Fingerprint forgery training: Easy to learn, hard to perform

Agata Kruzikova
kruzikova@mail.muni.cz
Faculty of Informatics, Masaryk University
Brno, Czech Republic

Vashek Matyas
matyas@fi.muni.cz
Faculty of Informatics, Masaryk University
Brno, Czech Republic

ABSTRACT

Many services offer fingerprint authentication, including sensitive services such as mobile banking. This broad adoption could make an impression to the end-users that fingerprint authentication is secure. However, fingerprint authentication is vulnerable to various attacks performed even by not-very-sophisticated attackers, e.g., fingerprint forgery. Will participants perceive fingerprint authentication differently after relevant theory education and the creation of their fingerprint counterfeit to overcome misunderstandings, especially regarding security? How will they perceive the fingerprint forgery process? We prepared a hands-on seminar with fingerprint forgery simulation. We focused on the difference in perception before and after the theoretical lecture on biometrics and a practical seminar on forgery creation. We applied an uncommon approach, reconstructing the fingerprint from a photo of the actual finger rather than its print on some surface – to illustrate the case of an attack based merely on a "thumb-up" photograph. Our results show that 19% of participants (out of 221) were successful in spoofing, according to the NIST Biometric Image Software, and 27% of participants could register their counterfeit into the smartphone. Participants perceived fingerprint authentication as less secure after the simulation and reported their intention to use it less for mobile banking operations. They also perceived the forgery attack as easier to learn than before the simulation – but harder to perform. Our study implies that participants intend to change their behaviour based on their experience from our seminar, however, they did not consider two-factor authentication as an option.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**;

KEYWORDS

fingerprint forgery, spoofing, IT security, authentication, usable security

ACM Reference Format:
Agata Kruzikova and Vashek Matyas. 2023. Fingerprint forgery training: Easy to learn, hard to perform. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3600160.3604990

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3604990

1 INTRODUCTION

Fingerprint authentication deployment has been rising over the past two decades. Biometrics are used, e.g., for unlocking smartphones and even for more sensitive services, e.g., mobile banking. However, biometrics are not secret; when leaked, it is impossible to change them as in the case of a password or hardware token. As shown by previous studies (e.g., [13]), users perceive biometrics not only as usable but also as secure—their perception of risks related to biometrics usually does not reflect reality. Unfortunately, these incorrect mental models also apply to computer science students [10], representing future IT professionals. Several studies show that it is possible to fool fingerprint authentication in multiple ways (e.g., [8], [4]).

Even though IT professionals often have a practical experience with fingerprint authentication, it does not imply that their understanding is more accurate than the regular population since they usually do not have any education specifically in biometrics. We prepared a practical seminar about fingerprint forgery to explore if a better understanding of biometrics will change the perception and authentication behaviour. We chose fingerprints because they are the most used biometrics [21]. During the seminar, participants learnt about the theoretical background behind biometrics, especially fingerprints, and they also created a counterfeit from a photo of their finger. Our research questions are: Will participants perceive fingerprint authentication differently after relevant theory education and the creation of fingerprint counterfeit to overcome misunderstandings, especially regarding security? How do they perceive the fingerprint forgery process? This simulation aimed to give participants a better understanding of fingerprint authentication so they could make informed choices.

The main contributions of our work are:

- Using a photo of the fingertip to illustrate the case of an attack based merely on a "thumb-up" photograph, where no physical proximity is needed.
- Examining the influence of user experience with reconstructing a fingerprint from a photo of the actual finger to changes of user's security perception.
- Demonstrating the spoofing simplicity/difficulty by a larger group of inexperienced impostors.

In the next section (2), related work, including fingerprint authentication perception and methods of fingerprint forgery, is described. Section 3 is about methodology and consists of a description of the course description, measures, the overall setup and counterfeit creation. Results are described in Section 4. Section 5 contains a discussion of the results and lessons learned.

2 RELATED WORK

2.1 Fingerprint security perception

Regarding security, even though security experts use biometric authentication, they are sceptical about its usage for sensitive operations [17], [24]. Concerning regular end users, Habibu et al. [9] found that users believe that using biometrics for authentication provides the same level of security as two-factor authentication. Buckley and Nurse [1] state that fingerprint is perceived as the most secure biometric. Slightly more than half of their participants also believed compromising biometrics is easy. Since users are now exposed to biometrics, their perceptions could differ. Mitra and Barlow [18] also show that usage of biometrics on smartphones can be associated with a higher risk perception and security concerns than when using traditional methods for banking and health apps.

A recent study on the general Android smartphone population [13] showed that users perceived fingerprint authentication as the most usable and secure method compared with PIN and token-based methods. High-security perception of fingerprints can also apply to the IT-savvy participants (44% of computer science students), as shown by [10]. Also, in another study about smartphone authentication mechanisms with the iPhone population, "more than 50% of participants stated that security provided by Touch ID was one of the reasons to use it" [7]. Misconceptions about fingerprint authentication include e.g. misunderstanding where the fingerprint is stored and shared with different apps (e.g., [12], [14]). Misunderstanding of fingerprint implementation and usability importance can apply to general users as well as IT professionals [24].

2.2 Fingerprint forgery

Fingerprint authentication is vulnerable to spoofing. One of the most basic ones is to create a fingerprint as a cast of the finger. This could be done with or without the full cooperation of the victim as shown by [3]. The cooperative approach of spoofing was already used for educational purposes, as shown by Burton et al. [2]. They described how to conduct smartphone fingerprint spoofing as an activity for children. The victims had to imprint their fingers into the prepared drop of glue. This glue mould was then filled with another glue. The result was used for attacking smartphones. However, Burton et al. [2] only described the process; they did not conduct any research. Also, spoofing can be perceived entirely differently when considering a scenario when victims fully cooperate in comparison without such cooperation or even knowledge in the creation of the counterfeits. An example is creating a counterfeit from a photo of latent fingerprints from the smartphone screen.

Goicoechea-Telleria et al. [8] showed that it is possible to fool smartphones with counterfeit created from photos of latent fingerprints on the smartphone screen. Casula et al. [5] have shown that it is possible to create a counterfeit from a photo of a latent fingerprint on a smartphone screen. They also found that such counterfeits can be a real threat. Their follow-up study [4] focused on recovering a fingerprint from a smartphone screen photo in more realistic conditions. In their first study, participants were instructed to place their fingers on the cleaned screen (so it was a cooperative approach). In the follow-up study, the smartphone screen was not prepared in advance (so it included smudges and dirtiness), which affected the quality of the counterfeit resulting in the ineffectiveness of this attack (as an example of a non-cooperative approach).

Ogane and Echizen [19] considered spoofing based on the photo of an actual finger rather than its print on some surface [6]. However, their main focus was developing a technique to prevent getting fingerprint data from a photograph – they mostly focused on their solution BiometricJammer. They also did not create physical counterfeits; they just compared processed photos with scans of genuine fingers via fingerprint readers. In real-life scenarios, this approach can be categorized neither as cooperative nor non-cooperative. It contains some cooperative elements as victims voluntarily take a photo of their fingers and then publish them, e.g., on social networks. However, the victims publish their photos without knowing they will be misused for fingerprint spoofing. When an impostor finds the photo online, the spoofing is done non-cooperatively.

We decided to use this approach – to reconstruct a fingerprint from a photo of the actual finger. Similarly to the [19], our approach cannot be described as cooperative or non-cooperative.

3 METHODOLOGY

3.1 Course description

Our biometric seminar was part of an introductory IT security course for computer science students, regardless of their specialisation. Students usually complete this course in the fourth semester of their bachelor's study. This course consists of pre-recorded lectures[1], in-person summary lectures with Q&A sessions, and hands-on weekly seminars. Before the biometrics seminar (taught in the middle of the semester), students were taught about privacy and the basics of cryptography. They also experienced a seminar covering password cracking.

3.2 Procedure

Our participants should start by watching a pre-recorded lecture about identity and access management, including passwords, tokens and biometrics in general, fingerprints and face recognition. Then participants visited the hands-on seminars focusing only on introduction to biometrics and fingerprints. The seminar started by filling in the first questionnaire about smartphone authentication practices and perception (further referred to as "before"). After the first questionnaire, 15 minutes of theory was provided by teacher assistants in seminar groups (around 16 participants per group). In the theory section, participants were briefly taught about biometrics in general, its criteria, error rates, and the principle of fingerprint processing. Then participants were instructed on how to create a replica of their finger—the simulation ended in the first seminar by putting glue on a printed inverted binarized fingerprint on transparent plastic foil. One week later, participants brought their replicas with them back to the seminar and processed them. They started by scanning them with an external fingerprint reader Futronic FS80H (used software: ftrScanApiEx_v4.2). Then they processed their scans with NIST Biometric Image Software (NBIS) packages to evaluate their quality[2] (as used, e.g., by [16])

[1] Due to COVID-related restrictions and class size.

[2] Evaluated from 1 to 5 using NIST Fingerprint Image Quality algorithm (NFIQ), where 1 represents the best quality.

and match scores[3] with their original fingerprints. They also tried to use and register their counterfeits on their smartphone[4]. After finishing this part, participants were asked to complete the second questionnaire about their smartphone authentication practices and perceptions and evaluate the forgery process (further referred to as "after"). Simmplified procedure is visualized in Figure 1. Data were collected in 2022 – the "before" part was collected from March 28 to April 1, and the "after" part was collected from April 4 to April 8.

Figure 1: Simplified schema of a procedure: After pre-recorded lecture, participants filled in the first questionnaire at the beginning of the Seminar 1, then created a counterfeit. When the counterfeit was dry, they continued at the Seminar 2 with the counterfeit processing. After that, they finished with the second questionnaire.

3.3 Counterfeit creation

The counterfeit was created from the photo of the fingertip. The process described below is visualized in Figure 2.

(1) Participants were instructed to take photos of their fingertips on the unstructured black background next to a coin with their smartphones. The coin served as a size estimator/reference object.
(2) Then, participants processed their photos with our prepared script that automatically detected the coin and the finger. The photo resulted in a black-white inverted mirrored picture.
(3) The black-white inverted picture was printed on plastic foil using a laser printer. The layer of ink on the foil creates a 3D form/mould to fabricate a cast (ink creates ridges and foil without ink creates valleys).
(4) Then white glue was applied on the printed mould because the mould was 3D, also the glue will reflect the structure and it will result in the 3D replica.
(5) Once dry, the counterfeit was prepared for further processing.

Participants were expected to do the whole process by themselves during the simulation (e.g., the glue was not applied by seminar tutors but by participants, so we achieved the most realistic scenario and the same conditions for all participants).

3.4 Research hypotheses

We want to know whether participants would perceive fingerprint authentication differently after relevant theory education and practical experience with the creation of fingerprint counterfeit. Putting

[3]We used NIST Bozorth3 algorithm for fingerprint matching.
[4]When participants did not have a fingerprint reader on their smartphone, a smartphone with a fingerprint reader was provided to them by seminar tutors (Huawei P Smart).

Figure 2: Steps of counterfeit creation: (1) photo of a fingertip, (2a) photo processing, (2b) result of photo processing, (3) printing mould on the foil, (4) applying of a glue on mould, (5) dry counterfeit.

fingerprint authentication into the context of smartphone authentication methods, evaluating its perceived security and several other smartphone authentication methods are needed. We hypothesize that participants would perceive fingerprint authentication differently than other authentication methods relevant to smartphones regarding security (*H1*). Since our seminars focus on fingerprint forgery, we expect participants to perceive fingerprint authentication differently before and after the simulation (*H2*). The first seminar also consists of the theory, where other types of attacks on fingerprint authentication are mentioned altogether with error rates. We are interested in participants reconsidering how securely the general public and IT security experts perceive smartphone fingerprint authentication. We hypothesize that participants' beliefs about IT security experts' perception of fingerprint authentication would differ before and after the simulation (*H3a*). Fingerprint authentication would be perceived differently by the general public and IT security experts (*H3b*).

According to the security-usability threat model, "perceived susceptibility to attacks" is a measurable metric for the security evaluation of a system [11]. Since we focus on attack, we expect differences in susceptibility perception before and after the simulation (*H4*).

Since fingerprint forgery is only one type of fingerprint attack, it is beneficial to know how participants perceive it in the context of fingerprint-related attacks. We expect fingerprint forgery attacks to be perceived differently in terms of (a) easiness to learn (*H5a*), (b) easiness to perform and in (*H5b*) (c) the expertise of an attacker needed to perform the fingerprint forgery attack vs the general attacks related to fingerprints (*H5c*).

We anticipate participants' expectations about fingerprint forgery attacks' learnability and performance difficulties to differ after the direct experience. Also, assumptions about the attacker level (e.g., novice or expert) can differ after such an experience. We hypothesize that (a) the learnability (*H6a*), (b) difficulty of performing (*H6b*) of a fingerprint forgery attack would be perceived differently after the simulation than before. Also, the expertise of an attacker needed to perform the fingerprint forgery attack successfully would be perceived differently after the forgery simulation than before (*H6c*).

We expect participants to perceive the fingerprint forgery process differently based on their achievements. We hypothesize that satisfaction with the counterfeit would differ between participants who successfully authenticated with their counterfeit and unsuccessful participants (*H7a*). We also expect they would evaluate the time (*H7b*) and effort (*H7c*) to create a counterfeit as different from unsuccessful participants.

This experience aimed to give participants a better understanding of fingerprint authentication so they could make informed choices. We are interested in participants feeling more confident deciding about fingerprint authentication usage since knowledge is a factor of security [11]. We expect participants' knowledge about fingerprint authentication to be perceived differently after the simulation (*H8*).

Even though immediately after simulation participants could not change their behaviour, the intention is considered an indicator of behaviour [20]. Even IT security experts use fingerprint authentication but are reserved to use it for sensitive accounts [24]. We assume that our participants would adopt this behaviour. We hypothesize that participants would intend to use fingerprint authentication on smartphones differently after the simulation than before for the following purposes (a) unlocking a smartphone (*H9a*), (b) logging into mobile banking (*H9b*) and (c) confirmation of transactions in m-banking (*H9c*).

3.5 Measures

An online questionnaire was used to collect data. Some variables were measured before and after the simulation to evaluate the experience impact, and others were measured only once. Most items were measured on a 5-point Likert scale if not stated otherwise. Items for risks and prevention are open-ended. For further details see Table 1 with selected questions. Items with numeric answers (e.g., age or the score given by NBIS software) are not presented.

Perceived susceptibility was measured with three items. The resulting perceived susceptibility score was computed as a mean value of these three items (before simulation: M = 2.85, SD = 0.72, Mdn = 3, Cronbach's alpha = 0.62 / after simulation: M = 2.53, SD = 0.79, Mdn = 2.67, Cronbach's alpha = 0.72).

3.6 Pilot testing

We tested our scenario in a pilot study with 19 students of a different course. These students had long-term computer security interests in contrast to our target group, so we mainly tested the procedure. Based on that testing, we excluded some questions from the questionnaire to make it reasonably short. We also improved instructions.

3.7 Ethics

Participants could participate in the research directly during the seminars. Participants were first approached for their informed consent with study participation. Participation in the research (filling in the questionnaires) was purely voluntary, and seminar tutors could not get the information if students participated in the research or not. Questions in the questionnaire have an option "I do not want to answer". Participants did not get any reward or disadvantage by participating in the research. The research team collected no photos or other data except self-reported data via questionnaires. The Institutional Review Board approved the study. To not cause any harm to anybody, participants were expected to create a forgery of their own fingers only.

4 RESULTS

4.1 Sample

Of the 295 students enrolled in the course, 257 decided to participate in the study. We excluded cases when participants completely skipped one of the questionnaires and cases with different conditions, e.g., the lab computers went down because of unexpected technical issues unrelated to the simulation. Our final sample resulted in 221 participants aged 19-26 (M = 21, SD = 1.04), 15% females, 83% males, 1% others (and 1% missing). 77% had a smartphone with Android and 23% with iOS. Most of them had access to a fingerprint reader: 95% have the reader on their current (81%) or past (13%) smartphone, and 49% on a device different than smartphone (43% on the laptop). 83% participants were using the fingerprint readers on any device at the time of data collection, 10% were former users and 3% only tried it but did not use it. Only 4% have no experience with a fingerprint reader. Participants perceived themselves mostly as advanced beginners in IT security (M = 2.19, SD = 0.87). 68% reported they watched the prerecorded biometric lecture before the seminar, 6% attended the in-person summary lecture with a Q&A section and 34% have some knowledge about biometrics regardless of the course. Only 15% of the participants reported not having any previous information about biometrics.

4.2 Data analysis

Data analysis was done with IBM SPSS 27. Due to the data distribution and outliers, we report corresponding non-parametric tests (Wilcoxon signed-rank for comparison before and after the seminar and the Man-Whitney test for comparing successful and unsuccessful groups). The significance is considered at 0.050 level.

4.2.1 Security perception. We used Friedman's ANOVA to find differences in methods' security perception (before: $\chi^2(6) = 401$, $p < 0.001$ / after $\chi^2(6) = 453$, $p < 0.001$). Results of the post-test for fingerprint (see Table 2) show that the observed differences between the fingerprint and the rest of the methods except a PIN are statistically significant (*H1 partially supported*). Methods were evaluated from the least secure to the most secure as follows: swipe pattern (Mdn = 3), face (Mdn = 3), PIN (Mdn = 3), fingerprint (before simulation Mdn = 4, after simulation Mdn = 3), software (SW) token (Mdn = 4), password (Mdn = 4) and hardware (HW) token (Mdn = 5). Fingerprint method was perceived as significantly less secure after the simulation (T = 1695, $p < 0.001$, r = -0.29, *H2 supported*).

We found differences in the expected IT security expert's perception of fingerprint authentication (T = 1793, $p < 0.001$, r = -0.27). Participants believed that after (Mdn = 2) the simulation, IT security experts perceived fingerprint authentication as less secure than before (Mdn = 3, *H3a supported*). General public (Mdn = 4) was expected to perceive a fingerprint as more secure than IT security experts before (T = 293, $p < 0.001$, r = -0.60) and after simulation (T = 54, $p < 0.001$, r = -0.62, *H3b supported*).

4.2.2 Perceived risks and prevention. Regarding perceived risks, most participants (N = 80) mentioned some form of falsification, and some also mentioned issues related to unconscious usage (e.g., during sleep, N = 22).

Regarding prevention, the technique mentioned most often was not to use a fingerprint (N = 17), followed by using it combined with

Table 1: Selected questionnaire items.

Group	Item(s)	Source
Security	How secure do you think these authentication methods on smartphones are?	[13]
	I think that fingerprint authentication for smartphones is considered secure by the general public/IT security experts.	
Risks	What risks are connected with fingerprint authentication according to you?[b]	
Prevention	Do you think that there is anything you can do to prevent risks related to fingerprint authentication?	
Susceptibility	I could be subject to a serious fingerprint attack on my smartphone.	[22]
	I feel that my smartphone could be vulnerable to a fingerprint attack.	[22]
	It is likely that my smartphone will be compromised via a fingerprint attack in the future.	[22]
Fingerprint Attacks	Do you consider the attacks related to fingerprint authentication as easy or hard to learn/perform?[b]	
Forgery Attacks	Do you consider fingerprint falsification attacks as easy or hard to learn/perform?	
Attacker Level	According to you, what kind of attacker is able to successfully perform the fingerprint falsification experiment?	
Knowledge	I have enough information about fingerprint authentication to be able to make an informed decision about what applications I will use it for.	
Behaviour	How often do you use fingerprint authentication on your smartphone for the following purposes? If you do not have a fingerprint reader on your smartphone, please imagine that you do.	
Satisfaction with a counterfeit	How are you overall satisfied with your fake fingerprint?[a]	[15]
Counterfeit perception	How do you evaluate an overall time/effort to create a fake fingerprint?[a]	

[a]Item included only in the questionnaire after the simulation in our seminar.
[b]Item included only in the questionnaire before the simulation in our seminar.

Table 2: Security perception of fingerprint in context to other methods: Values of T indicate how the mean rank of fingerprint security perception was higher (positive values – first 3 methods) or lower (negative values – last 3) than other methods. Fingerprint mean rank was 3.80 before and 3.47 after the seminar.

	Swipe pattern	Face	PIN	SW token	Password	HW token
Before	T = 1.27***, r = 0.29	T = 1.01***, r = 0.23	T = 0.49, r = 0.11	T = -0.97***, r = -0.23	T = -1.39***, r = -0.32	T = -1.82***, r = -0.42
After	T = 1.03***, r = 0.24	T = 0.73*, r = 0.17	T = 0.02, r = 0.01	T = -1.34***, r = -0.31	T = -1.91***, r = -0.44	T = -2.26***, r = -0.52

*p =< 0.05 ***p =< 0.001

another factor (such as two-factor authentication, N = 12) before the simulation. After the simulation, participants mentioned not using fingerprints (N = 16), not taking photos of them (N = 15), and two participants mentioned two-factor authentication.

4.2.3 Perceived susceptibility. Perceived susceptibility was significantly higher before (Mdn = 3) the simulation than after (Mdn = 2.67, T = 1944, $p < 0.001$, r = -0.35, *H4 supported*).

4.2.4 Forgery attack vs other fingerprint attacks. We found the fingerprint forgery attacks to be perceived as easier to learn (Mdn_{fogery} = 3, $Mdn_{general}$ = 3, T = 593, $p < 0.001$, r = -0.35) and perform (Mdn_{fogery} = 3, $Mdn_{general}$ = 3, T = 616, p = 0.012, r = -0.23) than the general fingerprint attacks (*H5a-b supported*). We did not find any significant differences in the level of an attacker concerning fingerprint forgery attack (Mdn = 3) and general fingerprint attack (Mdn = 3, T = 2235, p = 0.412, r = 0.06, *H5c not supported*).

4.2.5 Forgery attack perception. Fingerprint forgery attack was considered significantly harder to learn before (Mdn = 3) than after (Mdn = 2) the simulation (T = 1829, $p < 0.001$, r = -0.41, *H6a supported*) and significantly easier to perform before (Mdn = 3) than after (Mdn = 4) the simulation (T = 4607, p = .022, r = 0.15, *H6b supported*). Also, the level of the attacker was considered significantly higher before (Mdn = 3) than after (Mdn = 3) the simulation (T = 2311, $p < 0.001$, r = -0.27, *H6c supported*).

4.2.6 Spoofing experience. Participants could succeed with the spoofing when achieving a true match in NBIS software and/or logging into their smartphone. 19% of participants (N = 41) were successful in spoofing according to the NBIS system (a score above 40 is considered a true match [23]), and 26% (N = 57) participants were able to register the counterfeit into the smartphone. For the following comparison, participants with scores above 40 in NBIS and successful counterfeit registration into the smartphone are further referred to as the successful group (resulting in N=89, 41%, because N=9, 4% of participants were successful in both situations).

4.2.7 Counterfeit quality and perception. The unsuccessful group (Mdn = 1) had significantly lower counterfeit quality than the successful group (Mdn = 1, U = 4920, p = 0.019, r = -0.16). Regarding satisfaction with a counterfeit, the unsuccessful group (Mdn = 2) was significantly less satisfied with their counterfeit than the successful group (Mdn = 3, U = 6768, $p < 0.001$, r = 0.29, *H7a supported*).

As to counterfeit process perception, there were no significant differences between groups related to perceived time taken to create a counterfeit (Mdn = 3, U = 5464, p = 0.359, r = 0.06, *H7b not supported*) or related to the perceived effort to create a counterfeit (Mdn = 3, U = 5290, p = 0.642, r = 0.03, *H7c not supported*).

Applying the Kruskal-Wallis test for independent samples, we did not find any significant differences in counterfeit quality (H(17) = 22.33, p = 0.173), match score (H(17) = 19.52, p = 0.300), satisfaction (H(17) = 8.9, p = 0.943), perceived time (H(17) = 19.37, p = 0.308) or effort (H(17) = 16.22, p = 0.508) across seminar groups. We also did not find any significant differences in fingerprint security perception (U = 5091, p = 0.943, r = 0.01) and intention to use fingerprint for unlocking the smartphone (U = 5178, p = 0.305, r = 0.07) logging into the mobile banking (U = 5185, p = 0.171, r = 0.10) and confirmation of transaction in mobile banking (U = 5103, p = 0.204, r = 0.09) between successful and unsuccessful participants.

4.2.8 Knowledge. Participants believed they had significantly less information before (Mdn = 3) the simulation than after (Mdn = 4, T = 7672, $p < 0.001$, r = 0.56, *H8 supported*).

4.2.9 Frequency of fingerprint authentication usage. For unlocking a smartphone, logging into mobile banking and confirming transactions in mobile banking, the intention of use was significantly higher before the simulation than after (*H9a-c supported*). Statistics for individual purposes are as follows: (a) smartphone unlocking (Mdn_{before} = 5, Mdn_{after} = 5, T = 821, p = 0.021, r = -0.20), (b) logging into mobile banking (Mdn_{before} = 4, Mdn_{after} = 3.5, T = 980, $p < 0.001$, r = -0.39) and (c) confirmation of transaction in mobile banking (Mdn_{before} = 4, Mdn_{after} = 3, T = 1417, $p < 0.001$, r = -0.29).

5 DISCUSSION

As we can see from the results, participants perceived fingerprints as less secure after the simulation. Also, a fingerprint was the only method where their perception was affected (except for the swipe pattern with a weak effect). However, this could be caused by the participants becoming more aware of fingerprint security and related attacks. Smudge attacks are relevant for both the swipe pattern and fingerprint authentication. Participants also did not perceive fingerprint as the most secure method even before the simulation, which is positive. However, this could also be influenced by watching a lecture, so only theory can also be impactful. However, as the results show, practical experience with fingerprint forgery impacts the perception of fingerprint security even more. Participants also reflected on their new perception of assumptions for IT security experts and their security perception of fingerprint authentication to reflect a reality that general users "were more trusting of biometric authorisation for financial applications" [24].

Regarding risk perception and prevention, participants reported reasonable suggestions. However, it is quite surprising that only two participants reported the usage of two-factor authentication as a good way of prevention after the simulation (which was less than before). Each authentication method has weaknesses, so it is important to emphasize the advantages of two-factor authentication usage since that is the way most companies adapt to secure their employee and customer systems.

Regarding perceived susceptibility to fingerprint attacks, participants were more suspicious before than after the simulation. Even though participants perceived the fingerprint as less secure and planned to use fingerprint authentication on smartphones less often for sensitive accounts (i.e., banking), their perception of susceptibility may seem unexpected. This could be caused by the fact that participants could not log into their smartphones, so they do not perceive the risk as very probable.

In the context of attacks related to fingerprint authentication, a forgery attack was perceived as easier to learn and perform than other fingerprint-related attacks without any expected differences regarding attacker level. When comparing the forgery attack with their perception before the experience, participants perceived the forgery one as easier to learn but more difficult to perform than before, and even less experienced attackers were expected to create a good counterfeit. The overall process was not very difficult from the required technical knowledge. Still, it contained many steps where certain skills were needed, e.g., knowing how to take a good-quality photo of a fingertip. The quality of the input is crucial. We tried to keep as many realistic scenarios as possible, so we asked participants to take a photo at home. We instructed them on creating a good photo, but the differences in the quality were significant. Some participants did not understand the point of the reference object. Further, as stated in [16], "low contrast between fingerprint ridge and valley, and clarity of fingerprint are two of most common degradation can decrease fingerprint recognition system performance", which is also applicable for the photo.

Even though not all participants were successful in spoofing in any way, they could also see that some of their classmates were successful. We also discussed with participants that different smartphones have different fingerprint readers, and some would not even register that the counterfeit is attached not because of its low quality but because of the material. As mentioned earlier, we struggled with the correct size because of not always the correct use or detection of a reference object in the photo. Even though we can see that successful participants were more satisfied with their counterfeits than unsuccessful participants, they do not differ in security perception or intention to use after the simulation.

Participants also reported their intention to use fingerprints less often, especially for mobile banking. A positive outcome is that participants also believe they have more information about fingerprint authentication to make an informed decision about what applications they will use it for. Intention to use is considered an indicator of behaviour, so we can expect that participants change their behaviour based on the experience gained during the simulation.

5.1 Limitations

We struggled with the quality of the photo and size estimation. Because of that, we believe participants would be more successful in creating a successful fingertip counterfeit if the right fingerprint

size were achieved. Also, our software for photo processing did not reliably estimate the coin borders, even though we improved based on testing on a smaller sample of more advanced participants in a different course[5]. However, there was much bigger variability in our larger sample.

Participants also created a counterfeit of their fingertips, which is not common practice (the victim and attacker are two different people). Also, time was very likely also a limiting factor since the execution of such an attack would require various steps to complete to be effective. However, if it were a real scenario, attackers could be more motivated to be successful in attacking.

6 CONCLUSIONS

We conducted a hands-on seminar about fingerprint forgery for 221 participants. We provided theoretical education and an in-person experience with fingerprint forgery of their own fingers. Even though we faced some technical difficulties and used basic material, 41 participants were successful in the spoofing according to the NBIS package for fingerprint matching, and 48 participants could register their counterfeit into the smartphone. Despite the difficulties faced, participants gained experience and improved their knowledge about fingerprint authentication, which led to more secure indented behaviour and different perception.

The most significant finding of our work is that participants perceive fingerprint authentication after the simulation as less secure regardless of their success in the simulation. Participants perceived the forgery process as easy to learn but hard to perform. Despite their decreased susceptibility to fingerprint attacks, they intend to use it less often for mobile banking. Even though not many of them considered two-factor authentication as a more secure solution, it is beneficial to highlight secure options.

ACKNOWLEDGMENTS

We would like to thank Karel Stepka from the CBIA laboratory at the FI MUNI for the photo processing script. We also thank all students for participation, seminar tutors for their help with realization, Jan Kvapil for technical support and Katarina Galanska for her help with coding. Agata Kruzikova was supported by Red Hat Czech.

REFERENCES

[1] Oliver Buckley and Jason R.C. Nurse. 2019. The language of biometrics: Analysing public perceptions. *Journal of Information Security and Applications* 47 (2019), 112–119. https://doi.org/10.1016/j.jisa.2019.05.001

[2] Patrick Burton, Kristin Cook, Rob Kelley, Jessica Ivy, and Kevin Thomas. 2022. Fingerprint spoofing: Exploring cybersecurity with limited technology. *Connected Science Learning* 4, 6 (2022).

[3] Ryan Carvalho and Norbert Tihanyi. 2021. Creating effective fingerprint artefacts: a cooperative and a non-cooperative method for bypassing capacitive and optical sensors with high success rate. In *2021 International Carnahan Conference on Security Technology (ICCST)*. 1–6. https://doi.org/10.1109/ICCST49569.2021.9717377

[4] Roberto Casula, Marco Micheletto, Giulia Orrú, Gian Luca Marcialis, and Fabio Roli. 2022. Towards realistic fingerprint presentation attacks: The ScreenSpoof method. *Pattern Recognition Letters* (2022). https://doi.org/10.1016/j.patrec.2022.09.002

[5] Roberto Casula, Giulia Orrù, Daniele Angioni, Xiaoyi Feng, Gian Luca Marcialis, and Fabio Roli. 2021. Are spoofs from latent fingerprints a real threat for the best state-of-art liveness detectors?. In *2020 25th International Conference on Pattern Recognition (ICPR)*. 3412–3418. https://doi.org/10.1109/ICPR48806.2021.9413301

[6] Chaos Computer Club 2013. *Chaos Computer Club breaks Apple TouchID.* Retrieved April 27, 2023 from https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[7] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch ID on IPhone Passcodes. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 257–276.

[8] Ines Goicoechea-Telleria, Ana Garcia-Peral, Anas Husseis, and Raul Sanchez-Reillo. 2018. Presentation Attack Detection Evaluation on Mobile Devices: Simplest Approach for Capturing and Lifting a Latent Fingerprint. In *2018 International Carnahan Conference on Security Technology (ICCST)*. 1–5. https://doi.org/10.1109/CCST.2018.8585605

[9] Taban Habibu, Edith Talina Luhanga, and Anael Elikana Sam. 2022. Assessment of How Users Perceive the Usage of Biometric Technology Applications. In *Recent Advances in Biometrics*, Muhammad Sarfraz (Ed.). IntechOpen, Rijeka, Chapter 3. https://doi.org/10.5772/intechopen.101969

[10] Suncica Hadzidedic, Silvia Fajardo-Flores, and Belma Ramic-Brkic. 2022. User perceptions and use of authentication methods: insights from youth in Mexico and Bosnia and Herzegovina. *Information & Computer Security* ahead-of-print (03 2022). https://doi.org/10.1108/ICS-07-2021-0105

[11] Ronald Kainda, Ivan Fléchais, and A.W. Roscoe. 2010. Security and Usability: Analysis and Evaluation. In *2010 International Conference on Availability, Reliability and Security*. 275–282. https://doi.org/10.1109/ARES.2010.77

[12] Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner. 2018. Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Understood. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (Hamburg, Germany) *(ARES 2018)*. Association for Computing Machinery, New York, NY, USA, Article 39, 9 pages. https://doi.org/10.1145/3230833.3234514

[13] Agata Kruzikova, Lenka Knapova, David Smahel, Lenka Dedkova, and Vashek Matyas. 2022. Usable and Secure? User Perception of Four Authentication Methods for Mobile Banking. *Comput. Secur.* 115, C (apr 2022), 12 pages. https://doi.org/10.1016/j.cose.2022.102603

[14] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *USENIX Security Symposium*.

[15] James Lewis. 1992. Psychometric evaluation of the post-study system usability questionnaire: The PSSUQ. *Proceedings of the Human Factors Society* 2, 1259–1263.

[16] Xinwei Liu, Marius Pedersen, Christophe Charrier, Patrick Bours, and Christoph Busch. 2016. The Influence of Fingerprint Image Degradations on the Performance of Biometric System and Quality Assessment. In *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*. 1–6. https://doi.org/10.1109/BIOSIG.2016.7736935

[17] Vaclav Matyas and Zdenek Riha. 2002. Biometric Authentication - Security and Usability. In *Advanced Communications and Multimedia Security*. Springer, Boston, MA, USA, 227–239.

[18] Sinjini Mitra and Jordan B. Barlow. 2022. Perceptions of Risk and Security Concerns with Mobile Devices using Biometric vs Traditional Authentication Methods. In *AMCIS 2022 Proceedings*.

[19] Tateo Ogane and Isao Echizen. 2017. Biometric Jammer: Preventing surreptitious fingerprint photography without inconveniencing users. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*. 253–260. https://doi.org/10.1109/BTAS.2017.8272705

[20] R Rogers, John Cacioppo, and Richard Petty. 1983. *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation.* Guilford Press, New York, 153–177.

[21] Statista 2022. *Biometric usage worldwide in 2021, by type.* Retrieved January 12, 2023 from https://www.statista.com/statistics/1338824/global-biometric-usage-by-type/

[22] Nik Thompson, Tanya Jane McGill, and Xuequn Wang. 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security* 70 (2017), 376–391. https://doi.org/10.1016/j.cose.2017.07.003

[23] Craig I. Watson, Michael D. Garris ad Elham Tabassi, Charles L. Wilson, R. Michael McCabe, Stanley Janet, and Kenneth Ko. 1987. *User's Guide to Export Controlled Distribution of NIST Biometric Image Software (NBIS-EC).* Technical Report. Gaithersburg, MD, USA.

[24] Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2019. "Pretty Close to a Must-Have": Balancing Usability Desire and Security Concern in Biometric Adoption. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300381

[5] These participants voluntarily provided their photos for better estimation of coin and finger borders, with destructed papillary lines of their fingers, so only borders of a finger, coin, and the background were visible.