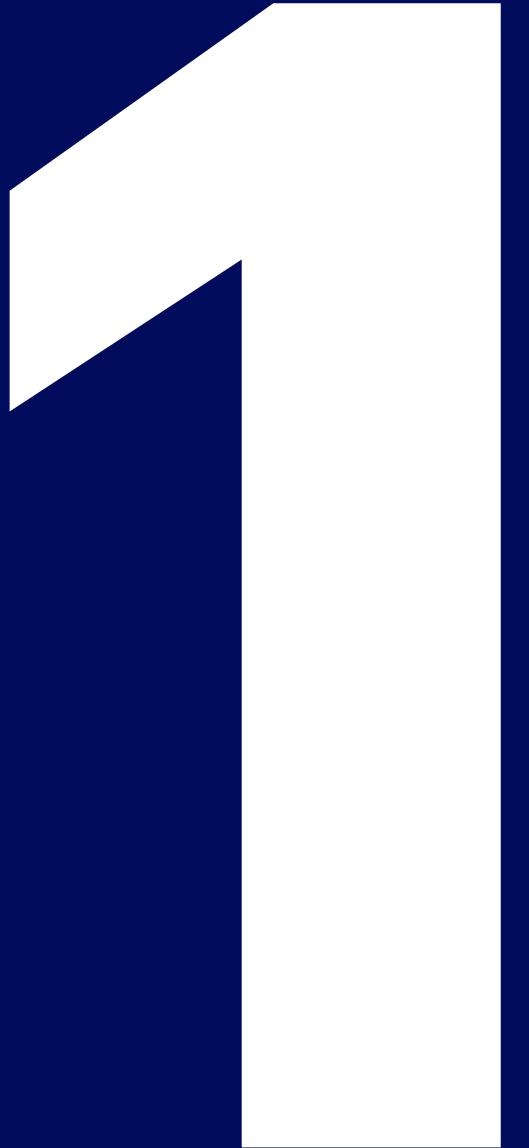
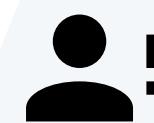
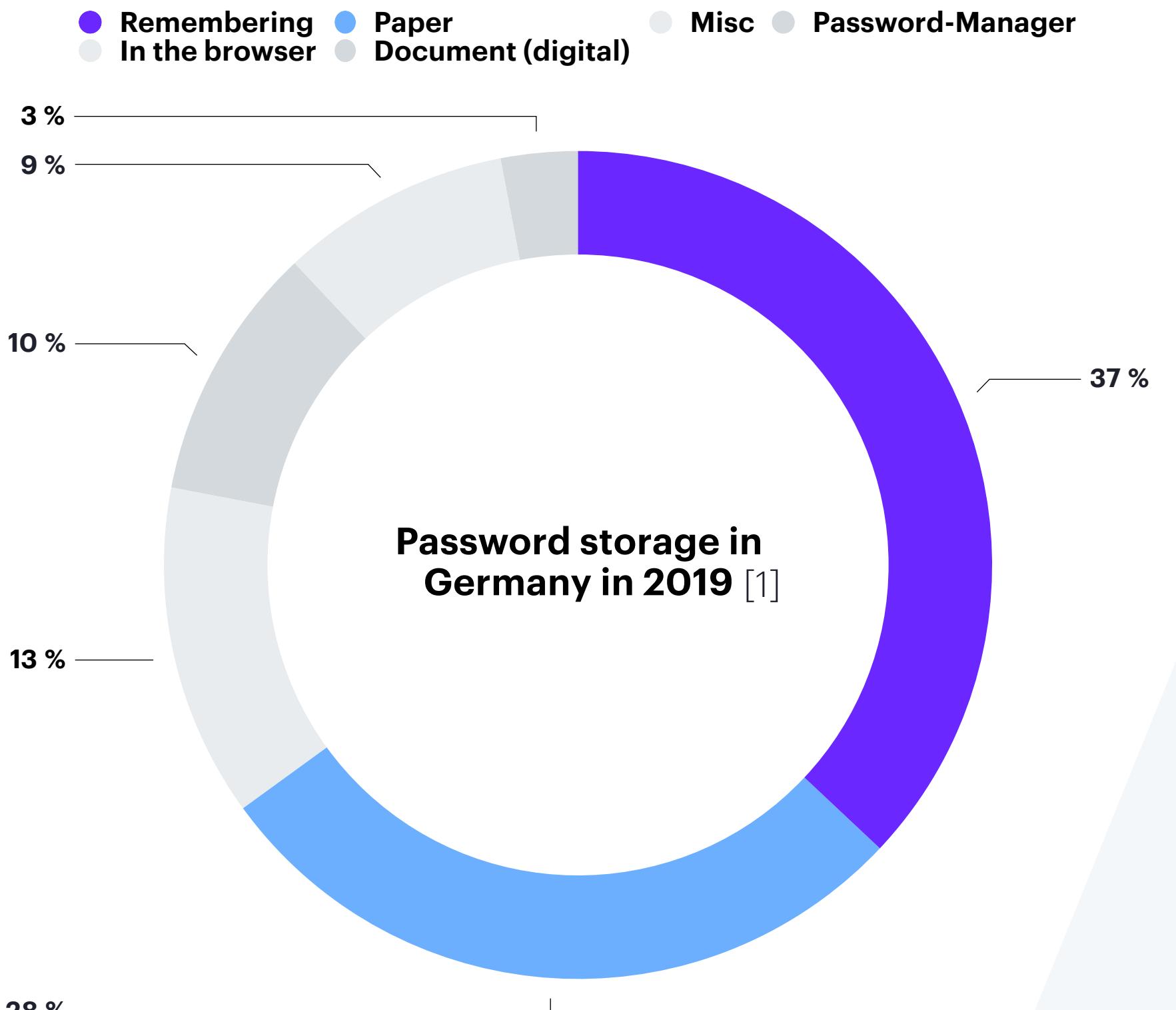


Security Evaluation of Multi-Factor Authentication in Comparison with the Web Authentication API

Motivation

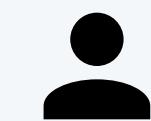
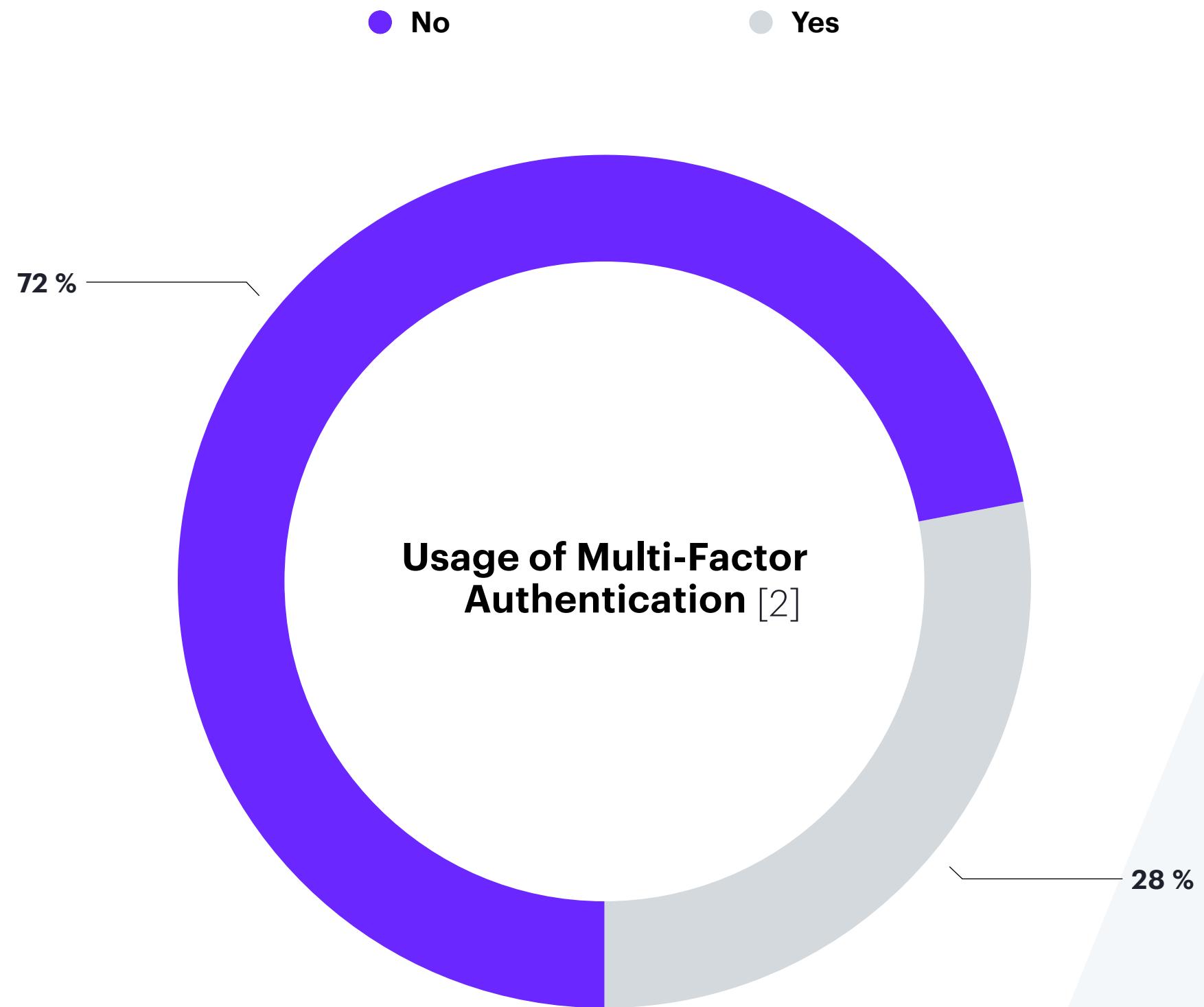


Password storage in Germany in 2019



Over 65% do not use password manager!

Usage of Multi-Factor Authentication in the US in 2017



Over 70% do not use multi-factor authentication!

Amount of Breached Credentials in One Year

1 900 000 000^[3]

One-Factor Authentication



Methods of Authentication

Knowledge

- > Secret only the user knows
- > Examples
 - > Password, PINs
 - > Security question

Possession

- > A possession only the user has (access to)
- > Hard- or Software
- > Examples
 - > Chipcard
 - > (Security-) key
 - > App

Biometrics

- > Physical trait
- > Examples
 - > Face, Iris, Ear
 - > Fingerprint, ...

Further methods

- > Location-based
- > Time-based
- > Behavior-based
- > Social authentication

Security Aspects



Threats Independent of the Authentication Method

Initialization

- > Malware on infected devices can intercept, eavesdrop, and forward secrets
- > Security cameras (IoT), a colleague looking over your shoulder or webcams can gain access to the information, too

Transmission

- > Eavesdropping on the communication (i.e. HTTP traffic)
- > Manipulation of the ports (e.g. USB port) or sensors

Knowledge

- > The human brain has difficulties remembering a strong, unique password for every account
- > Re-usage of the same password for different/multiple accounts
- > Usage of easy to guess passwords, or passwords that are associated with the user
- > Saving/storing passwords in a unsecured manner

- > Security questions can decrease the security when answered honestly
- > Forced password change does not increase the security

- > Unknown if the service provider, e.g., hashes, salts or peppers the passwords
- > Often one password hash is enough for further attacks

Possession

- > Danger of theft, loss, damage, or oblivion
- > Usable by other persons upon theft or loss
- > Wireless communication might be eavesdropped on
- > Replacement is more expensive than knowledge

Biometrics

- > Traits can change over time
- > (Temporary) unavailability due to injuries
- > Problems of the “intra-user variance”
- > Data privacy and security concerns of the user
- > Traits are copyable; but not replaceable

Multi-Factor Authentication



One-Time Passwords

- > Event-based (HOTP) and time-based (TOTP), both are standardized in the RFCs
- > Based on “Message Authentication Codes”
- > Usage of a shared secret
- > Generation on the client side (e.g. via Apps) or on the server
 - > Transmission of the password via e-mail or SMS
- > Proprietary solutions from RSA and Yubico exist, too

Security Keys

- > Can be realized in both hardware and software
- > RSA SecurID is a well known example
 - > Generates 60s OTP, too
- > Universal Second Factor (U2F) as an open standard
 - > No specification by, e.g. the W3C; experimental API
 - > Security keys can communicate via USB, BLE, or NFC
 - > Usage of public-key authentication and the challenge-response protocol

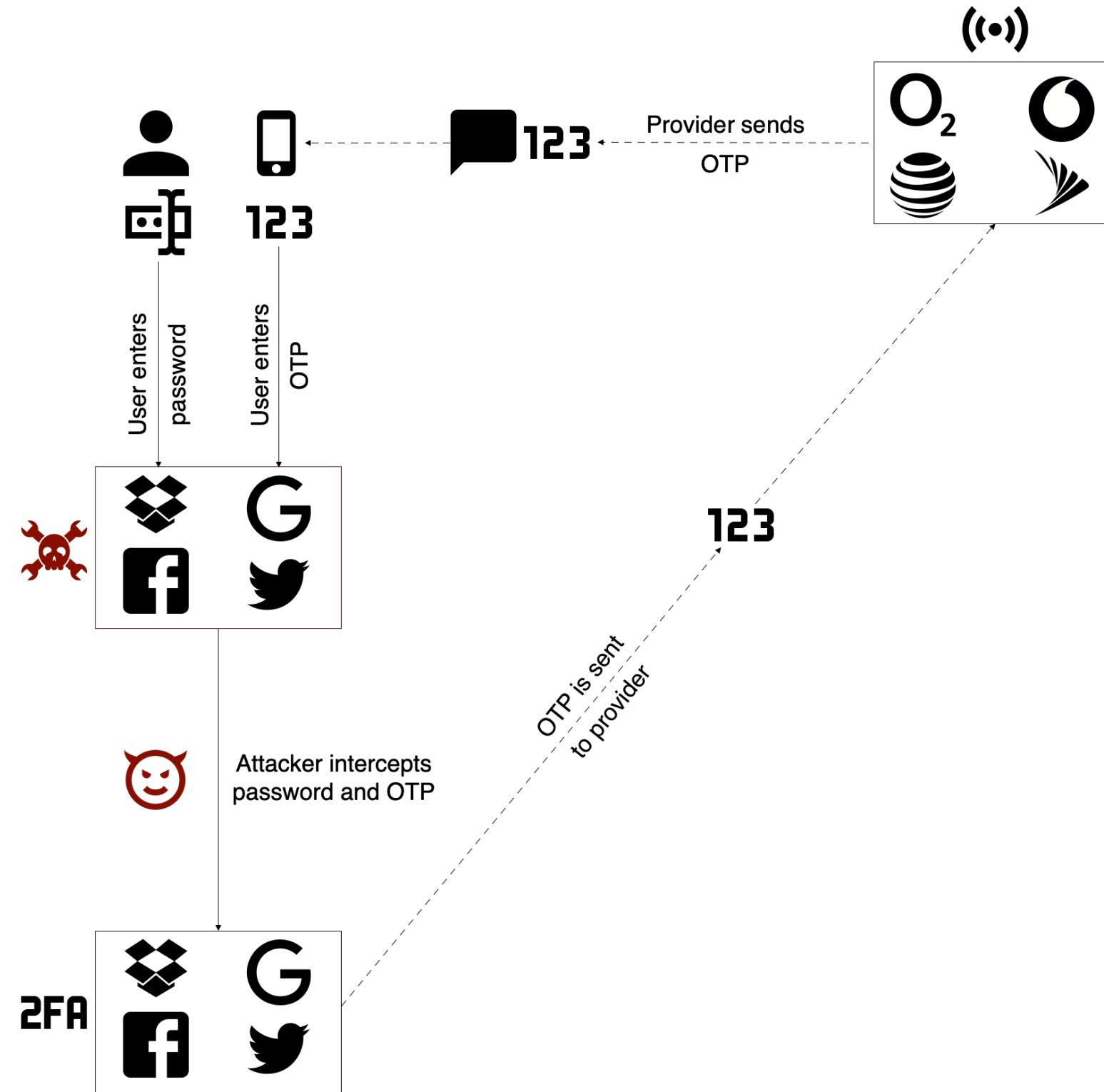
Security Aspects



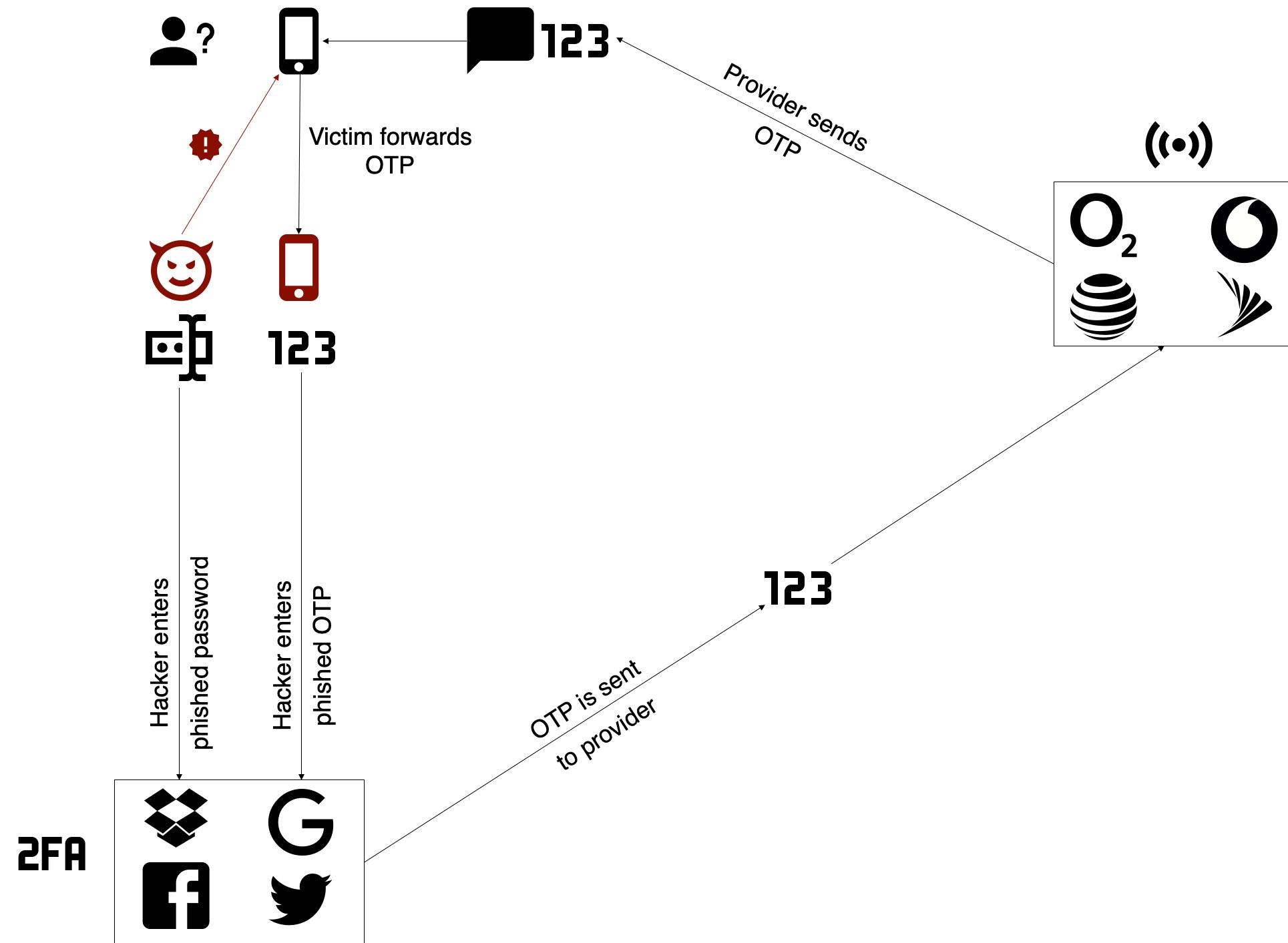
One-Time Passwords

- > Used algorithm are secure
- > Collisions of MD5 and SHA-1 do not expose a threat
- > Exploitation of faulty configurations
 - > Chosen alphabet is too small
 - > Missing invalidation of the passwords
 - > No restriction of authentication can enable brute-force attacks
 - > Problems with time synchronization
 - > Look ahead window can increase the attack surface
- > Lack of requiring the second factor when disabling it

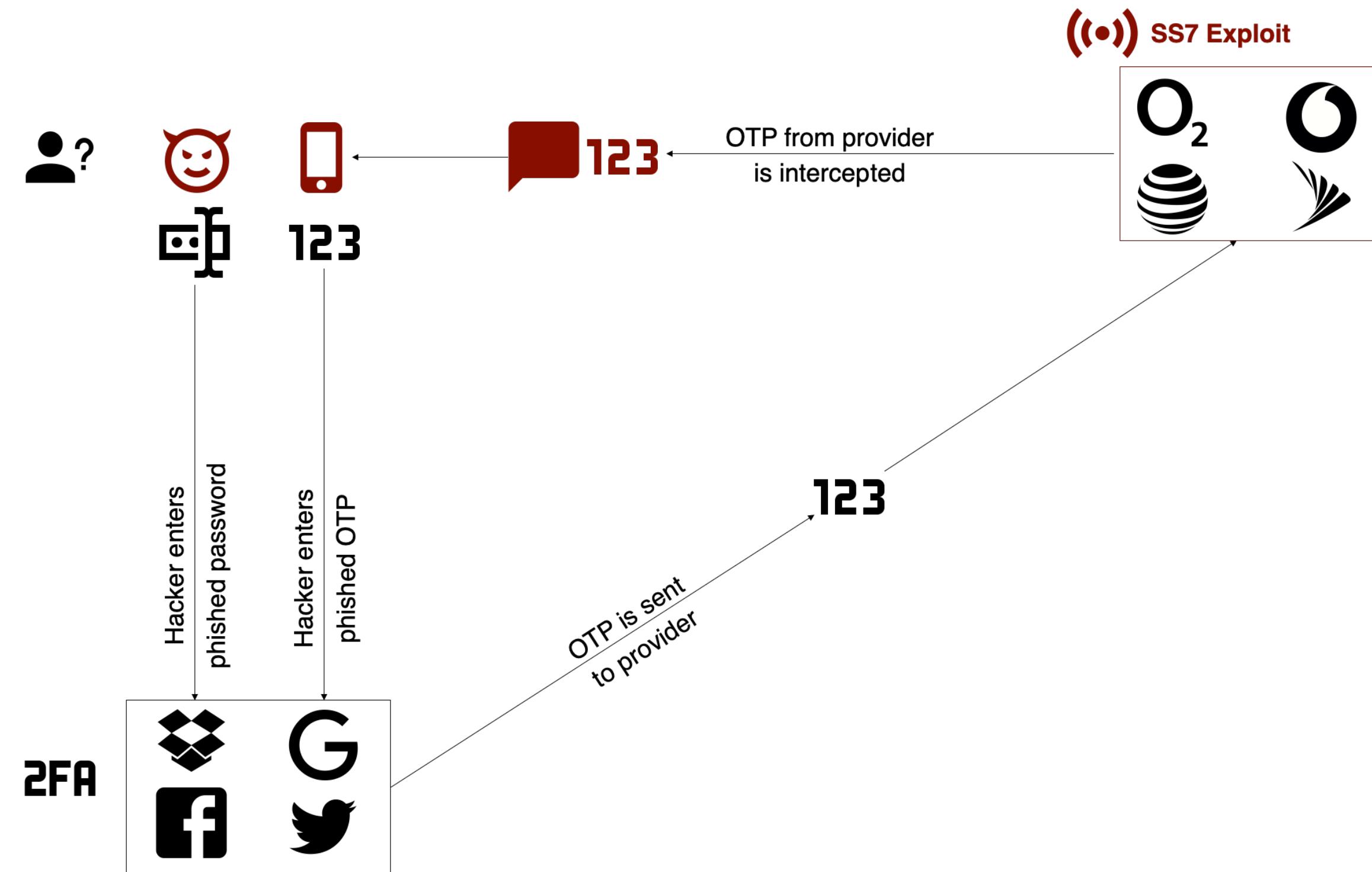
Successful Phishing Attack With 2FA enabled



Verification Code Forwarding Attack



SS7 Attack



Security Keys

- > Threats of authentication by possession apply, too
- > RSA Hack in 2011 resulted in the replacement of 40 million tokens because the private key was stolen
- > Often no possibility to upgrade the firmware on the security keys

- > Vulnerability to side-channel attacks
- > Physical attacks against the chips

- > Central metadata service of the U2F protocol is a lucrative target

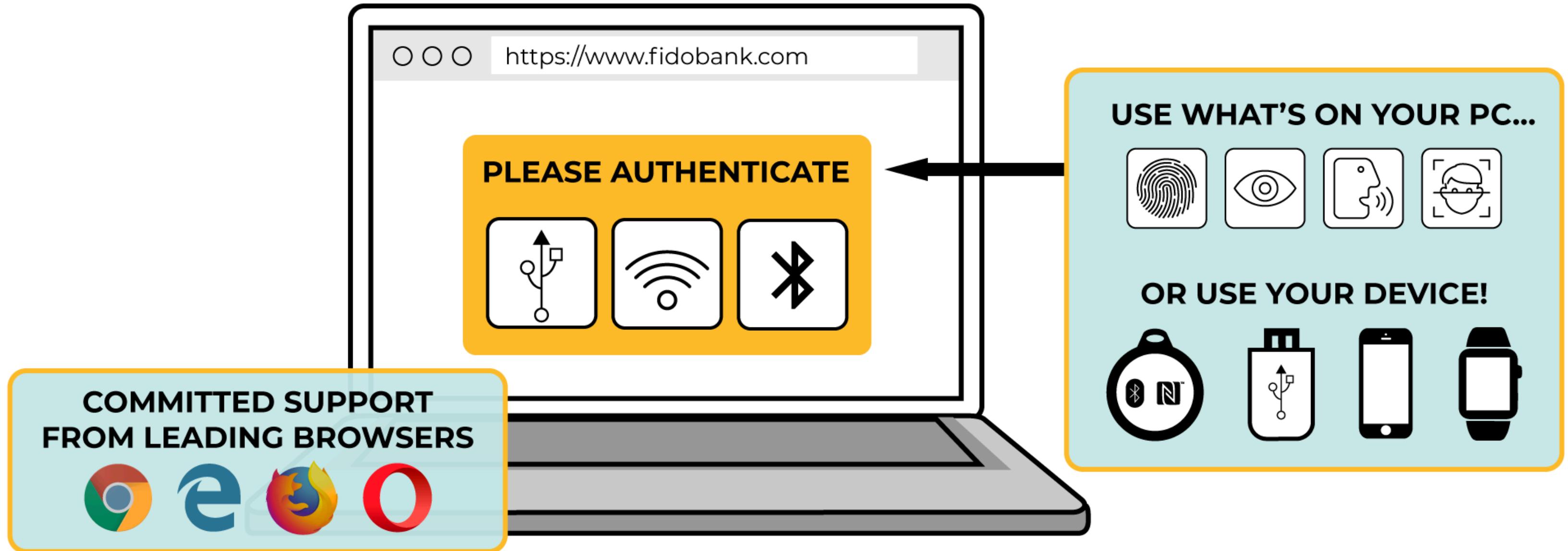
Web Authentication API



**“An API for accessing Public Key
Credentials [...]”** ^[4]

**“[...] enabling the creation and use of
strong, [...] public key-based
credentials by web applications, for
the purpose of strongly authenticating
users.”** ^[4]

Web Authentication API

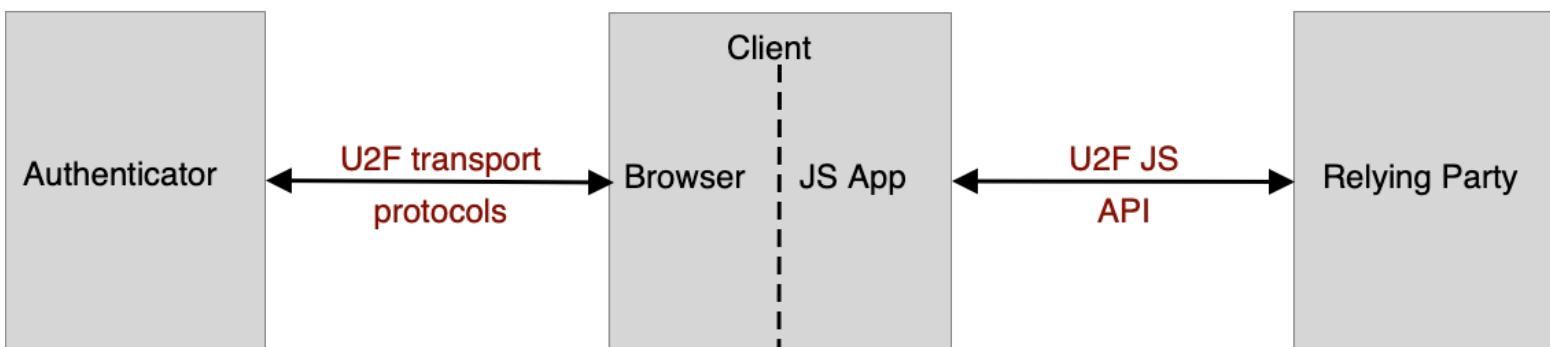


Source: <https://www.w3.org/2018/04/pressrelease-webauthn-fido2.html.en>; last accessed on 11/03/2019

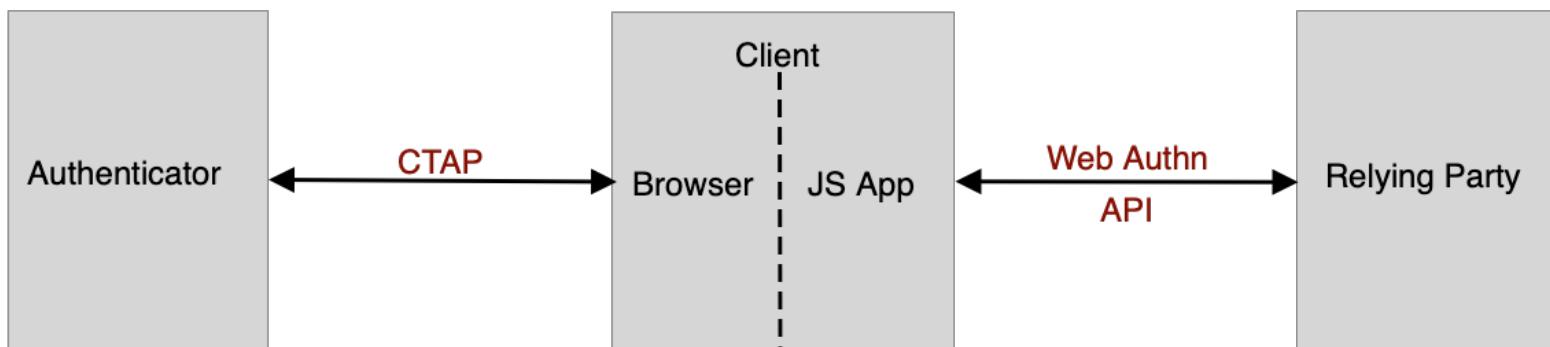
Web Authentication API

- > Allows **passwordless** registration, login und multi-factor authentication
- > Based on Public-Key Authentication
- > Part of FIDO2 (CTAP & Web Authentication API); specified as a standard by the W3C
- > Backwards compatible to U2F

U2F



FIDO2



- > Fast IDentity Online (FIDO)
- > Founded in 2013
- > Members (et al.)
 - > PayPal, Google, Microsoft, Mastercard, VISA, Samsung, BSI
- > Specifications of UAF, U2F, CTAP, and the first draft of the Web Authentication API as FIDO 2.0

Web Authentication API

- > Authenticator can either be internal (built-in) or external (via USB, Bluetooth, or NFC)
- > Supported by Chrome, Edge, Firefox, Safari, Chrome & Firefox für Android

- > No support of the API by the Internet Explorer; problematic for the enterprise sector
- > Many Android web browsers do not support the API
- > No support of iOS Safari, only third-party app “Brave Browser” supports the API

Security Aspects



Security Aspects and Usability

> No known successful attacks

- > Formally verified
- > Security problems are only on a protocol level
 - > Missing requirement of a secure random number generator
 - > Support of RSASSA PKCS#1 v1.5 (=> Bleichenbacher's attack)
 - > No point compression on the elliptic curve required
 - > “Weak” choice of elliptic curves (Barreto-Naehring) with reduced amount of bits for security
- > No possibility to backup or export the key material
 - > Each account should be associated with at least two different authenticators

Comparison to Other MFA solutions

- > Evolution of the U2F protocol, authentication by possession threats apply, too
 - > Due to the specification by the W3C the browser support is increases
- > In comparison to, e.g., TOTP some browsers and operating systems are missing support and interoperability
- > WebAuthn is resistant against phishing, many other MFA solutions are not
- > WebAuthn has no backup functionality
- > No solution provides a protection for, e.g., session hijacking

Conclusion

15

Conclusion

Generally

- > Sensitization of the users about the dangers
- > Increase awareness for a secure handling of credentials

Existing MFA solutions

- > MFA can increase the security, but is often not resistant against phishing
- > SMS traffic can be eavesdropped
- > Problems with password still remain

Web Authentication API

- > Can replace passwords with public-key authentication
- > Allows registration, login, and MFA with the help of public-key authentication
- > Currently not supported enough, especially in mobile operating systems and web browsers
- > Few websites have implemented the API

Sources

1. Christian Friemel. Trotz „Collection #1-5“: Beim Passwortschutz lernen deutsche Internet-Nutzer nur langsam dazu. Mar. 27, 2019. URL: <https://newsroom.web.de/2019/03/27/trotz-collection-1-5-beim-passwortschutz-lernen-deutsche-internet-nutzer-nur-langsam-dazu> (last accessed on 11/03/2019).
2. Olabode Anise and Kyle Lady. State of the Auth: Experiences and Perceptions of Multi-Factor Authentication. Nov. 7, 2019: URL: <https://duo.com/blog/state-of-the-auth-experiences-and-perceptions-of-multi-factor-authentication> (last accessed on 11/03/2019).
3. Kurt Thomas et al. “Protecting accounts from credential stuffing with password breach alerting.” In: 28th USENIX Security Symposium. USENIX Security ’19. Santa Clara, CA, USA: USENIX Association, Aug. 2019, pp. 1556–1571. ISBN: 978-1-939133-06-9.
4. Dirk Balfanz et al. Web Authentication: An API for accessing Public Key Credentials Level 1. Mar. 4, 2019. URL: <https://www.w3.org/TR/2019/REC-webauthn-1-20190304> (last accessed on 11/03/2019).