

Towards Secure and Usable Authentication for Augmented and Virtual Reality Head-Mounted Displays

Reyhan Düzgün, Peter Mayer, Sanchari Das, Melanie Volkamer

COMPETENCE CENTER FOR APPLIED SECURITY TECHNOLOGY (KASTEL)
RESEARCH GROUP SECURITY · USABILITY · SOCIETY (SECUSO)

SECURE AND PRIVACY RESEARCH IN NEW-AGE TECHNOLOGY (SPRINT) LAB
HUMAN AND TECHNICAL SECURITY (HATS) LAB

Rise of Augmented & Virtual Reality (AR & VR)



Growing market with projections to reach \$114 billion in AR and \$65 billion in VR in 2021



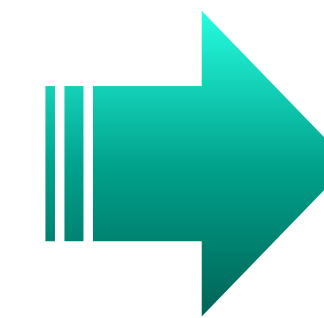
Increasingly provide social activities which require authentication

Virtual
Gaming

Virtual
Shopping

Navigation
Support

Virtual
Meetings



Use of AR/VR Head-Mounted Displays (HMD) in shared and public places

Challenges in Authentication with AR & VR HMDs

Nowadays authentication on HMDs is usually conducted on another device, e.g. smartphone/PC



- ⚡ Interrupts AR/VR experience
- ⚡ Not conform with the goal of using HMDs as independent units

Alternative 1: Adapting typical concepts for smartphone/PC like password or PIN with e.g. a virtual keyboard



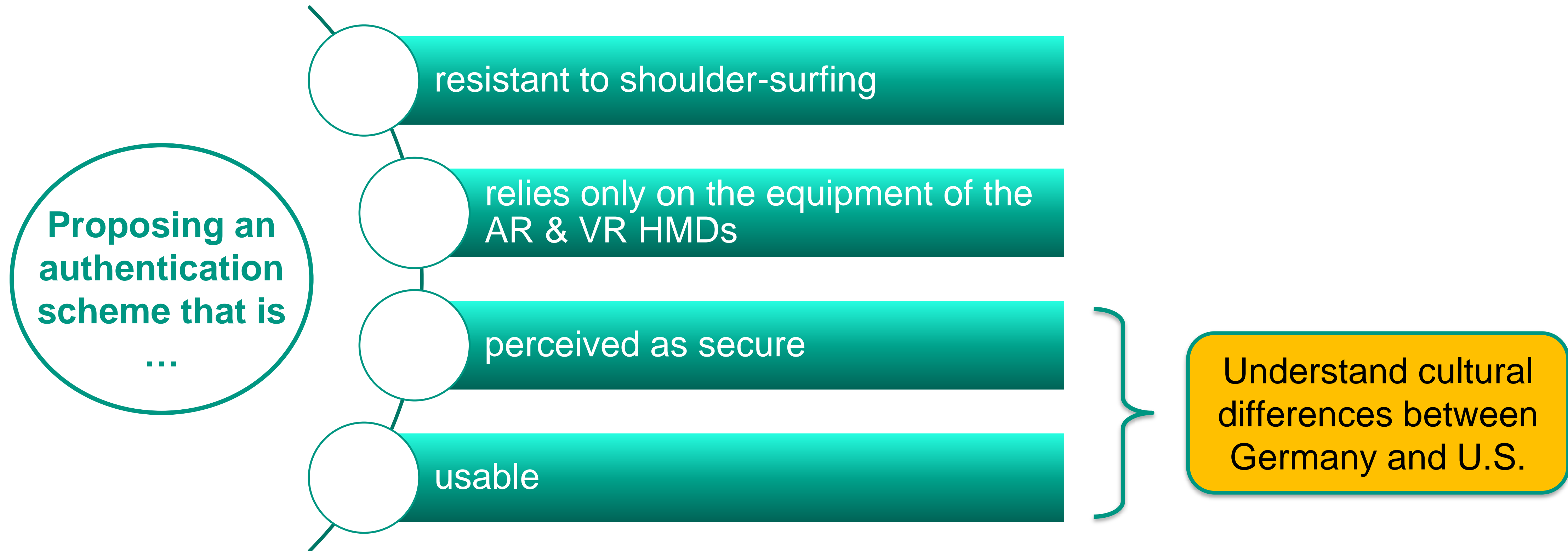
- ⚡ Not usable
- ⚡ Not resistant to shoulder-surfing

Alternative 2: Biometric authentication



- ⚡ Is more for continuous authentication
- ⚡ Require additional hardware
- ⚡ Works just on own device

Research Goals



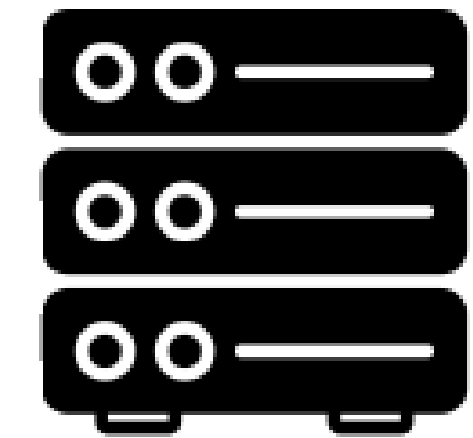
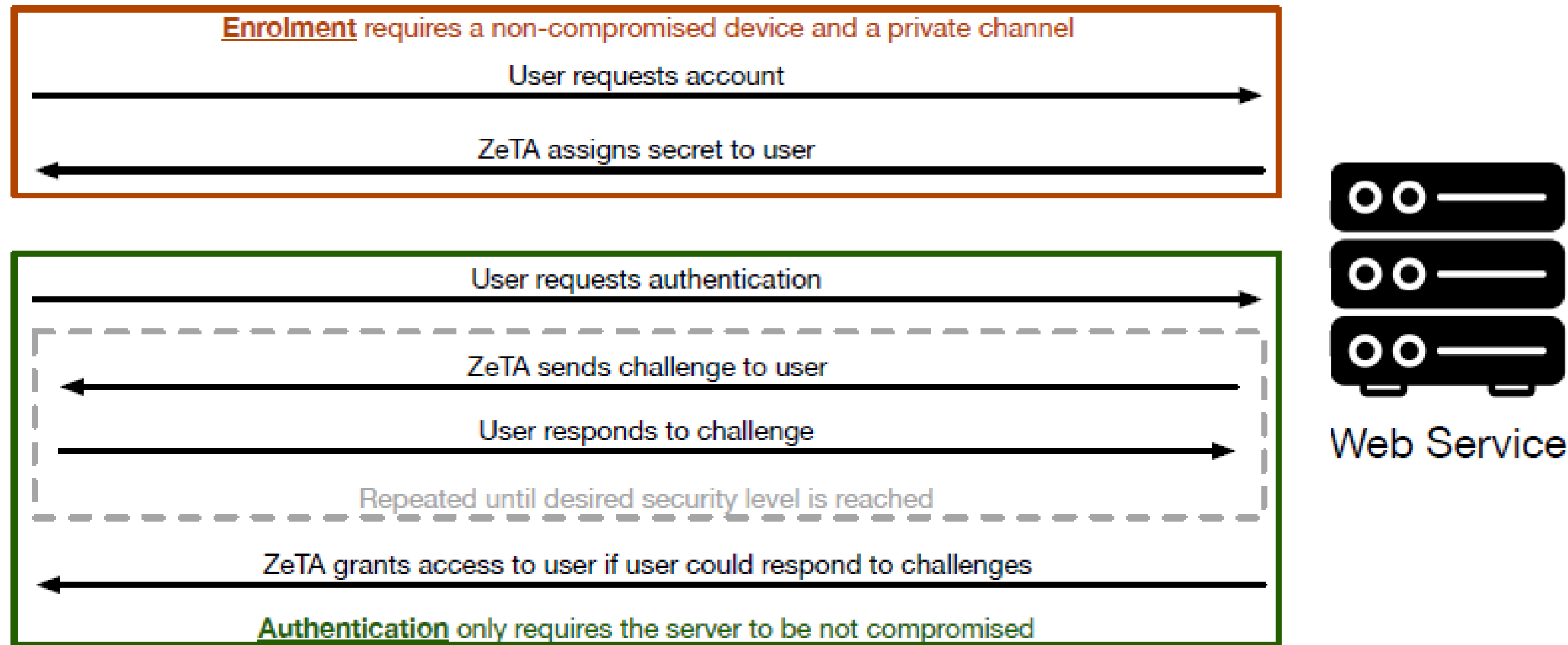
Our Proposal: Zero-Trust Authentication (ZeTA)



Authentication using innate human-based computation*



User



Web Service

Two or more concepts and their logical connection (AND, OR) building the secret (= password)

E.g.: “yellow OR forest”

Authentication by answering if a specific attribute is related or not

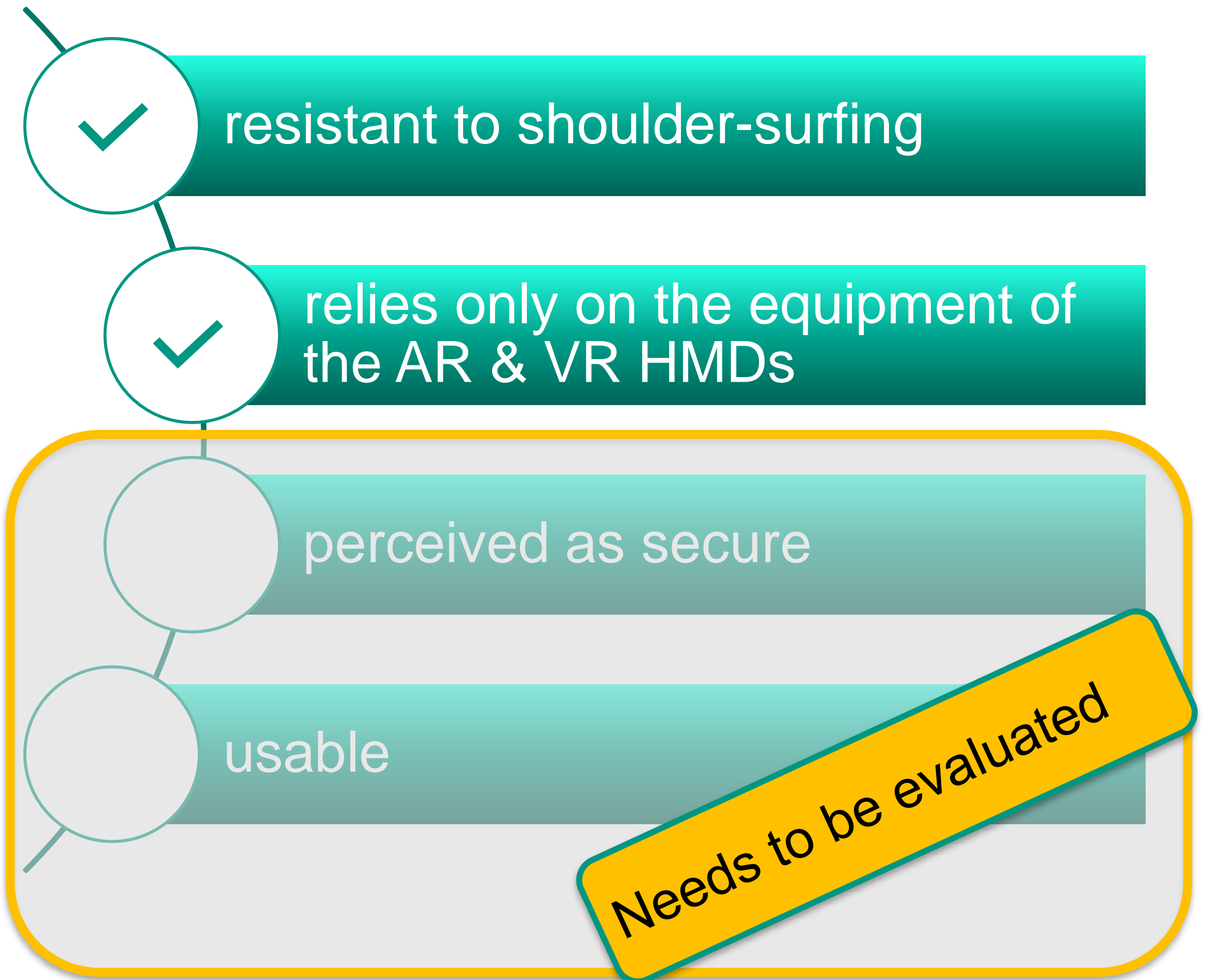
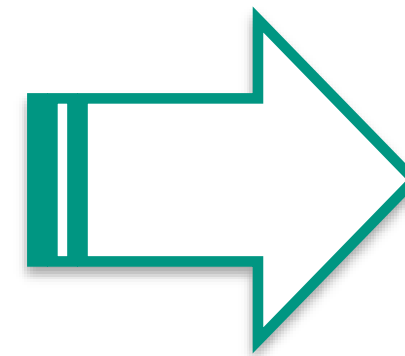
E.g.: „sunflower“ – Yes

*Gutmann, A., Renaud, K., Maguire, J., Mayer, P., Volkamer, M., Matsuura, K., & Müller-Quade, J.. (2016) ZeTA-Zero-Trust Authentication: Relying on Innate Human Ability, Not Technology. IEEE EuroS&P.

ZeTA Authentication on AR/VR HMD

HMDs use display as output and diverse input mechanisms

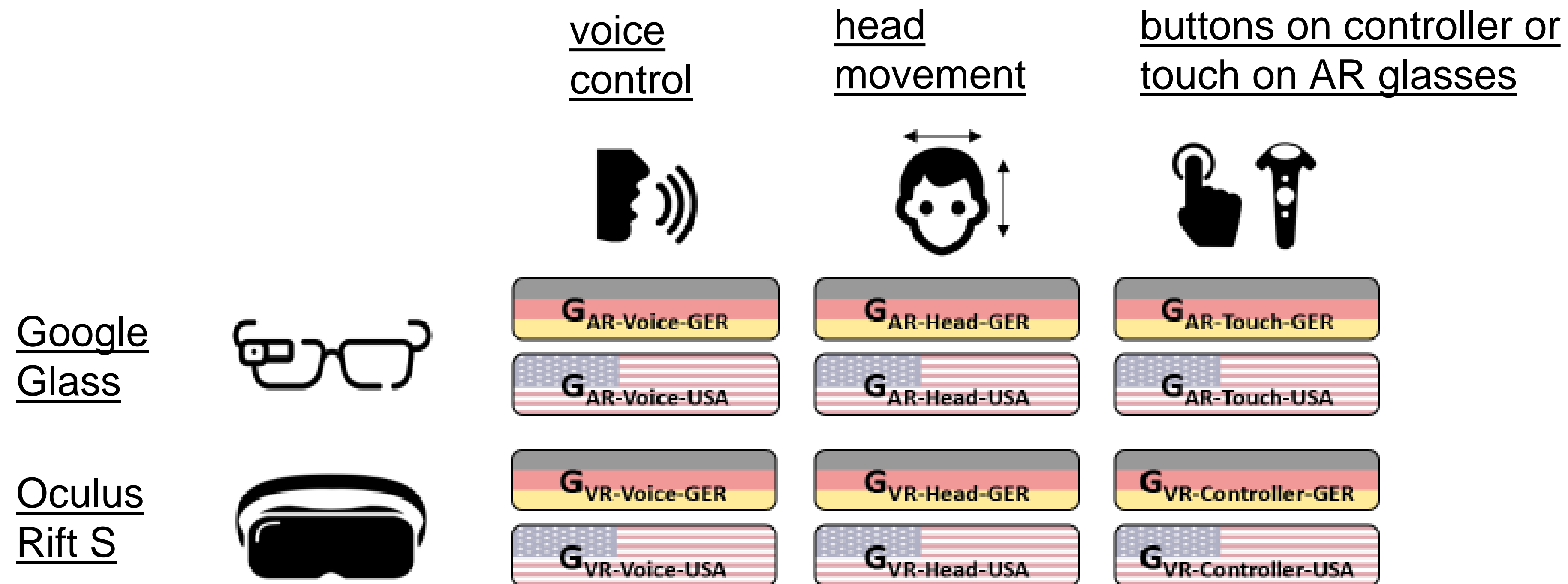
- Challenge is shown on the display
- User answer with Yes/No with given input systems




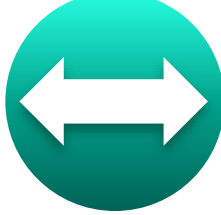

Development of ZeTA on AR/VR HMD

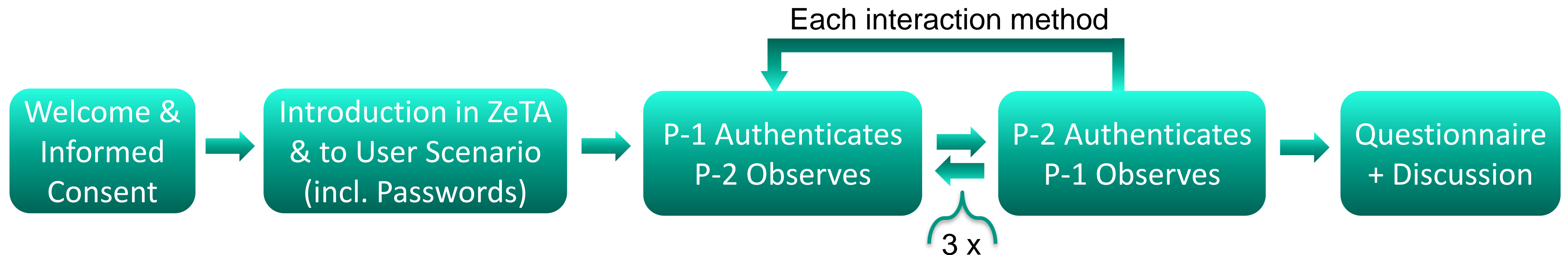


User-centered design approach: Iterative development of 12 mock-ups



Proposed Methodology for User Evaluation (1/2)

- 
 Evaluation of **usability** (i.e. effectiveness, efficacy and satisfaction) | **perceived risk** regarding its security
- 
 Within-subject design to compare interaction methods | Between-subject design to compare countries and devices
- 
 Two participants testing simultaneously, each authenticates with each interaction method 3 times with a different password



Proposed Methodology for User Evaluation (2/2)



Measurement of usability and user's risk perception

- Effectiveness: Ratio of correct password entries among three
- Efficacy: Average time needed for authentication across three passwords
- Satisfaction: System Usability Scale (SUS)
- User's risk perception: Scales by Fischhoff et al., Liang & Xue, and Das will be adapted to our use case

Conclusion

Currently authentication on HMDs is ...

- require additional hardware
- not resistant to observations

ZeTA is resistant to shoulder-surfing and does not require additional hardware.

Secret: “yellow OR forest”

Attr.: „sunflower“ – Yes

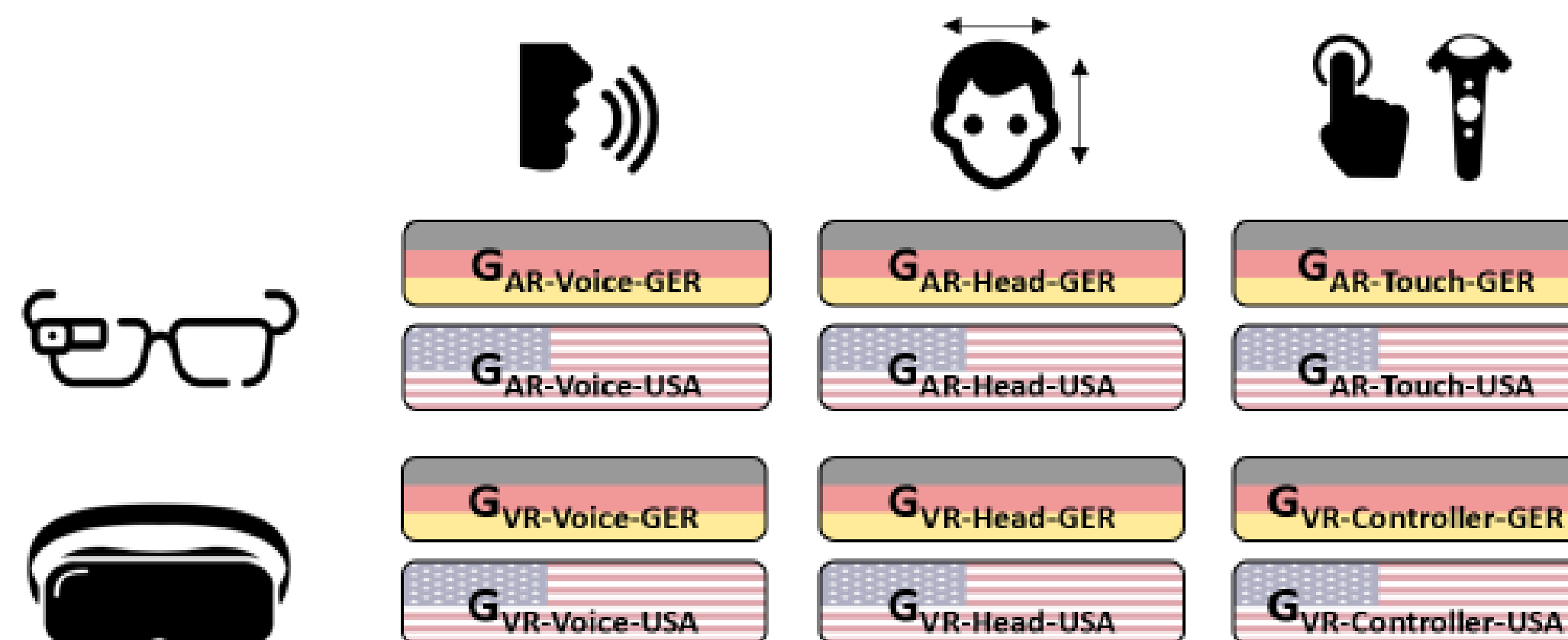
- not usable and perceived as secure

User studies are going to evaluate its usability and perceived risk regarding its security.

Thank You!



Feedback and contributions are welcome: reyhan.duezguen@kit.edu 😊



References

- Andreas Gutmann, Karen Renaud, Joseph Maguire, Peter Mayer, Melanie Volkamer, Kanta Matsuura, and Jörn Müller-Quade. Zeta-zero-trust authentication: Relying on innate human ability, not technology. In EuroS&P, pages 357–371. IEEE, 2016.
- Peter Mayer, Nina Gerber, Benjamin Reinheimer, Philipp Rack, Kristoffer Braun, and Melanie Volkamer. I (don't) see what you typed there! shoulder-surfing resistant password entry on gamepads. In CHI, pages 1–12, 2019.
- Huigang Liang, Yajiong Lucky Xue. Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the association for information systems, 11(7):1, 2010.
- Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol. Biometric gait authentication using accelerometer sensor. JCP, 1(7):51–59, 2006.
- Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. Vr pursuits: interaction in virtual reality using smooth pursuit eye movements. In AVI, pages 1–8, 2018.
- Das, Sanchari. A Risk-reduction-based Incentivization Model for Human-centered Multi-factor Authentication. Diss. Indiana University, 2020.
- Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits." Policy sciences 9.2 (1978): 127-152.