Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

/DAS
Data and Application Security Group

Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication

Johannes Kunke, Stephan Wiefling*, Markus Ullmann#, Luigi Lo Iacono

H-BRS University of Applied Sciences

*Ruhr University Bochum

Bundesamt für Sicherheit in der Informationstechnik

The problem

- **Passwords still really relevant in Web**
  - **Also threats to passwords**
    - **Phishing → obtaining login credentials with fake emails or websites**
    - **Credential stuffing → automated injection of breached login credentials to gain access to user accounts**
  - **Increased due to COVID-19 pandemic and Home-Offices in March 2020**

The problem

- **FIDO two-factor Authentication**
- **FIDO2 passwordless Authentication**
- **Lyastani et al.* mentioned that users are more afraid to lose access rather than get hacked**

* Lyastani et al. (2020): Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In: SP '20. IEEE.

The problem

- Account recovery very important for user acceptance
- No uniform procedure for account recovery
- FIDO-Whitepaper* recommends to register backup authenticator
  - But: High burden for users
    - Must be done for each web service
    - Must be restored for each web service

* Gomi et al. (2019): Recommended Account Recovery Practices for FIDO Relying Parties

Agenda

- **What we did**
- **What we found**
- **Results**
- **Conclusion**

What we did

- **Heuristic evaluation of 12 account recovery mechanisms**
- **Criteria orientated on frequently cited heuristics**
  - **Bonneau et al.** (2012): The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: SP ’12. IEEE.
  - **Nielsen** (1994) Enhancing the explanatory power of usability heuristics. In: CHI ’94. ACM.
  - **Saltzer and Schröder** (1975): The protection of information in computer systems. In: Proc. IEEE, 63(9).
  - **Stajano** (2011): Pico: No More Passwords! In: Security Protocols XIX. Springer.

What we did

- **Criteria divided into three categories**
  - **Usability benefits**
  - **Deployability benefits**
  - **Security benefits**

What we did

- **Set up criteria**
- **Collection of 12 mechanisms**
- **Evaluation of mechanisms**
- **Point out proposals for improvement of passwordless FIDO2 recovery mechanisms**

Mechanisms & criteria

		Security Questions	**Password**	**OTP**	Pico	**Delegated Account Recovery**	**FIDO2 Backup Token**	Identity Card	**Advanced Protection Program**	Let's Authenticate	Key Copy	Online Recovery Storage	Pre-emptive Syncing
Usability	Memorywise-Effortless	○	○	●	●	○	●	●	●	○	●	●	●
	Scalable-for-User	○	○	●	●	○	○	○	○	●	●	●	●
	Nothing-to-Carry	●	●	○	○	○	○	○	○	●	○	○	○
	Physically-Effortless	●	●	○	●	○	●	●	○	●	●	●	●
	Easy-to-Learn	●	●	●	○	○	●	○	●	●	●	●	●
Deployability	Match System-Real World	●	●	○	○	●	●	●	○	●	●	○	○
	Accessible	●	●	○	●	○	●	●	○	●	●	●	●
	Negligible-Cost-per-User	●	●	○	○	○	○	●	○	●	○	○	○
	Browser-Compatible	●	●	●	○	○	●	○	●	○	●	○	○
	Non-Proprietary	●	●	●	●	●	●	○	○	●	●	●	●
	Implemented	●	●	●	○	●	●	●	●	○	○	○	○
Security	Resilent-Physical-Observation	○	○	●	●	○	●	●	●	○	●	●	●
	Resilent-Targeted-Impersonation	○	●	○	●	○	●	●	○	●	●	●	●
	Resilent-Internal-Observation	○	○	○	●	○	●	●	○	○	●	●	●
	Resilent-Leaks-from-Other-Verifiers	○	○	●	●	○	●	●	○	●	●	●	●
	Resilent-Phishing	○	○	○	●	○	●	●	○	○	●	●	●
	Resilent-Theft	●	●	○	○	○	○	●	○	●	○	○	○
	No-Trusted-Third-Party	●	●	○	●	○	●	○	●	○	○	○	●
	Requiring-Explicit-Consent	●	●	●	○	●	●	●	○	●	○	○	○
	Unlinkable	○	●	○	●	○	●	○	○	●	●	●	●
	Open	●	●	●	●	○	●	●	○	●	●	●	●
	Work-Factor	○	○	●	●	○	●	●	○	●	●	●	●
	Complete-Mediation	●	●	●	●	●	●	●	○	●	●	●	●

● Criteria fulfilled ○ Criteria not fulfilled **Bold**: Deployed in account recovery practice

Johannes Kunke, Stephan Wiefling, Markus Ullmann, Luigi Lo Iacono

What we found

- **12 mechanisms**
  - **Security questions**
  - **Backup password**
  - **One-Time Password**
  - **Pico**
  - **Delegated Account Recovery**
  - **FIDO2 Backup Token**

What we found

- **12 mechanisms**
  - **Identity Card**
  - **Advanced Protection Program**
  - **Let‘s Authenticate**
  - **Key Copy**
  - **Online Recovery Storage**
  - **Pre-emptive Syncing**

Results

- **Security questions unsuitable as recovery mechanisms**
- **Backup-Password also unsuitable**
- **PICO**
  - **No detailed description of how docking station works with backup**

Results

- **Delegated Account Recovery Protocol allows traceability**
  - **Worst overall rating (18/23 failed)**
- **Google advanced Protection**
  - **Similar to Facebooks mechanism (17/23 failed)**

Results

- **Backup-Token achieves best rating (4/23 failed)**
  - **However not Negligible-Cost-per-User**
    - **Serious criterion**
- **nPA/eID meets this criterion**
  - **However not Easy-to-Learn and Unlinkable**

Results

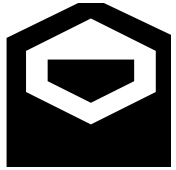
- **Let‘s Authenticate is ultimately based on passwords again**
- **Key Copy intuitive**
  - **Must be kept always up to date**
- **ORS and Pre-emptive Syncing best compromise (7/23 failed)**
  - **Just theoretical concepts**
  - **One-time initialization necessary**

Conclusion

- Concepts of pre-emptive syncing should be further investigated
  - To address problem of memory and computational load
- FIDO Alliance take up the proposal to adopt the Transfer Access Protocol in its standards
  - FIDO Alliance could eliminate the problem of inadequate access recovery

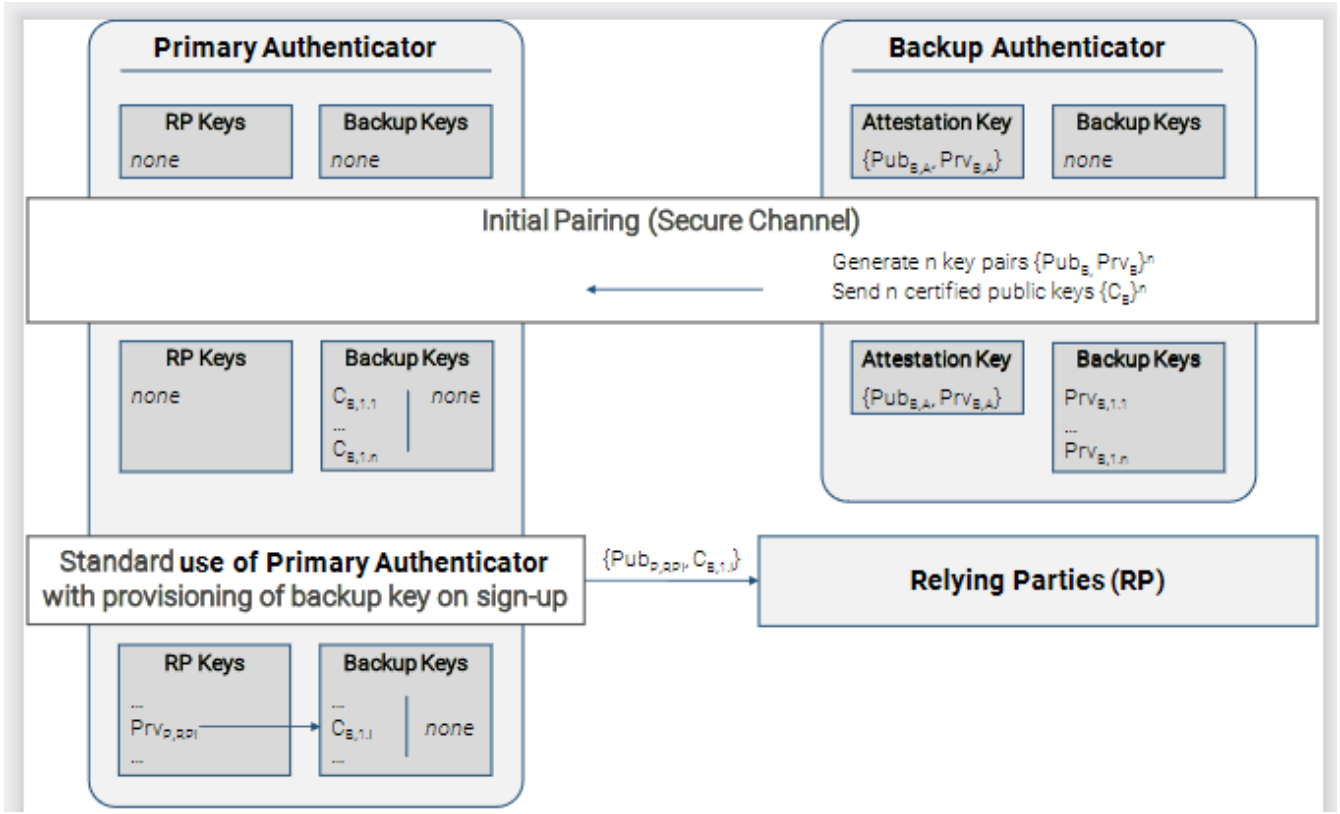
Thank you

das.h-brs.de



johannes.kunke@smail.inf.h-brs.de

Pre-emptive syncing 1



Pre-emptive syncing 2