# Research Proposal

## VirSec - A Virtual Environment as Cost-Effective Test Bed for Usability and Security Evaluation of Authentication Schemes

Florian Mathis

January 2019

**Abstract**

Today, evaluations of authentication schemes have been limited in many ways. In particular, evaluating novel systems such as smart homes or autonomous cars, and also larger scale systems (e.g. ATMs) represent a challenge. Namely, the design and evaluation of authentication schemes is costly, time consuming and limited to conditions that can be physically replicated in the lab. The objective of this project is to enable and expand the possibilities for researchers to evaluate authentication schemes in a feasible, cost-effective and timesaving way. This proposal seeks to address the limitations of current methods for evaluating authentication schemes by presenting VirSec, a virtual environment that can be used as a cost-effective test bed for usability and security evaluations of authentication schemes.

# 1 Background Information

My bachelor thesis, titled *"The bird is the word: a usability evaluation of emojis inside text passwords"* was published in OzCHI 2017, and received an honorable mention award (top 5% submissions). This sparked my interest in Usable Privacy and Security research. Later, I studied the use of obfuscation to preserve privacy in lifelogging videos in the Advanced Topics in HCI course, and I designed a novel biometric authentication scheme for my Usable Privacy and Security course. My experience in designing novel authentication mechanisms, as well as developing and evaluating prototypes (both software- and hardware-driven), encouraged me to pursue this area further.

# 2 Related Work and Potential Research Questions

**Challenges of Evaluating Authentication Schemes**

Evaluation of human-centred novel authentication schemes typically takes place within lab or field studies. Previous research investigated the security and usability of authentication on traditional platforms (e.g., handheld devices, personal computers) [1,2,4,5,6,8,9]. This is often done by implementing a prototype and deploying it for actual use by participants. This becomes challenging when authentication is evaluated on large scale systems (e.g., ATMs, smart homes, autonomous cars, public displays), because prototyping these systems is time-consuming, costly, and it is often infeasible to create all the evaluation conditions in the lab. For example, consider a case where a researcher wants to evaluate observation attacks against authenticating at an ATM from 5 different angles; this would require placing 5 cameras at the required positions to record the authentication process at a real world ATM.

We propose VirSec, a system that uses virtual reality (VR) to allow researchers to create cost- and time-efficient high-fidelity prototypes to evaluate authentication schemes. In the same example above, evaluating a virtual replica of the system would 1) cut down costs as hardware solutions will no longer be required in the evaluation process, and 2) enable infinite options for observation angles from a single 3D recording. Previous work by George et al. [3] shows that the performance of authentication schemes in virtual reality is comparable to their performance in the real world. VirSec is inspired by this previous work which shows preliminary evidence that results acquired by evaluating authentication schemes in virtual environments match those collected in real world experiments.

This underlines the first research question of this project. **R1**: *Which and how well do results of evaluating authentication schemes in virtual reality match results acquired from similar experiments in the real world?* Our first step to tackle this research question is described under *Experiment 1* below.

## 2.1 Authentication in Virtual Reality (VR)

Few previous works already looked into transfering authentication systems that are well-established in the real world to virtual environments [3,10]. This was mainly motivated by the need for authentication in VR (e.g., to make purchases in VR), and because requiring users to take off the VR headset to authenticate would decrease the user's immersion and overall user experience.

**The Transfer of Well-Established Authentication Systems to Virtual Environments**
Many VR applications require authentication, such as virtual shopping, and micro transactions in VR games. George et al. [3] investigated the use of PINs and Android unlock patterns, which are common on today's mobile device, in VR. Their work was a proof-of-concept that schemes that are used for mobile devices are transferable to VR. Similarly, Yu et al. [10] implemented three password methods for VR, and found a trade-off between usability and security of password systems for VR and new upcoming challenges have to be tackled. Both works [3,10] show that virtual environments are promising for evaluating authentication schemes, and that show preliminary evidence that results acquired in VR match those acquired from similar studies in the real world. This suggests that using a virtual environment like VirSec to evaluate authentication schemes is a promising alternative to traditional methods that are costly, time-consuming and limited in various ways.

### 2.2 State of the Art Methods in Evaluating Authentication Schemes

To cover a huge set of different conditions in which users can authenticate, it is often necessary to tweak the experimental setup after every individual session. This is not only costly, it is also time consuming. Furthermore, post-hoc manipulations of recorded data is not possible without re-running the whole experiment. In a Wizard-of-Oz study by Mecke et al. [7], they investigated and explored authentication systems for doors. A similar design of the study could be developed within a virtual environment which would decrease a) the costs of building such a prototype and b) would allow post-hoc manipulations (e.g., adding other authentication mechanisms, changing environment conditions like lighting, alternating between different feedback mechanisms such as haptic or visual feedback) without having to invite participants for an additional session. Similar to that, the use of VirSec would not only allow researchers to avoid purchasing expensive equipment to record user sessions (e.g., like in [4,5] where multiple cameras were used to record gaze interaction for authentication), a modification of the setup (e.g. generating views from different angles for observation analysis) is straightforward in VR using Unity. A virtual environment system such as VirSec would also decrease the necessity of multiple input devices. Whereas a work by von Zezschwitz et al. [9] used three different input devices (an iPhone, an iPad and a Desktop PC), VirSec would not require high-cost hardware devices and would thereby reduce development and evaluation costs.

In summary, I interpret the mentioned works as a promising direction for using virtual environments as test beds for designing, developing and evaluating novel authentication schemes. However, it is necessary to build VirSec in a modular way to allow different researchers to use it for different evaluation needs. This raises the second research question. **R2**: *What are the key challenges and requirements for VirSec to be versatile to different evaluation needs?* Our first step to tackle this research question is described under *Experiment 2* below.

## 3 Proposed First Year Research Plan

The first year will be used to execute a systematic literature review. This paves the way to get a broad and deep knowledge of existing experiments in the area of Usable Privacy and Security and resulting challenges which can be taken into consideration for designing VirSec. The first year also includes the establishment of a list of requirements and the fundamental set of guidelines which are derived from the systematic literature review, weekly meetings and collaborations with other Ph.D. students, developers, researchers, and through experiments. An initial set of experiments within the first year should indicate to what extent authentication schemes in virtual environments can be transferred to the real world.

**Experiment 1: Gaze and Touch Authentication in VR and the Real World**
I envision that the first experiment would involve 1) implementing an authentication scheme in the real world, then 2) implementing a replica in virtual reality, and 3) evaluating both and comparing the results. One possibility is to implement GazeTouchPass [4], an authentication scheme that uses gaze and touch input, and extending it by exploiting advances in front-facing cameras. We will then implement a replica of GazeTouchPass in VR using the HTC Vive headset for VR and the integrated Tobii eye tracker, which Dr. Mohamed Khamis has already procured for my project. We can then design a between-subjects experiment where one group uses the system in the real world, and the other group uses it in VR. We can similarly simulate observation attacks in both groups to collect data about resilience to shoulder surfing. The results from both experiments will be analyzed in terms of usability (authentication time, authentication errors, memorability, and mental demand), as well as security (resistance to shoulder surfing attacks). This novel experiment will help us unveil the differences and similarities between authentication in VR and in the real world, and will help us draw insights about which evaluation aspects can be expected to match in both environments. Thus this contributes to Research Question 1.

**Experiment 2: Understanding the needs of Usable Security researchers and practitioners**
Another project to conduct in parallel is understand the needs and requirements of researchers and practitioners who evaluate authentication schemes. This will be done through a literature review and also qualitative methods such as surveys and interviews. This will contribute to Research Question 2.

# 4 Research Significance

Using VirSec as a test bed for usability and security evaluation of authentication schemes contributes to: 1) **Reducing costs of designing and evaluating novel authentication schemes:** Building expensive testing environments within VirSec as a low cost high-fidelity prototype (e.g., smart homes, ATMs, credit card payments in supermarkets); 2) **Enabling the possibility to replicate experiments without time consuming re-building of the whole scenarios** and 3) **Expanding scenarios researchers can evaluate**: Participants are often invited to execute an authentication process multiple times with different conditions (e.g, a simulated attack from a camera positioned at different locations). Therefore it is necessary to manipulate the test environment manually. VirSec will allow post-hoc manipulation of the recorded 3D scenes by automatically generating multiple views from different angles, and simulate the conditions (e.g. lighting) that researchers want to examine. VirSec provides a simulation of the real world in authentication scenarios and creates scenarios which are not feasible to replicate in the lab and thus, has the potential to create an **unprecedented infrastructure for human-centred security research**.

The goal of this research project is to understand to which extent the resulting insights of the experiments within a virtual environment (VirSec) can be transferred to the real world. Through a series of user studies, the outcome of this project will be 1) a modular VR system, VirSec, to provide a central hub for evaluation of authentication schemes, and 2) a set of guidelines which ensure that resulting insights in VirSec will match those in the real world. Thus, VirSec has the potential to change the way security and privacy protection is evaluated.

## References


**[1]** Agarwal, M., et al. "Secure authentication using dynamic virtual keyboard layout." Proceedings of the International Conference & Workshop on Emerging Trends in Technology. ACM, 2011. https://doi.org/10.1145/1980022.1980087

**[2]** De Luca, Alexander, et al. "Now you see me, now you don't: protecting smartphone authentication from shoulder surfers." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2014). ACM, 2014. https://doi.org/10.1145/2556288.2557097

**[3]** George, Ceenu, et al. "Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality." NDSS, 2017.http://dx.doi.org/10.14722/usec.2017.23028

**[4]** Khamis, Mohamed et al. “GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices.” in Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA 2016). ACM, 2016 https://doi.org/10.1145/2851581.2892314

**[5]** Khamis, Mohamed, et al. "GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication." Proceedings of the 19th ACM International Conference on Multimodal Interaction (ICMI 2017). ACM, 2017. https://doi.org/10.1145/3136755.3136809

**[6]** Khamis, Mohamed, et al. "GTmoPass: two-factor authentication on public displays using gaze-touch passwords and personal mobile devices." Proceedings of the 6th ACM International Symposium on Pervasive Displays (PerDis 2017). ACM, 2017. https://doi.org/10.1145/3078810.3078815

**[7]** Mecke, Lukas, et al. "Open Sesame!: User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors." Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (MUM 2018). ACM, 2018. https://doi.org/10.1145/3282894.3282923

**[8]** Von Zezschwitz, Emanuel, Paul Dunphy, and Alexander De Luca. "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices." Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI 2013). ACM, 2013. https://doi.org/10.1145/2493190.2493231

**[9]** Von Zezschwitz, Emanuel, Alexander De Luca, and Heinrich Hussmann. "Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance." Proceedings of the 8th nordic conference on human-computer interaction: fun, fast, foundational (NordiCHI 2014). ACM, 2014. https://doi.org/10.1145/2639189.2639218

**[10]** Yu, Zhen, et al. "An exploration of usable authentication mechanisms for virtual reality systems." Circuits and Systems (APCCAS), 2016 IEEE Asia Pacific Conference on. IEEE, 2016. https://doi.org/10.1109/APCCAS.2016.7804002