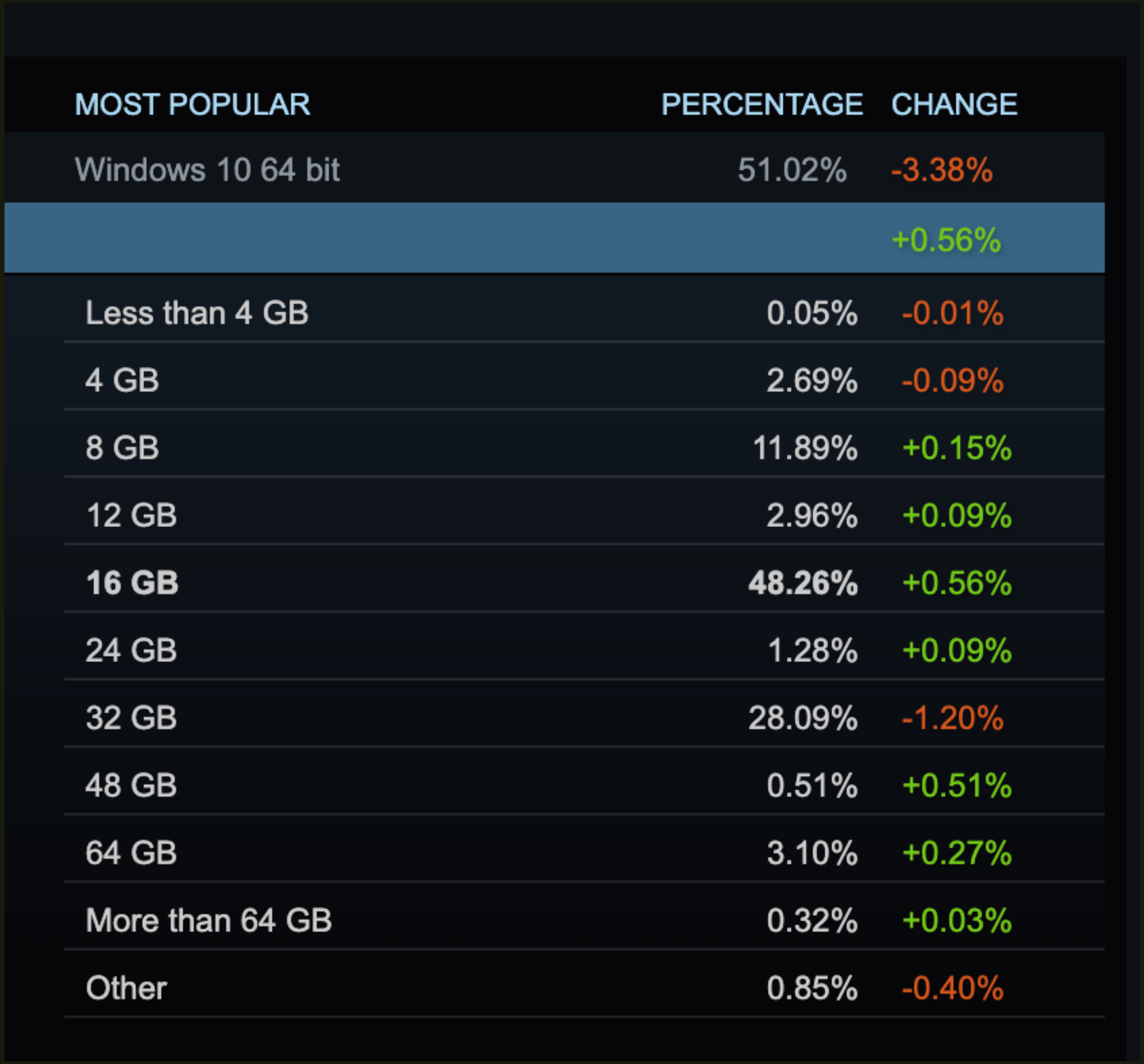
- Imagine first: dumped hashes going to bruteforced via botnets, distributed around the world
- Analyze current typical botnet PC, e.g. Steam hardware report (worst case, expensive botnet)
- Adjust rates to calculate hash for reasonable/longest time, e.g. your password-hashing farm should calculate it within 50-100ms
- Length to avoid DoS: just reasonable, seems 1024 is fine so far
- Check weak passwords during login, while you have them in plaintext (throw stones at those who hash passwords before sending them to the server)

HOW TO STORE PASSWORDS
HARDENING STAGE 1/3



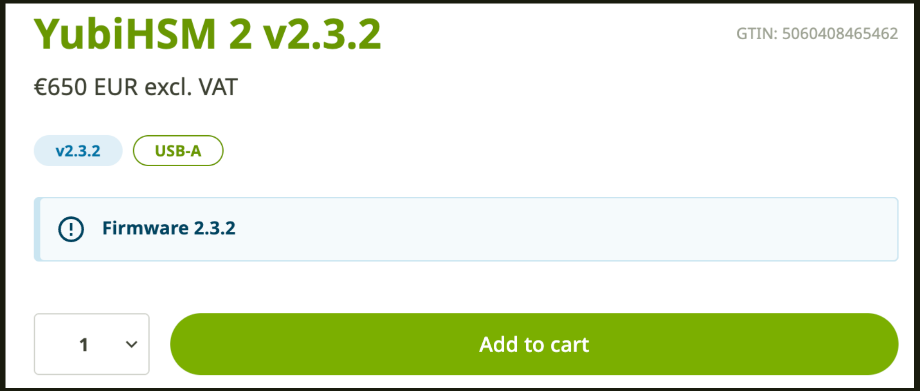
ALL VIDEO CARDS	DEC	JAN	MAR	APR	
NVIDIA GeForce RTX 3060	5.29%	4.98%	6.92%	**5.71%**	-1.21%
NVIDIA GeForce GTX 1650	4.69%	4.67%	4.07%	**4.32%**	+0.25%
NVIDIA GeForce RTX 3060 Ti	3.51%	3.44%	4.05%	**3.70%**	-0.35%
NVIDIA GeForce RTX 2060	3.70%	3.50%	4.10%	**3.60%**	-0.50%
NVIDIA GeForce RTX 3070	3.34%	3.13%	3.98%	**3.49%**	-0.49%
NVIDIA GeForce GTX 1060	3.87%	3.68%	3.70%	**3.48%**	-0.22%
NVIDIA GeForce RTX 3060 Laptop GPU	3.48%	3.86%	3.06%	**3.45%**	+0.39%
NVIDIA GeForce RTX 4060 Laptop GPU	2.03%	2.61%	2.36%	**2.86%**	+0.50%

HOW TO STORE PASSWORDS *HARDENING STAGE 1/3*



MOST POPULAR	PERCENTAGE	CHANGE
Windows 10 64 bit	51.02%	-3.38%
		+0.56%
Less than 4 GB	0.05%	-0.01%
4 GB	2.69%	-0.09%
8 GB	11.89%	+0.15%
12 GB	2.96%	+0.09%
16 GB	**48.26%**	+0.56%
24 GB	1.28%	+0.09%
32 GB	28.09%	-1.20%
48 GB	0.51%	+0.51%
64 GB	3.10%	+0.27%
More than 64 GB	0.32%	+0.03%
Other	0.85%	-0.40%

HOW TO STORE PASSWORDS *HARDENING STAGE 2/3*



YubiHSM 2 v2.3.2

GTIN: 5060408465462

€650 EUR excl. VAT

ⓘ Firmware 2.3.2

YubiKey 5 Series

YubiKey 5 Nano

GTIN: 5060408461457

€60 EUR excl. VAT

How to store passwords *Hardening stage 2/3*

Attacker got physical access to server with hashes and have a full access to the filesystem. How to protect? Let’s use YubiHSM!

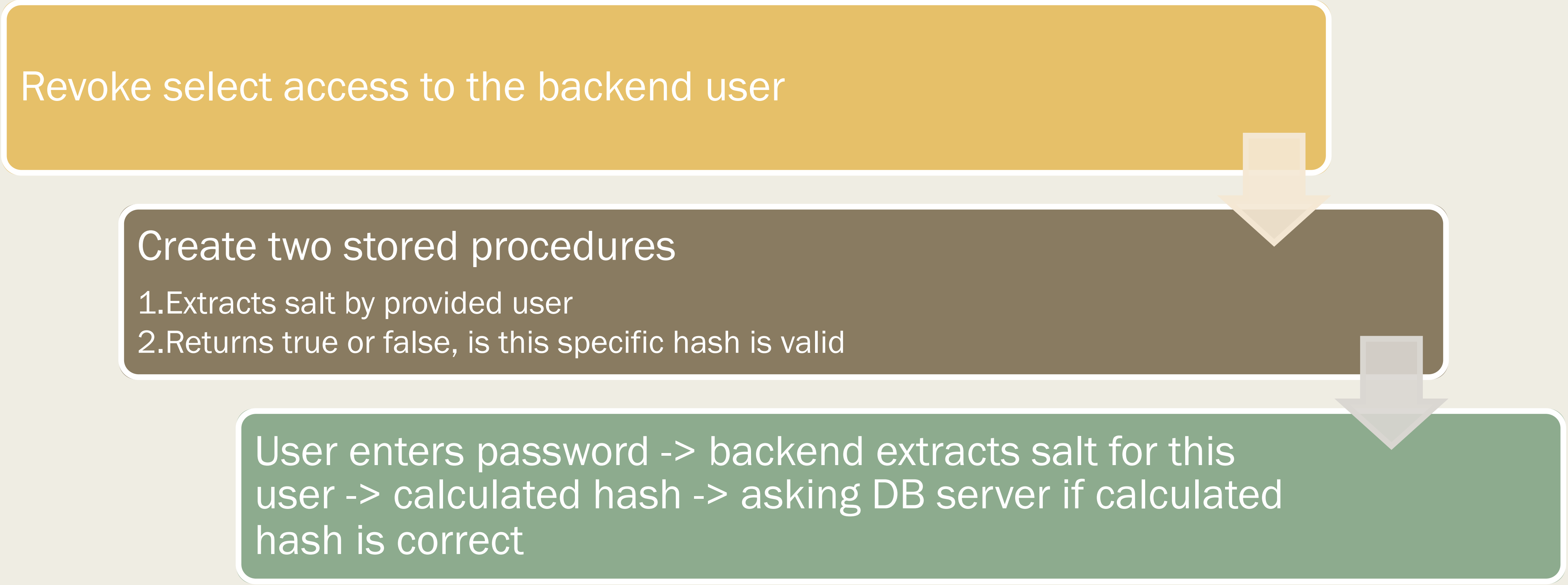
- AES-(128|192|256)-CCM-Wrap: ~10ms
- ECDSA-P224-SHA1: ~64ms

HOW TO STORE PASSWORDS

HARDENING STAGE 3/3

Imagine, all the frontends backends are compromised, but attacker cannot dump password hashes. How?

HOW TO STORE PASSWORDS
HARDENING STAGE 3/3

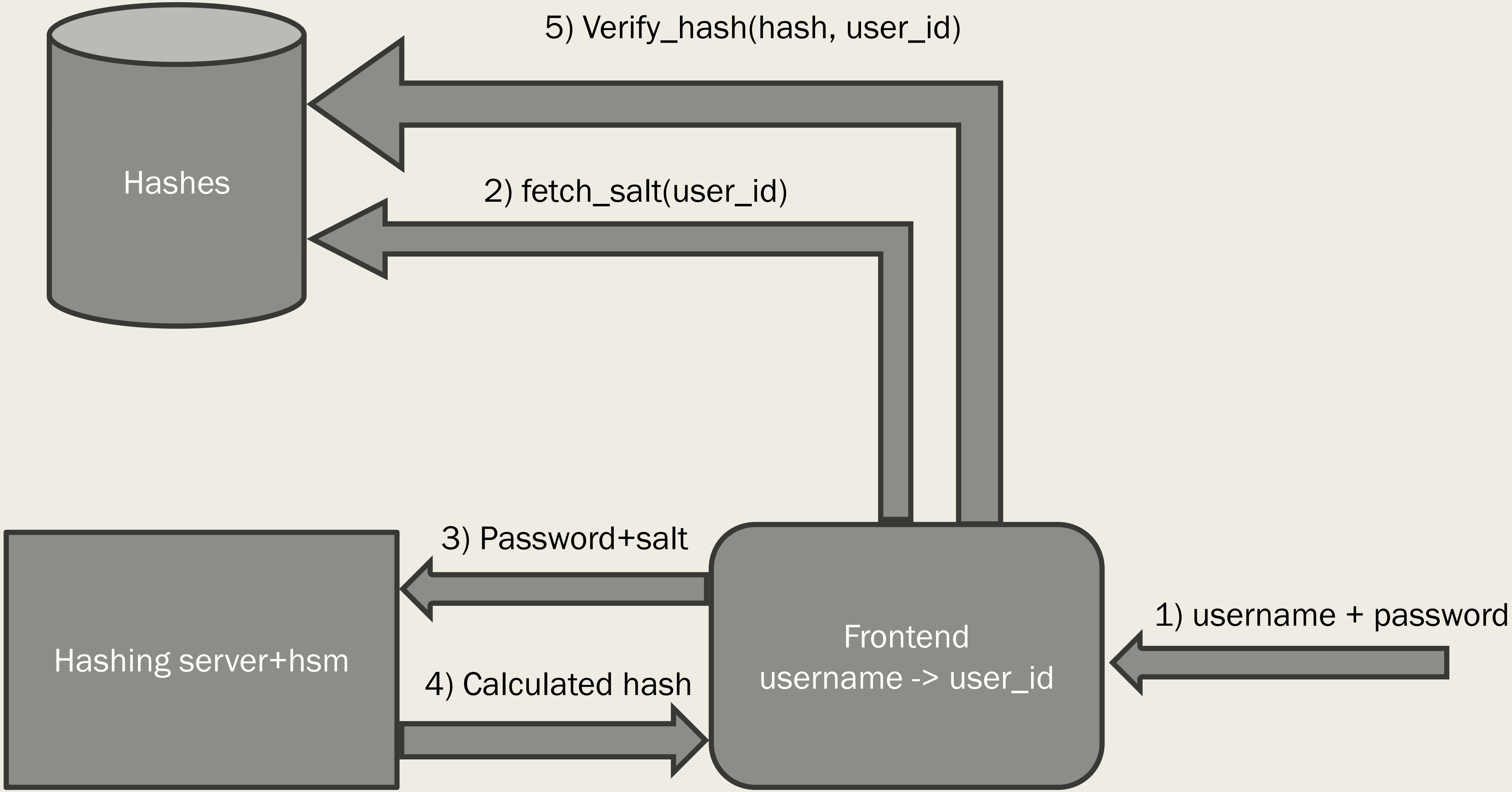


Revoke select access to the backend user

Create two stored procedures

1.Extracts salt by provided user
2.Returns true or false, is this specific hash is valid

User enters password -> backend extracts salt for this user -> calculated hash -> asking DB server if calculated hash is correct


5) Verify_hash(hash, user_id)
Hashes
2) fetch_salt(user_id)
3) Password+salt
Hashing server+hsm
4) Calculated hash
Frontend
username -> user_id
1) username + password

SBOM SBOM SBOM

Supply chain

Supply chain

Supply chain

Supply chain

What is the European Cyber Resilience Act (CRA)?

The European Cyber Resilience Act (CRA) is a legal framework that describes the cybersecurity requirements for **hardware and software products with digital elements** placed on the market of the European Union. Manufactures are now obliged to take security seriously throughout a product’s life cycle.

Software Bill of Materials (SBOM)

Collecting SBOM is one of the technical requirements by CRA

3 common ways to implement

Dependency track (go.mod, requirements.txt, other includes) – well-known process, but limited coverage

Runtime dynamic trace – coverage challenge

Unpacking and Reverse Engineering

SBOM - Reverse Engineering

Collecting SBOM is one of the technical requirements by CRA

Challenges:

- *External binary static-linked libraries (multiple versions of cURL, SQLite, etc)*
- *Dynamic loading over internet upon needs*
- *Copy-pasted code from 3rd party*
- *“Copy-pasted” cryptographic primitives*
- *UEFI, firmware of network cards etc in case of shipping hardware (WAFs, email sandboxes)*

Only commercial tools are available to solve this task

(say if you know proper free tools?)

ANONYMIZED PSEUDONYMIZED DE IDENTIFIED

Statistics – is it real?

BBC

Google to delete records from Incognito tracking

Google has agreed to delete billions of records and submit to some restrictions on its power to track users, under the terms of a proposed...

1 Apr 2024

NPR

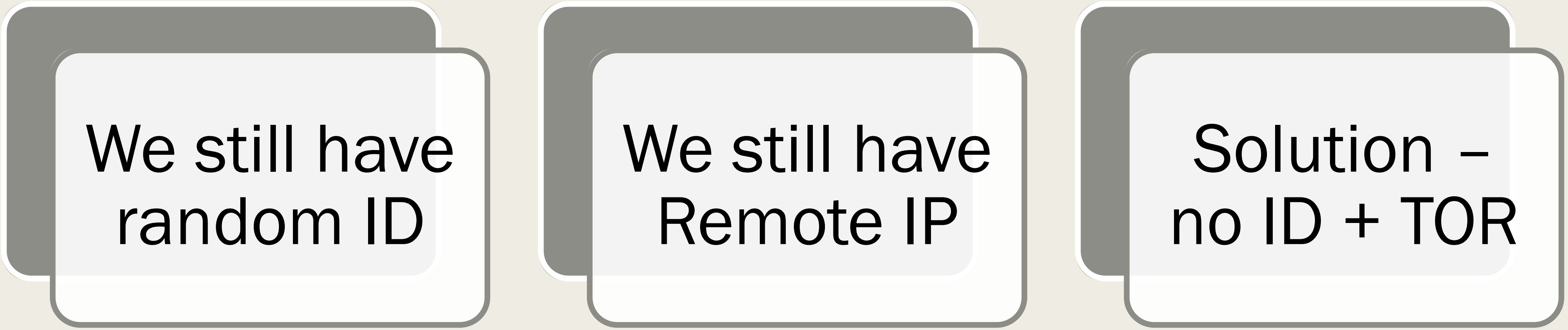
Google to delete search data of millions who used 'incognito' mode

In an agreement released on Monday, Google said it will permanently remove information it secretly gathered when millions of people were...

1 Apr 2024

France 24

Google to delete incognito search data to end privacy suit



We still have random ID

We still have Remote IP

Solution – no ID + TOR

CHEERS EVERYONE!

Any questions?

@sergeybelove