IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2024.0429000

No Thumbs Up in Pictures! Fingerprint Forgery for the Masses...

AGATA KRUZIKOVA[1], ALESSIA MICHELA DI CAMPI[2], VASHEK MATYAS[3], and TOMAS CERNY

[1]University, Brno, Czech Republic (e-mail: kruzikova@mail.muni.cz)
[2]University Ca' Foscari of Venice, Venice, Italy (e-mail: alessia.dicampi@unive.it)
[3]Masaryk University, Brno, Czech Republic (e-mail: matyas@fi.muni.cz)
[4]University of Arizona, Tucson, Arizona, USA (e-mail: tcerny@arizona.edu)

Corresponding author: Agata Kruzikova (e-mail: kruzikova@mail.muni.cz).

None of the authors have a conflict of interest to disclose.

ABSTRACT Fingerprint verification is a popular smartphone authentication method used even for sensitive services such as banking. However, fingerprint verification also has some issues, such as spoofing even by inexperienced impostors utilizing a thumbs up Instagram picture without the victim's knowledge. This can be a considerable risk with partial scanning of fingertips used on smartphones. To better understand the fingerprint forgery process and perception, we performed a hands-on forgery simulation to assess the robustness of smartphone fingerprinting technologies. Overall, 370 inexperienced participants created glue or silicone counterfeits from a photo of their fingers. Five participants logged in to smartphones with their counterfeits, and 74 registered them into smartphones as a ''finger''. With improvements in the forgery process in the second run, we achieved an increase in true matches from 41 to 113. Our study shows that quality and scan enhancement is important during the forgery process – enhancement improves the match score. Our analysis also provides insights into user perceptions regarding the forgery experience. Participants intend to use fingerprint authentication less often, but we found mixed results regarding the perception of fingerprint security.

INDEX TERMS authentication, finger-photo, fingerprint, forgery, smartphone.

I. INTRODUCTION

he adoption of biometric technology in smartphones has been on the rise, with 71% of smartphones featuring enabled biometrics as early as 2021 [1]. Biometrics are a ''desired feature'' for sensitive services such as mobile health applications [2, p. 12] or mobile banking [3]. The most widespread biometrics is fingerprint [4].

Plenty of studies considered the usability and the security perception of fingerprint authentication (e.g., [3], [5]). These investigations suggest that fingerprints are popular for their high usability and perceived security. They also show that it is widely adopted among users and often integrated into devices and applications, making it a broadly accepted and recognized authentication method. Nevertheless, there are many misconceptions related to fingerprint security [6], [7]. While perceived as a very secure authentication method, several risks exist, e.g., spoofing [8], [9], which can be done even by inexperienced impostors (i.e., non-genuine user who are committing the act of spoofing for the first time) and without the knowledge of a victim (e.g., by taking a photo of a screen full of fingerprints' smudges [10]). The security concern is even more significant for smartphone fingerprint readers that scan only a part of the fingerprint, typically without liveness detection. This means that when only a portion of the fingerprint is captured, there is a higher likelihood of generating a false match due to ''entropy loss'' [10], [11]. In this context, ''entropy loss'' refers to reducing the amount of unique information available for verification when only a partial fingerprint is used, increasing the risk of unauthorized access.

This work focuses on creating a 3D physical counterfeit from a photo of a finger (i.e., finger-photo) and then unlocking a smartphone with such an artifact. It explores how this vulnerability misuse is effective when done by inexperienced impostors to demonstrate its potential concerning current fingerprint readers. Since fingerprint authentication is used often on smartphones, we focus on differences between using counterfeits on distinct smartphone fingerprint readers to address the following research question:

RQ1: Are the current readers vulnerable to counterfeits cre-

ated from a photo of a fingertip by inexperienced impostors concerning the type (i.e., capacitive, optical and ultrasonic) and position (i.e., front, rear and side) of the reader?

To better understand the quality of counterfeits created from a finger-photo, counterfeits and corresponding genuine fingertips were scanned and processed to evaluate their quality and compute match scores on a computer. Also, we investigated the role of fingerprint enhancement on the quality of scans and match scores to answer the following research question:

RQ2: What is the achieved quality of counterfeits created from a photo of a fingertip by inexperienced imposters? What is the impact of fingerprint enhancement and scan quality of counterfeits on achieved match scores?

This paper explores the effectiveness of exploiting a vulnerability in common fingerprint readers towards a 3D physical counterfeit from a finger-photo to unlock a smartphone. As mentioned above, users often perceive fingerprint as the most secure authentication method. In our previous study about the security perception of fingerprint authentication [12], we expected that this perception is based on misconceptions about fingerprint authentication. These misconceptions were meant to be overcome by educating users about biometrics, including a hands-on spoofing experience on creating a counterfeit from a finger-photo, which is not a common approach. As part of our study, we also extended our investigation for another experiment run about user perception to respond to the following research questions:

RQ3a: What is the perception of fingerprint forgery and fingerprint security after fingerprint forgery simulation?

RQ3b: Do changes in the simulation affect the changes in the perception?

To answer the research questions, we conducted a hands-on spoofing simulation of creating a 3D physical counterfeit from a finger-photo with a larger group of 370 inexperienced impostors. We simplified the process of counterfeit creation from a finger-photo described in [12], but we used different materials for counterfeits. Also, in that study, we focused only on user perception (answering the RQ3a, but not the RQ3b). Notably, we did not consider the effectiveness of counterfeits on different fingerprint readers (not considering the RQ1) or the role of the quality of scans and their enhancement on match scores (not considering the RQ2). This contrasts with the approach in the study presented in this paper, where all these research questions were addressed. Further, regarding user perception, we collected data from 149 additional participants to revise our findings after some changes in the simulation.

The contributions of our work to fingerprint verification security are:

- Spoofing feasibility demonstration: We demonstrated that it is relatively simple for inexperienced impostors, without any special equipment, to forge a fingerprint from a finger-photo within just two hours.
- Demonstration that these counterfeits are a real risk to smartphone fingerprint readers because even few inexperienced imposters could log their first-made counterfeits into a smartphone. However, achieving such quality for the first-ever-made counterfeit is not highly probable.
- Exploring the vulnerability of current smartphone fingerprint readers used by a young population – around 20% of the investigated smartphones accepted a counterfeit as a human finger (during the registration as a new ''finger'').
- Examining achieved quality and effectiveness (match score) of such spoofing. We also examined the role of fingerprint enhancement on achieved match scores.
- Rigorously examining (in a two-year study) the perception of fingerprint spoofing before and after the forgery experience concerning changes in the simulation process.

This manuscript is organized as follows: Section II provides related work regarding fingerprint readers, fingerprint quality and forgery, security perception, and education. Section III contains the methodology and description of the forgery process emphasizing changes made in contrast to the first run [12]. Section IV presents the findings obtained regarding smartphone readers, achieved scan quality and match scores, and forgery perceptions. In Section V, results and implications are discussed. The paper is concluded by Section VI.

II. BACKGROUND

This section elaborates on fingerprint readers to highlight how they may react to counterfeits. It describes the aspects influencing the quality of fingerprints. It also provides background on finger-photos. With a focus on fingerprint forgery, it presents prior research on fingerprint replicas. Finally, it details user perception of fingerprint security, cybersecurity education, and intervention.

A. FINGERPRINT READERS

Three commonly used types of fingerprint sensors in smartphones are optical, capacitive, and ultrasonic. Each technology has its unique approach to capture and process fingerprint data. *Optical* sensors use light to capture the fingerprint image. The reflected light is converted into a digital image, and unique fingerprint features are extracted [13]. *Capacitive* sensors use electrical current and an array of tiny capacitors to detect fingerprint details. The finger's ridges and valleys alter capacitance, generating a fingerprint image based on electrical field variations [13]. *Ultrasonic* sensors use sound waves to create a detailed fingerprint image by bouncing waves off the finger's ridges. The reflected waves are analyzed to generate a digital fingerprint image [13]. Smartphone fingerprint readers are specific in their partial scanning, which makes them more vulnerable than full fingerprint scans [11].

B. FINGERPRINT QUALITY

Damaged or injured skin can pose challenges to fingerprint identification. Conditions like burns, dryness, or scars can

disrupt ridge patterns, making it difficult for automated systems to identify individuals precisely.

Automated systems may struggle to match and identify individuals accurately, as *skin diseases* cause texture and clarity variations in fingerprints, reducing their reliability as biometric identifiers [14]. E.g., patients with hand dermatitis were approximately four times more likely to have dystrophic fingerprints that failed the verification process compared to healthy individuals [15].

Sport activities involving physical contact and extreme conditions can increase the risk of fingerprint damage. Repetitive friction and trauma during sports can alter fingerprints' texture and clarity, compromising their reliability as biometric identifiers [16]. Exposure to extreme environmental conditions may contribute to fingerprint deterioration, leading to challenges in using fingerprint recognition systems as e.g., weightlifters, gymnasts, tennis players, and rock climbers are susceptible to ''black palm'' caused by haemorrhage [17, p. 37].

Fingerprint Ridge Density varies among individuals of different ethnicity, geographical locations and gender – males have generally lower densities than females, but there is some overlap within the population [18].

C. CONTACTLESS AND CONTACT-BASED ACQUIRED FINGERPRINTS

Authentication with a finger can be done in two ways on smartphones: via a sensor (fingerprint-based authentication) and via a standard smartphone camera (finger-photo-based authentication) [19]. Current smartphones widely use touch-based sensors for capturing fingerprints, but contactless finger-photos are not widely used for authentication, likely due to various challenges associated with their use [19]. Finger-photos captured by a smartphone camera have several issues compared to contact-based sensors, such as lower contrast between ridges and valleys, parts of the finger being out of focus, and problematic backgrounds, requiring additional processing [20], [21]. However, in both cases, a finger(print) sample is registered and then compared with another sample obtained in the same (touch-based or touchless) way for authentication purposes.

When combining contactless and contact-based samples, there is a problem of reliably comparing finger(prints) acquired by these two methods. For example, issues arise when enrollment is done via a fingerprint sensor (touch-based) but verification is done with a standard smartphone camera (touch-less) [22]. Nonetheless, some techniques for matching contactless and contact-based fingerprint images exist (e.g., [23]). These techniques aim to improve touch-less fingerprint sensing for direct processing and comparison with samples in the database. In our research, we used contactless acquired finger-photos for forgery purposes. The resulting physical counterfeit was then scanned by a standard touch-based fingerprint scanner and compared to a genuine sample also scanned by the same touch-based fingerprint sensor.

D. FINGERPRINT FORGERY

There are several ways to create a replica of a fingertip, with two approaches: cooperative and non-cooperative. The first example of a replica is a simple cast of the fingers, which could be done regardless of the victim's cooperation [24]. A cast of the finger was already done during hands-on exercises with children as an educational activity [25].

More sophisticated spoofing is done without the knowledge and cooperation of the victim, e.g., by creating a counterfeit based on the photograph of the latent fingerprints on the smartphone screen [10], [26]–[28]. Casula et al. [27], [28] showed that such counterfeit works on smartphone readers, but the quality of the input is crucial. They achieved better results on cleaned screens with intentionally created fingerprint smudges (cooperative) than when simulating the real live environment with dirt (non-cooperative approach).

There are two studies reconstructing a fingerprint directly from a finger-photo. Ogane and Echizen [29] simulated extracting papillary lines from a photo to develop a solution for fingerprints that disables extracting fingerprints from a finger-photo. In our previous study [12], focusing on creating a counterfeit from a finger-photo made by 221 students at a university, we found out that 26% of our participants could register the counterfeit into their smartphones. However, the study [12] presents only participants' perceptions and reports their achievements without further details. It does not investigate the relationship between scan quality, the role of scan enhancement and the effectiveness of counterfeits on different smartphone readers.

These two studies cannot be classified as cooperative or non-cooperative – victims publish photos of their fingers by themselves, but not with the intention that their fingers will be spoofed. When impostors find a photo that includes a detailed fingertip on the internet, they could misuse it for spoofing without the victim's knowledge. Our threat scenario is as follows: users take photos of their fingers and put them onto their social network, e.g., as a challenge on Instagram with a thumb-up photo. Then, the impostor finds this photo and creates a replica without users' knowledge.

E. USER PERCEPTION OF FINGERPRINT SECURITY

Recent studies found that fingerprint is perceived as the most secure biometric [30] or authentication method compared to token and knowledge-based methods [3], [31]. Some users even consider biometrics as ''unhackable'' [7, p. 5]. As [10, p. 522] states, ''users may not perceive the risk of Touch ID because of the latent fingerprints left on the smartphone''.

Perceptions of fingerprint security can differ based on the domain where it is used for authentication. Even though security experts use fingerprint authentication, they do not use it for sensitive services, such as banking [32]. Fingerprint can be used as two-factor authentication (e.g., with a combination with a PIN), which seems acceptable to users [7], [33].

Several misconceptions surround the perception of fingerprint authentication, e.g., storage of the fingerprint data and its privacy [6] or user expectation for biometrics providing

the same protection as two-factor authentication [34]. Misconceptions could also relate to IT savvy users as well [32] together with a perceiving fingerprint as secure [35].

F. CYBERSECURITY EDUCATION AND INTERVENTION

There are several hands-on hacking exercises, mostly targeting university students [36]. Also, intervention in computer security (e.g., [37]) or cybersecurity education (e.g., [38]) is a widely adopted approach, frequently in the field of fishing (e.g., [39]). Regarding university education about cybersecurity, intervention also plays an important role, and authentication is one of the bigger topics [40]. For example, an intervention regarding secure coding on students achieved a positive outcome [41]. Also, ''achievement-based teaching interventions'' were found to help students to improve their knowledge about network security [42, p. 129]. Even multidisciplinary intervention of ethics into computer security education helped students to perceive it as ''interesting and relevant'' [43, p. 475].

III. METHODOLOGY

To answer our research questions regarding the demonstration of fingerprint spoofing feasibility and its perception, our study participants collected finger-photos for the extraction of fingerprint templates for mold. These templates are utilized to create 3D counterfeits, which are tested across various smartphones. Given the need for scalability, we performed this on a large scale utilizing university coursework. We did not collect data from experienced perpetrators who routinely forge fingerprints, possibly without any relevant technical background. Instead, we choose computer science (CS) students as our participants because a basic understanding of current technical solutions is part of their education and knowledge – they must know as professionals if they can trust the technical solutions. We prepared a fingerprint forgery simulation seminar to collect data from the CS student sample. We examined participants' experience with fingertip pattern counterfeits on various smartphone fingerprint readers, quality assessment and effectiveness via match score of their created counterfeits, and understanding of their perception of fingerprint authentication and forgery. The first simulation run from the Spring of 2022 comprised a lecture and two hands-on seminars. For Spring 2023, several changes were made, repeating the experiment (i.e., one lecture and one hands-on seminar), as shown in Figure 1.

A. COURSE DESCRIPTION

The course where data was collected is taught in the second year of bachelor studies at a university. It is a mandatory course for all computer science students regardless of specialization, introducing them to IT security and covering several topics, including the basics of cryptography, privacy policies, network security, secure programming, usable security, and authentication. These were not computer (cyber)security students, so only the basics of computer security were presented to them in this course.

Students should start with a lecture[1] about the topic for the week, followed by a hands-on seminar in smaller groups (∼16 students per group). For the fingerprint forgery seminar, the lecture covered identity and access management, including fundamental concepts like passwords, tokens, and biometrics. The focus was on error rates, fingerprints, and face recognition.

The seminar structure consisted of the following:

1) Inviting students to participate in a study.
2) Measuring their perception of fingerprint authentication and forgery using a questionnaire.
3) Introducing forgery simulation in a hands-on manner.
4) Allowing participants to create physical counterfeits.
5) Instructing participants to process these counterfeits using matching software on a computer.
6) Encouraging participants to use their counterfeits to unlock and register them on their smartphones.
7) Collecting results on the processing of the counterfeits (without collecting any personal or biometric data).
8) Continuing the survey on perception.

B. FINGERPRINT FORGERY PROCESS

The participants created a counterfeit from the finger-photo. The forgery process demonstrated in Figure 2 consisted of the following steps:

leftmargin=.45cm

1) **Finger-photo:** Participants had to take a finger-photo with the proper lighting and next to the reference object to estimate the fingertip size on a uniform black background. Participants used their devices (e.g., smartphones) to photograph their fingertips[2]. This demonstrated to the participants how challenging or easy it can be to capture a finger-photo of their own finger using their smartphone camera. Participants were expected to take the finger-photo before the seminar.
2) **Extracting papillary lines – template for mold:** Participants processed their finger-photos with our prepared software to get a life-size inverted black-white picture of their fingertip pattern. Firstly, a reference

[1]Lectures were pre-recorded due to class size and COVID-19 restrictions in 2022. Lectures were taught in person, with the possibility of watching recorded lectures with a few days' delay in 2023.

[2]We provided a device for photographs only in exceptional cases where participants struggled to get the finger-photo and asked for help.

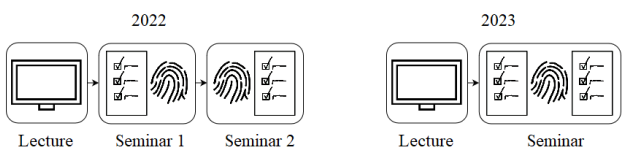

FIGURE 1. Simplified schemes of procedures in 2022 [12] and 2023: The number of seminars varied, but the basic idea remained the same – first was a theoretical lecture, then the first questionnaire at the beginning of the hands-on part (seminar). The seminar then focused on the creation and processing of counterfeits. The seminar finished with the second questionnaire.

FIGURE 2. Schema of the fingerprint forgery process adapted from [12]: (1) a finger-photo, (2a) template preparation – extracting papillary lines, (2b) inverting colors on the template, (3) printing the mold on the printer (4a) application of a cast material on the mold and (4b) resulted counterfeit.

object was detected to estimate the size of the finger. Then, the borders of the fingertip were detected. In the area of the detected fingertip, the software was looking for fingertip patterns – papillary lines, i.e., ridges and valleys. After that, the colors of ridges and valleys were inverted to get a template for the mold (''negative'').

3) **Mold for 3D counterfeit:** The inverted horizontally flipped black-white picture was printed on a plastic foil to create a mold. The layer of ink creates the ridges (that impress valleys into the counterfeit material), while a plastic foil without ink creates valleys (resulting in counterfeit ridges). Plastic foil has no structure, and the ink has no grades of shade, so it keeps all template features designed on a computer.
4) **3D counterfeit:** The form was then filled with some cast material. All participants applied the material by themselves. The final counterfeit cast was created when the material was dried out solid.

C. COUNTERFEITS PROCESSING

When a physical 3D counterfeit was created, participants were expected to process it with NIST Biometric Image Software (NBIS) tools [44]. These tools were used to evaluate the artifacts on a computer. Specifically, NFIQ was used for quality evaluation, MINDTCT for creating a minutia map, and BOZORTH3 for computing match scores by comparing the counterfeits to genuine fingertips. These tools were also used by, e.g., [45]. In addition to using NBIS tools for evaluation, participants attempted to log into their smartphones using these physical counterfeits. Counterfeit processing consisted of the following steps:

1) **Scanning:** It was necessary to scan genuine fingertips and counterfeits first to be able to process them on a computer with NBIS tools. An external fingerprint reader Futronic FS80H was used.
2) **Quality evaluation:** The quality of genuine fingertips and counterfeits scans was evaluated with the NFIQ tool. Participants were informed about the quality of their scans.
3) **Enhancement:** When processing fingerprints, enhancing the images is a good practice. For fingerprint enhancement, Gabor filtering [46], [47] was used. However, the enhancement requires input scans of a certain quality [48]; otherwise, false minutiae points are created. In the first run, scan enhancement was applied to the template for mold. In the second run, mold was created from the non-enhanced (raw) template, and enhancement was used only on scans of genuine fingertips and counterfeits (see Section III-E).
4) **Minutia map creation:** The minutiae map of genuine fingertips and counterfeits scans was created with the MINDTCT tool.
5) **Matching:** The match score was computed with the BOZORTH3 algorithm based on the files created in the previous step. Raw and enhanced scans of genuine fingertips were compared to raw and enhanced scans of counterfeits.
6) **Smartphone activity:** Participants were encouraged to try logging into smartphones with their counterfeits (after registration of the corresponding genuine fingers into the smartphones). Also, they were attempting to register the counterfeits into the smartphones as new fingers.

D. DIFFERENCES BETWEEN RUNS

Based on the experience from the first run [12], changes were incorporated into the second run. One seminar (2 hours) was used instead of two (2x2 hours) (see Figure 1). For example, the presentation part done by seminar tutors was shortened and did not repeat the theoretical part of the lecture. Also, the basics of Gabor enhancement were explained to the participants during the second seminar run. Other significant changes are outlined in the following subsections.

1) Material used for counterfeit

The first issue was the drying time of the material used for counterfeit creation. The glue used in the first run is a very accessible and cheap option for many possible perpetrators. However, the most significant disadvantage of glue is its long drying time (several hours). In the second run, silicone Body Double Fast was used instead, with a drying time of minutes, enabling us to have only one hands-on seminar. Silicone Body Double was also used for presentation attacks in [28].

2) Finger-photo

Participants struggled with taking a good finger-photo in the first run. They also pointed out that achieving a good finger-photo was challenging. In the second run, a summary of recommendations on taking pictures of a fingertip was presented to our participants (e.g., to avoid insufficient resolution, blurred parts, shades and angles). Also, in the second run, participants could use a photo box painted black inside (see Supplementary materials). Adequate lighting to the box was provided – a ring light with warm and cold light, so everybody could choose what works best for their (smartphone) cameras or use their camera's built-in flash. A stock of coins was prepared as a reference object to be at the same level as a photographed fingertip to overcome misunderstandings and wrong size estimation when processing. Also, participants had to manually mark the fingertip and reference object area in the second run since some difficulties were faced when it was done automatically in the first run.

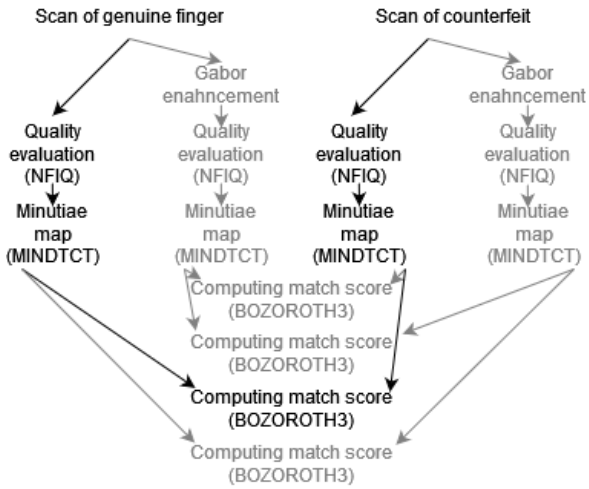

FIGURE 3. Schema of scans' processing. Black parts were done in both runs, grey parts were done only in the second run in 2023.

3) Fingerprint enhancement

Gabor enhancement was used before printing a form onto the foil in the first run. However, after the pilot (see Section III-E) and our internal testing, we decided not to apply the enhancement on the template made from the processed finger-photo before printing it onto the foil. Still, the enhancement was used on scans of genuine fingertips and counterfeits, as shown in Figure 3.

4) Scan processing

Participants worked with the external fingerprint readers independently without seminar tutors' assistance (assistance was provided only where needed) in the second run, in contrast to the first run, where participants needed their seminar tutors' assistance. This change enabled participants to scan their fingerprints (genuine and counterfeit ones) into the computer multiple times – precisely ten times each to simulate the registration phase better when a fingertip is not scanned just once but several times. Ten attempts were set up to limit the maximum number of attempts when simulating logging into a system. Then, participants processed their scans with prepared scripts, generating a file with the quality evaluation (a result of the NFIQ tool) of all scans (of genuine fingertips and counterfeits and their enhanced versions) and the match score (a result of the BOZORTH3 tool) of each combination. There is no such file and data for the first run as participants got only a few scans, and they reported only the best-achieved value.

5) Usability of the process

We improved the usability of the process when using the tools, so participants could focus more on the core topic of counterfeiting. In the first run, participants had to work with all the tools themselves (i.e., software for finger-photo processing and NBIS tools from the command line). In the second run, participants used a prepared Jupyter notebook [49] where they did not have to look for the software or copy commands into the terminal – they were simply running the cells in the notebook. Participants were already familiar with them from previous seminars.

E. PILOT TESTING

After the first run for around 300 students, new challenges were identified. Some changes described in Section III-D were incorporated and tested with ten students of another Master-level course taught in the autumn of 2022. Since this pilot sample (10 students interested in IT security) differed from our main sample group (all CS students), the pilot's main focus was logistics finetuning. The questionnaire was not piloted since we asked selected questions from the first run. We tested the influence of the Gabor enhancement in various phases of counterfeit creation and processing. Instead, participants were asked to create two counterfeits – one raw and one enhanced with the Gabor filtering. Then, our participants scanned their genuine finger, raw counterfeit, and enhanced counterfeit. They continued processing all the scans as they were, and they also applied enhancement on all scans. Then, they reported quality evaluation and match scores of their scans. Eight of ten provided us with the testing data (automatically generated into a file), where six achieved a true match for their counterfeits in BOZORTH3. Then, only five shared their results of logging in to their smartphone with their counterfeit, resulting in one successful pilot participant. Based on the testing, we decided to use raw and enhanced scans, but not to enhance the template for a mold.

F. MEASURES

Three data types were measured: (1) position and type of smartphone fingerprint readers and their response to login with and registration of counterfeits, (2) quality and match score of genuine fingertips and counterfeits scans, and (3) user opinions and experiences.

1) Fingerprint readers (RQ1)

Participants reported the smartphones they used for attempting to log in with counterfeits via survey, ideally as a link on a specification of the smartphones. The links with smartphone specifications were manually researched by us to identify their fingerprint readers. Then, the smartphones were classified according to their type and the position of the sensor into the following categories: optical, capacitive, and ultrasonic for type and front, rear, and side for position.

For our analysis, we divided the participants' achievements into three groups (see Table 1): (1) $GLog_1, GReg_1$ as to those who could log in with or register the counterfeits into smartphones; (2) $GLog_2, GReg_2$ as those who could not log in with or register their counterfeits but that the smartphones recognized that "a finger" was touching the sensor; and (3) $GLog_3, GReg_3$ as those who could not log in with or register their counterfeits into the smartphones. The results belonging to login are reported as $GLog$ followed by a number (from 1 to 3 depending on what the sensor perceived during login). At

TABLE 1. Participant group acronyms.

Stage	Answer proposed in the questionnaire	Group acronym
Responses when participants logged into smartphones with their counterfeit	Yes, I was able to log into the smartphone	$GLog_1$
	No, but the smartphone recognized that something was touching the reader	$GLog_2$
	No, the smartphone did not even recognize that something was touching the reader	$GLog_3$
Responses when registering their counterfeits into the smartphones as genuine finger	Yes, I was able to register my counterfeit into the smartphone	$GReg_1$
	No, but the smartphone recognized that something was touching the reader	$GReg_2$
	No, the smartphone did not even recognize that something was touching the reader	$GReg_3$

the same time, the acronym *GReg* followed by a number (1 to 3 depending on what the sensor perceived at registration) is used for the results regarding the counterfeit registration into the smartphone.

2) Scan quality and match score (RQ2)

Concerning counterfeit processing, the quality of genuine fingertip and counterfeit scans and match scores were measured. Quality was measured with the NFIQ tool. The evaluation is on a scale from 1 (the best) to 5 (the worst). The BOZORTH3 algorithm computed the match score. The resulting value (match score) indicates the number of corresponding minutiae points. In this case, a score equal to or above 40 is considered a true match.

3) Perception (RQ3)

An online questionnaire was used to measure perceptions of fingerprint authentication and forgery. Since we were primarily interested in changes in perception before and after the forgery simulation, most items were measured repeatedly before and after the simulation on a 5-point Likert scale, where a higher value represents stronger perception. The questionnaire items are in Supplementary materials. If not stated otherwise, items were adapted from the first run. Participants already knew the results of their counterfeit processing when answering questions after the forgery simulation, so their experience and achievements could influence them.

Observations are classified into two main groups: fundamental and other interesting. Among the fundamental observations are fingerprint security perception, perception of difficulty in learning and performing fingerprint forgery, intention to use fingerprint for unlocking smartphones, login into mobile banking, and confirming transactions in mobile banking. Other observations cover expected fingerprint security perception by security experts and the general public, perceived susceptibility, the expected level of the attacker able to do forgery, and (measured after the simulation) satisfaction with created counterfeit and time and effort perception of the forgery.

G. ETHICS AND REPRODUCIBILITY

Participants created a counterfeit of their own finger from their own finger-photo. This does not reflect the real scenario, but participants processed only their own data concerning personal data processing. The research team did not collect any biometric data (e.g., finger-photos or maps of the minutiae points) from participants. When participants provided the file with match scores and quality evaluations, this file contained no biometric data. We got ethical approval from the Institutional Review Board as a component of the research effort consisting of several investigations centered on user authentication.

Study participation (filling out the questionnaires and providing the file with match scores and quality evaluations) was voluntary and done during the seminar(s). There were no advantages or disadvantages from (non-)participation. Seminar tutors were unaware of whether students participated or not. The questionnaire started with informed consent with participation, and all the questions could be unanswered if the participant did not want to. We prepared a substitute task for cases when somebody was unwilling to participate even in the hands-on seminar.

Regarding reproducibility, the questionnaire is in Supplementary materials. Nevertheless, the data from participants cannot be published because some of our participants added identifications to their data even though they were explicitly asked not to do so.

H. LIMITATIONS

Due to sensitive personal data, we did not collect biometrics data – all the analyzed data were processed or reported by our participants. However, we still consider our study beneficial as we achieved data from a large sample of 370 participants and 190 distinct smartphone models, and we got quality evaluations for 6402 scans and 59821 match scores in total.

Another limitation pertains to accurately identifying the type and location of fingerprint readers on smartphones. Even though participants were encouraged to put the link of the smartphones where they tried to log in and register their counterfeit with the smartphone specification, some reported just the model's name. The same models could differ based on their manufacturing year, so the data do not have to be precise in all cases. Nevertheless, this was the only practical approach to gather such information from a large sample of currently used smartphones.

IV. RESULTS

This section aims to comprehensively analyze the data collected and the statistical analyses performed, offering insights into the research questions. The primary objective is to examine the impact of scan quality on achieved match score and explore the relationships between location and type of fingerprint sensors within the context of our research framework, together with users' perception. Python3 scipy

stats (library dedicated to statistical analysis) was used for data analysis [50]. Perception data were analyzed with IBM SPSS 27 [51]. Perception data for both runs were analyzed separately and statistically compared to each other. Due to the outliers and data distribution, we used non-parametric tests. The significance is considered at the level 0.05.

A. SAMPLE

Overall, data from 370 participants were analyzed. The sample is described in Table 2. Before analyzing the data, we excluded cases where participants did not finish one of the questionnaires or filled both questionnaires after the simulation. We also excluded participants from our analysis who failed to scan their genuine fingertip and counterfeit ten times or did not report match scores. The participants in the first run are different from those in the second run.

TABLE 2. Sample characteristics.

	2022 [12]		2023	
Variable	N	%*	N	%*
Enrolled students	295		297	
Seminar tutors	16		20	
Final sample	221		149	
Gender				
– Female	32	15	18	12
– Male	183	83	124	83
– Others	3	1	2	1
– Missing	3	1	5	3
Age M (SD)	21	(1.0)	21	(1.1)
Having a fingerprint reader on a smartphone				
– Currently	180	81	117	79
– In the past	29	13	29	20
– Never	11	5	3	2
Having (ever) a fingerprint reader on:				
– Laptop	96	43	63	42
– Other device (not smartphone/laptop)	13	6	9	6
– Nowhere	108	49	76	51
– Missing	4	2	1	1
Fingerprint authentication at any device				
– Currently using	183	83	122	82
– Used in the past	23	10	15	10
– Tried, never used	7	3	9	6
– No experience	8	4	3	2
Own fingerprint registered on someone else's smartphone	-	-	36	24

*Percentage does not give always 100% due to rounding.

B. FINGERPRINT READERS (RQ1)

1) Counterfeit login

Based on the success of logging into smartphones with counterfeits, Table 3 provides insights into the distribution of participants. We reported only $GLog_1$ for the first run in [12] with a mere 0.5% of participants. However, in the first run, we also measured $GLog_2$, which accounted for 41%, and $GLog_3$ represented the majority with 58%. In the second run, $GLog_1$ recorded an increase, with 3% of participants. $GLog_2$ experienced a decrease, falling to 20% and $GLog_3$ continued to be the predominant group, with a substantial 78%. In conclusion, $GLog_1$ and $GLog_3$ increased over $GLog_2$.

2) Counterfeit registration

By examining the collected data, we aim to shed light on the effectiveness and accuracy of the registration process for a fingerprint. These results encompass the success of registering counterfeits into smartphones as genuine fingers. As Table 3 shows, $GReg_3$ experienced growth, becoming the predominant group with 75% in the second run, while $GReg_1$ and $GReg_2$ reduced.

TABLE 3. Participants divided by group for login, registration and login after registration.

		2022		2023	
	Group	N	%*	N	%*
Counterfeit login	$GLog_1$	1	0.5	4	3
	$GLog_2$	91	41	29	20
	$GLog_3$	129	58	116	78
Counterfeit registration	$GReg_1$	57	26	17	11
	$GReg_2$	46	21	20	13
	$GReg_3$	118	53	112	75
Counterfeit login after counterfeit registration	$GRLog_1$	38	17	14	9
	$GRLog_2$	14	6	2	1
	$GRLog_3$	5	2	1	1
	NA	164	74	132	89

3) Counterfeit login after counterfeit registration

These results are for participants who were able to register their counterfeit on a smartphone as a new "finger" ($GReg_1$). Table 3 shows how many of them were able to successfully log in ($GRLog_1$) or at least trigger the phone's fingerprint reader ($GRLog_2$) after a successful counterfeit registration in contrast to the overall sample. When considering only participants with successful registration in the first run, $GRLog_1$ rates are as follows: out of 57 participants who were able to register their counterfeit, 67% (N = 38) unlocked the smartphone with such counterfeit. In the second run, $GRLog_1$ had a success rate of 83%, with 14 out of 17 attempts being successful.

4) Types and locations of readers

Table 4 provides a thorough comparison of the different types of fingerprint readers and where they are located on the devices. The most prevalent type in both runs was the capacitive one. Optical readers were the second most common type, and the ultrasonic ones had the lowest representation. Regarding fingerprint reader locations, the front was the most common position in both runs, followed by rear and side locations. Finally, the data indicate a notable shift in fingerprint reader types and locations between runs. Capacitive readers witnessed a slight decline in usage, while optical readers increased. Moreover, there was a significant increase in fingerprint readers placed on the front and a corresponding decrease in rear placement.

Since we divided data into groups according to whether or not there had been a success in log-in or registration, we inves-

tigated which locations and types of fingerprint sensors belonged to groups 1 and 2 ($GLog_1, GLog_2$ and $GReg_1, GReg_2$) by excluding the unsuccessful group 3 ($GLog3$ and $GReg3$). Table 4 shows the data for different types and locations of sensors. The comparison below shows the differences between the first and second run. The percentage of capacitive vulnerabilities decreased for $GReg_1$ and for $GReg_2$. However, during the same period, the percentage of optical vulnerabilities increased for $GReg_1$ and $GReg_2$. Additionally, the percentage of ultrasonic vulnerabilities decreased for $GReg_1$ and $GReg_2$.

Regarding fingerprint sensor locations, the percentage of vulnerabilities located in the front increased for $GReg_1$ and $GReg_2$ from the first to the second run. The percentage of vulnerabilities located in the rear decreased for $GReg_1$ and $GReg_2$ during the same period. The percentage of vulnerabilities of readers located on the side for $GReg_1$ increased, while for $GReg_2$ it decreased.

5) Diverse responses for the same smartphone models

During the analysis, some observations emerged, revealing diverse behaviors among smartphones of the same model during login and registration processes. Notably, we encountered 20 distinct smartphone models comprising a total of 94 devices in the first run, while in the second run, six models encompassed 32 devices. In the first run, most of these devices belonged to the $GReg_2$ and $GReg_3$ groups. However, the iPhone 8 model stood out due to its conflicting behaviors during registration, being successful in one case and failing to detect any touch input in another. In the second run, the new smartphone models demonstrated varying registration behaviors, with three displaying opposing responses. Moreover, these contrasting behaviors occurred more frequently in the second run compared to the first one. Examining the login phase, in the first run, out of the 94 smartphone models, 10 exhibited responses that surpassed the number of models showing opposite behaviors during registration. In the second run, only two of the four smartphone models from that year demonstrated responses to opposites compared to the registration stage. In conclusion, the second run witnessed increased mixed responses in both the login and registration phases. The smartphone model that exhibited diverse behaviors in both runs was the Huawei P Smart DS.

C. SCAN QUALITY AND MATCH SCORE (RQ2)

We noted an increase in achieving a true match in the BOZORTH3 tool from 19% (N = 41) participants in the first run to 76% (N = 113) in the second run. However, we only measured the quality and match score of all attempts in the second run.

In the linear regression, it is expected that NFIQ-G and NFIQ-C are quality measures used to evaluate genuine finger and counterfeit scans, respectively. We found a relationship between the quality of scans and the match scores. The model explains approximately 14.8% of the variation in the match scores, indicating that other factors not accounted for in the model may also influence the match scores (F = 0.531, $p < 0.001$, R^2 = 0.148). The k coefficients for NFIQ-G and NFIQ-C are -0.6255 and -2.8284, respectively. These coefficients represent the estimated changes in the match score for a one-unit increase in the corresponding NFIQ measure while holding other variables constant. The standard errors of these coefficients (0.038 for NFIQ-G and 0.028 for NFIQ-C) indicate the precision of the estimates. The results suggest that both NFIQ-G and NFIQ-C have statistically significant relationships with the match scores, meaning that changes in the quality of scans are associated with changes in the match scores.

To analyze the impact of scan quality further, we explored different combinations of enhanced scans of genuine fingers (further referred to as EG) and enhanced counterfeit scans (further referred to as EC). Raw (non-enhanced scans) are further referred to as RG for genuine fingers and RC for counterfeits. Table 5 contains the average match scores for these combinations, indicating that EG and EC have the highest average match scores.

To compare the score distribution of the match score between the groups, a Kruskal Wallis test was applied for each category, and the results are as follows: match score is not affected by RG and RC ($H(4) = 5.97, p = 0.113$) or by RG and EC ($H(4) = 4.44, p = 0.217$). The match score is affected by EG and EC ($H(4) = 34.62, p < 0.001$), and by EG and RC ($H(4) = 8.88, p = 0.030$).

Regarding enhanced scans of genuine fingertips and enhanced scans of counterfeits, the Mann-Whitney test revealed a significant difference between EG with good quality (2, further referred to as EG2) – EC2 and EG with best quality (1, further referred to as EG1) – EC2 ($U = 249.5, p < 0.001$) as well as between EG2 – EC2 and EG1 – EC1 ($U = 24.0, p = 0.015$). Additionally, a highly significant difference was observed between EG2 – EC1 and EG1 – EC2 ($U = 11.5, p < 0.001$) and a significant difference between EG2 – EC1 and EG1 – EC1 ($U = 0.0, p = 0.011$). Regarding enhanced scans of genuine (EG) and raw counterfeits (RC), there is a significant difference in the matching score between EG2 – RC with bad quality (4, further referred to as RC4) ($U = 108.5, p = 0.014$) and EG1 – RC4 ($U = 51.0, p = 0.033$) differ significantly from the EG2 – RC with medium quality (3, further referred to as RC3) (see Table 6 for more details).

D. PERCEPTION (RQ3)

First, we separately compared the possible differences in perception before and after the simulation for each run with the Wilcoxon signed-rank test. Then, the differences between each run for the effect of the forgery simulation were compared. Next, we compared the variables measured before the forgery simulation in both runs to assess the population's perception change before the simulation due to other factors outside of this study (with the Mann-Whitney test). Results in Table 7 present the two-year observations, where the following could occur:

TABLE 4. Locations and types of fingerprint readers divided by groups 1 and 2 (login and registration).

		No division		$GLog_1$		$GLog_2$		$GReg_1$		$GReg_2$	
		2022	2023	2022	2023	2022	2023	2022	2023	2022	2023
	Sensor	N %*	N %*	N %*	N %*	N %*	N %*	N %*	N %*	N %*	N %*
Type	Capacitive	154 70	96 64	1 100	0 0	55 60	9 31	29 50	6 35	35 76	7 35
	Optical	52 23	44 32	0 0	4 100	24 26	18 62	20 35	10 58	7 15	12 60
	Ultrasonic	15 6	7 4	0 0	0 0	12 13	2 6	8 14	1 6	4 9	1 5
Location	Front	78 35	68 46	1 100	3 75	41 45	22 75	31 54	12 70	11 23	16 80
	Rear	133 60	53 36	0 0	0 0	43 47	4 13	23 40	2 12	30 65	3 15
	Side	10 4	26 17	0 0	1 25	7 7	3 10	3 5	3 18	5 10	1 5

*Percentage does not give always 100% due to rounding.

TABLE 5. Mean match scores based on combining genuine fingerprints and counterfeits (2023 only).

Combination	Mean	SD
Raw Genuine – Raw Counterfeit	23.73	7.05
Raw Genuine – Enhanced Counterfeit	28.86	6.71
Enhanced Genuine – Raw Counterfeit	25.70	5.54
Enhanced Genuine – Enhanced Counterfeit	33.39	7.97

TABLE 6. Mean match score (BOZORTH3) between scans of genuine fingertips and counterfeits (E = Enhanced, R = Raw) based on the quality assessment (1 = best, 2 = good, 3 = mean, 4 = bad, 5 = worst). "-" implies no matches. (2023 only.)

		Genuine					
		1		2		3	
		E	R	E	R	E	R
Counterfeit 1	E	M=27.67 SD=2.62	M=28.00 SD=0.00	M=39.57 SD=5.57	-	-	M=28.33 SD=5.60
	R	-	M=28.89 SD=6.31	-	-	-	-
Counterfeit 2	E	M=26.48 SD=5.36	-	M=35.94 SD=7.21	-	-	M=29.41 SD=6.85
	R	-	M=24.56 SD=4.90	-	-	-	-
Counterfeit 3	E	-	-	-	-	-	-
	R	M=20.00 SD=2.16	M=25.00 SD=0.00	M=21.14 SD=4.39	-	-	M=21.33 SD=5.03
Counterfeit 4	E	-	-	-	-	-	-
	R	M=25.48 SD=4.64	-	M=26.57 SD=5.69	-	-	M=23.41 SD=7.09

- no difference found between runs, so the results correspond with expectations (further referred to as *correspondence*),
- difference between runs based on our expectations due to a change (intervention) of the process (*shift*),
- and the unexpected difference between runs (*difference*).

1) Intention to use

Participants differed in their intention to use fingerprint authentication after the forgery simulation (*correspondence*) – they intended to use fingerprint authentication less often for logging into mobile banking and confirming transactions in mobile banking.

2) Perceived security

Participants' perceptions of fingerprint security after the forgery simulation differ – the expected shift to perceiving fingerprint authentication as less secure after the simulation was observed only in the first run (*difference*). They expected to perceive fingerprint security as less secure after the simulation by the IT security experts only in the first run and by the general public in only the second run (*difference*). When considering only the perception before the simulation (''initial'' values) in both runs, participants of the second run expected IT security experts to perceive fingerprints as less secure than a year before (U = 11191.5, $p < 0.001$).

Concerning IT security experts vs general public, participants expected that the general audience would perceive fingerprint authentication as more secure than IT security experts (2022: T_{before} = 292.5, $p_{before} < 0.001$, T_{after} = 54, $p_{after} < 0.001$, 2023: T_{before} = 217.5, $p_{before} < 0.001$, T_{after} = 306, $p_{after} < 0.001$), (*correspondence*).

3) Perceived susceptibility

Participants were less susceptible after the forgery simulation than before (*correspondence*). Also, they were slightly more susceptible before the simulation in the first run than in the second one (U = 12504, $p = 0.007$).

4) Forgery perception

Participants perceived fingerprint forgery as easier to learn after the simulation (*correspondence*). Before the changes made to the process, participants perceived fingerprint forgery as easier (but still slightly hard) (*difference*) and expected more advanced attackers (but still somewhat competent) to create a counterfeit before experiencing the simulation than after (*difference*). Also, participants initially expected less experienced attackers to be successful in forgery in the second run (U = 13306, $p = 0.018$).

5) Forgery evaluation/reflection

Regarding satisfaction, participants were more satisfied with their counterfeit (*shift*) and perceived the shorter time needed to create it after the changes made to the procedure (*shift*). There was no difference in effort perception of forgery (*correspondence*).

Possible differences in perception between successful and unsuccessful groups for each run after the forgery simu-

TABLE 7. Median ($\tilde{x}$) results of perception changes in years 2022 and 2023 and statistics for differences between both years (results of Mann-Whitney test in *Difference* column).

	2022 [12]		2023		
Variable	Before	After	Before	After	Difference
Unlocking smartphone	$\tilde{x}$=5	$\tilde{x}$=5	$\tilde{x}$=5	$\tilde{x}$=5	U=14002
	$p = 0.021$		$p = 0.099$		$p = 0.661$
Login into banking	$\tilde{x}$=4	$\tilde{x}$=3.5	$\tilde{x}$=4	$\tilde{x}$=4	U=12764.5
	$p < 0.001$		$p < 0.001$		$p = 0.140$
Transactions in banking	$\tilde{x}$=4	$\tilde{x}$=3	$\tilde{x}$=4	$\tilde{x}$=3	U=12918
	$p < 0.001$		$p < 0.001$		$p = 0.309$
Fingerprint security	$\tilde{x}$=4	$\tilde{x}$=3	$\tilde{x}$=4	$\tilde{x}$=4	U=12317
perception	$p < 0.001$		$p = 0.604$		$p < 0.001$
Expected fingerprint security	$\tilde{x}$=3	$\tilde{x}$=2	$\tilde{x}$=2	$\tilde{x}$=2	U=10235.5
perception by security experts	$p < 0.001$		$p = 0.259$		$p < 0.001$
Expected fingerprint security	$\tilde{x}$=4	$\tilde{x}$=4	$\tilde{x}$=4	$\tilde{x}$=4	U=16288
perception by general public	$p = 0.544$		$p = 0.008$		$p = 0.006$
Perceived susceptibility	$\tilde{x}$=3	$\tilde{x}$=2.7	$\tilde{x}$=2.7	$\tilde{x}$=2.3	U=10294.5
	$p < 0.001$		$p < 0.001$		$p = 0.245$
Forgery perception	$\tilde{x}$=3	$\tilde{x}$=2	$\tilde{x}$=3	$\tilde{x}$=2	U=12758.5
– easy/hard to learn	$p < 0.001$		$p < 0.001$		$p = 0.204$
Forgery perception	$\tilde{x}$=3	$\tilde{x}$=4	$\tilde{x}$=3	$\tilde{x}$=3	U=15919
– easy/hard to perform	$p = 0.022$		$p = 0.569$		$p = 0.023$
Attacker level	$\tilde{x}$=3	$\tilde{x}$=3	$\tilde{x}$=3	$\tilde{x}$=3	U=11911.5
	$p < 0.001$		$p = 0.583$		$p = 0.003$
Satisfaction with counterfeit		$\tilde{x}$=3		$\tilde{x}$=3	H(1)=20.473
					$p < 0.001$
Time perception of forgery		$\tilde{x}$=3		$\tilde{x}$=2	H(1)=26.860
					$p < 0.001$
Effort perception of forgery		$\tilde{x}$=3		$\tilde{x}$=3	H(1)=3.386
					$p = 0.066$

*Statistics for the Wilcoxon signed-rank test for the first run are provided in [12] and for the second run in Supplementary materials.

lation were compared. Participants considered a successful group for perception analysis achieved a true match (in BOZORTH3) or registered their counterfeit into the smartphone or unlocked a smartphone with their counterfeit. In the first run, there were 89 successful participants, and the number increased to 116 in the second run. All observations were consistent in no change of perception based on their achievement (*correspondence*) except one: successful participants also perceived less effort needed to create counterfeits when the forgery process was already simplified (*shift*). The only consistent difference in perception was that the successful group was satisfied with their counterfeits more than the unsuccessful group (*correspondence*). During the simulation run with more successful participants, these successful ones were even more satisfied with their counterfeits (see Supplementary materials).

V. DISCUSSION AND IMPLICATIONS

This section provides a discussion of our results in the three areas. Firstly, observations regarding behavior of various smartphone fingerprint readers are discussed. Subsequently, the focus shifts to the quality of scans. Lastly, user perception regarding the forgery process and fingerprint security is considered.

A. FINGERPRINT READERS (RQ1)

During the two-year observations, five participants in total were able to log into a smartphone with their counterfeits. This demonstrates that it is possible to create a high-quality counterfeit from a finger-photo taken by a standard camera and done even by inexperienced impostors, which is effective on some current smartphones. However, we do not consider this a high-level risk because of the low success rate of inexperienced impostors. On the other hand, this also shows that this is a real risk considering motivated and expert imposters and professionally taken photos including detail on a fingertip, with expert-made molds and cast fingertip counterfeits.

Even though our inexperienced imposters usually did not achieve counterfeits of such quality to be recognized as registered genuine fingers, our results demonstrate that current smartphone fingerprint readers often recognize the counterfeit as a human finger because around 20% of the participants were able to register their counterfeits as a ''finger'' into their smartphones. This leads to questioning security of smartphone fingerprint sensors since manufacturers do not publish technical details about the sensors they use.

Fewer participants could register their counterfeit as a ''finger'' into a smartphone in the second run, which could be because of different materials used for counterfeits (glue in the first run, silicone in the second run). In the second run, it was observed that optical fingerprint sensors had a slightly higher vulnerability rate in contrast to capacitive sensors which was found as the most vulnerable in the first run. Capacitive and ultrasonic sensors are typically more secure than optical ones since they capture more detailed fingerprint data [13]. However, we found some successful registrations of counterfeit smartphones with capacitive readers even though silicon usually seems not to be working on them [9].

Furthermore, we achieved a higher success rate after logging in with counterfeits after registering them as new fingers. Around 67% of participants in the first run and 83% in the second run were able to login with their counterfeit after registration as a genuine finger. This demonstrates that the counterfeits were realistic enough to be identified as human fingers but not accurate enough to match registered genuine fingers. The performance of a fingerprint reader can be affected by its size, which can impact accuracy and convenience.

Over the years, some participants' smartphones demonstrated conflicting behavior for the same model. The reasons could be (a) environmental conditions (i.e., humidity or temperature) affecting the sensors' detection and registration of counterfeits and (b) defects or variations in the fingerprint sensor – even if the same smartphone model, there may be defects or variations in the fingerprint sensor. There could be a discrepancy in the characteristics or calibration of the sensor between group cases, affecting its ability to detect and register counterfeits. Also, differences in manufacturing or updates to the production process can cause variations in smartphones' hardware or software configurations from different batches. This can result in differences in how the touch input is responded to, such as differences in the touch screen's sensitivity or the fingerprint reader's accuracy.

It is essential that the fingerprint reader is tightly integrated into the device security framework. Manufacturers should

also provide software updates regularly to fix any security vulnerabilities that may be discovered in the reader or related software. The security of the fingerprint authentication also depends on the user's behavior. Educating users on best practices for fingerprint security, such as not sharing their finger-photos, regularly cleaning the sensor, and setting strong backup authentication methods, can ultimately improve the security of the device.

B. SCAN QUALITY AND MATCH SCORE (RQ2)

Our results demonstrate that it is possible to create fingertip patterns from a finger-photo of good quality. We found that the match score is affected by the quality of scans, suggesting that the quality plays a non-negligible role in affecting the accuracy of the matching process. Enhanced scans of genuine fingertips and enhanced scans of counterfeits combination achieved the highest mean score. Even though some information was lost while taking a finger-photo and during the papillary line extraction on a computer, the enhancement can improve the scan when the counterfeit is of good quality.

It is challenging to make a counterfeit of good quality from the whole photographed fingertip, so only a part of a counterfeit corresponds to the genuine fingertip [20]. However, this can simulate partial scanning on smartphones, even though scans are processed via an external reader on a computer with NBIS tools.

Good quality finger-photo is a core part of the overall process [29]. The group achieving a true match probably had better finger-photos than the unsuccessful group. We leave it to future work to investigate the differences between finger-photos and successful and unsuccessful groups since we did not have finger-photos of our participants to conduct such an analysis due to ethical constraints. Taking a good quality finger-photo was a challenging part of the process, which may not be affected by the actions of participants – e.g., if participants did not have very nicely visible ridges on their fingers [18], had destroyed fingerprints because of skin disease [14], or had a worse smartphone camera for taking finger-photos. Since our participants employed various devices to capture images of their fingers, we cannot offer consistent suggestions regarding lighting. We observed that certain participants obtained superior finger-photos when using our photography environment, while others achieved better results with the flash feature on their devices. However, in a real-life scenario, an attacker has no control over the finger-photo quality – the photo, including detailed information about the fingertip, is published online and may have been taken professionally with high-quality equipment.

Finally, participants experienced a big increase in achieving a true match between runs (19% $\rightarrow$ 76%). This could be affected by scanning genuine fingers and counterfeits ten times each during the second run in contrast to the first run, where participants processed only (usually) one scan for genuine fingers and one for counterfeits. Also, there were no issues with size estimation as before, which could also contribute to a higher success rate of participants in the second run.

C. PERCEPTION (RQ3)

Results show that not all perceptions changed consistently in both runs. We consider results marked as *correspondence* or *shift* for fundamental differences based on forgery simulation. We provide only hypothetical explanations for results marked as *difference*, so more focus should be on this in future work.

Intention to use: The results on the intention to use fingerprint authentication less often after the forgery simulation for unlocking a smartphone, login into banking, and transaction confirmation are consistent (*correspondence*). However, participants reported lower intent to use fingerprint authentication after the simulation in the first run but not in the second run for unlocking smartphones. Nevertheless, even in the previous run, the effect was weak. Weaker results regarding unlocking smartphones, in contrast to banking-related actions, reflect that users prioritize their accounts. Users are looking for some balance between usability and security [32], so they care to use more secure authentication methods for more sensitive services such as mobile banking.

Perceived security: No consistent shift in fingerprint security perception was observed in participants themselves or their expected perception shift of the general public and IT security professionals in the second run (*difference*). Even though the initial security perception of fingerprint authentication was the same in both runs, the fingerprint was perceived as less secure after the forgery simulation only in the first run. It could be due to the lecture modification between runs, which placed more emphasis on fingerprint insecurity in the second run. Participants expected that IT security experts would perceive fingerprints as less secure than in the first run. This explains why the expectation of IT security experts' perception of fingerprint security shifted in the first run but not in the second one. The expectation that the general public perceives fingerprints as less secure than IT security experts, which aligns with [32], was consistent across both runs.

Also, the forgery simulation ran in 2022 for the first time, so participants had no information about what to expect from resources other than lecturers and seminar tutors. In the second run, participants could get some information from their schoolmates who had already taken this course the previous year.

Smartphone manufacturers integrating fingerprint readers into their models can influence participants' security perceptions. Since fingerprint readers have been in smartphones more often recently and manufacturers responsible for them integrate the reader there, the users believe it is secure.

Although the success rate was higher in the second run, our simulation did not shift participants' security perception of fingerprint security in the second run. Success in registering their counterfeits into smartphones or achieving a true match does not affect security perception, which was a consistent result for both runs (*correspondence*). On the other hand, our participants' lack of security perception change may be

caused by an inability to log into smartphones with their counterfeit. Only 3% of our participants could log into a smartphone with their counterfeits in the second run. So, most successful cases were registering their counterfeit into smartphones or achieving a true match in BOZORTH3. Since we do not expect our participants to use the BOZORTH3 tool in real life and it is necessary to have authorized access to register counterfeit into the smartphones, these risks could be perceived as irrelevant.

Perceived susceptibility: Perception shift was consistent regarding lower susceptibility after the forgery simulation in both runs (*correspondence*). As explained above, participants could mostly not log in with their counterfeit into a smartphone, so they could not ''perceive the risk as very probable'' [12, p. 6]. However, participants were less susceptible in the second run than in the first one.

Forgery perception: Regarding forgery perception, participants consistently perceived forgery as easier to learn after the simulation than before (*correspondence*). However, in the second run, participants expected forgery to be as hard to perform before as after the simulation and expected competent attackers to be able to do forgery regardless of the simulation (*difference*). Since we simplified the process in several areas the current form of the simulation reflected participants' expectations.

Also, there were struggles with size estimation in the previous run [12], resulting in possible issues related to improper size scaling. Since seminar tutors explained the issue of size estimation to the participants, this might have resulted in different expectations and consequent perceptions based on the accuracy of the scaling. Most of the participants whose smartphones detected that the counterfeits were touching the sensor could be expected to log into smartphones with their counterfeits when having the correct size. Since there were no issues with size estimation in the second run, some participants interpreted their inability to log in with their counterfeits as they did high-quality ones, but smartphone fingerprint readers had liveness detection. However, smartphones do not detect a ''finger'' in most cases because of the type of contact. For example, in the case of capacitive readers, a conductive material (not silicone-based) is needed. When using a capacitive ink for a counterfeit, such an artifact would work on capacitive readers [8], [45].

Since participants saw during the simulation that the forgery was ineffective for logging into a smartphone, that could increase their trust in fingerprint security because they did not consider other threats related to fingerprint authentication [12].

Forgery evaluation/reflection: Since more participants achieved true match in BOZORTH3 in the second run, they were also more satisfied with their counterfeits than in the first run (*shift*). However, their satisfaction with counterfeits was still relatively moderate. Also, participants perceived the time needed to create counterfeits as shorter in the second run (*shift*), which reflects that the simulation was shortened from two seminars to one even though the participants knew about this change. However, the effort was perceived as similar in both runs (*correspondence*). That could be since participants still had to do all the steps needed to complete the forgery process, so even though it was easier to perform, the effort required to conduct it was still relatively low.

VI. CONCLUSIONS

We demonstrated the feasibility of fingerprint spoofing: a hands-on fingerprint forgery simulation from a finger-photo could be performed within two hours by inexperienced impostors without any professional equipment. To show how real is the risk of such spoofing, we investigated a success rate (1) for computer processing in NBIS tools (a true match) and (2) on smartphones (login with counterfeit and counterfeit registration as a new ''finger''). In contrast to the first run, we achieved a higher success rate in both scenarios: (1) more participants achieved true match on a computer (19% $\rightarrow$ 76%), and (2) more participants were able to login with their counterfeit into a smartphone (0.5% $\rightarrow$ 3%). However, fewer participants were able to register their counterfeit into a smartphone (26% $\rightarrow$ 11%), and nearly half of the smartphones did not recognize that not a finger but a counterfeit was touching the sensor. This points out the inability of current smartphone fingerprint readers to recognize counterfeit items from a human finger. Since a few inexperienced impostors could create a first-ever-made counterfeit from a finger-photo from a standard camera that unlocked a smartphone, the risk is real (mostly to the optical scanners when using glue or silicone for a cast), but currently not high-risk level.

Quality plays an important role during the forgery process – from the quality of a finger-photo to the quality of scans of genuine fingers and counterfeits. We demonstrated that it is possible to achieve sufficient quality counterfeits. Since some information is lost during the forgery process (when taking a finger-photo, papillary line extraction, and printing on the foil), the most effective combination regarding match score is a high-quality counterfeit enhanced scan and a little bit lower-quality genuine finger-enhanced scan.

Regarding the perceptions, participants reported an intention to use fingerprint authentication less often for banking-related operations, regardless of their achievements in fingerprint reader fooling. However, we identified mixed results regarding the perception of fingerprint authentication security before and after the forgery simulation. We leave the investigation of this for future work.

REFERENCES

[1] Duo, ''The 2021 duo trusted access report,'' tech. rep., 2022.
[2] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, ''End-users' knowledge and perception about security of clinical mobile health apps: A case study with two saudi arabian mhealth providers,'' *Journal of Systems and Software*, vol. 195, p. 111519, 2023.
[3] A. Kruzikova, L. Knapova, D. Smahel, L. Dedkova, and V. Matyas, ''Usable and secure? user perception of four authentication methods for mobile banking,'' *Comput. Secur.*, vol. 115, apr 2022.
[4] Statista, ''Biometric usage worldwide in 2021, by type,'' 2022.
[5] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. Cranor, and M. Savvides, ''Biometric authentication on iphone and android: Usability, percep-

tions, and influences on adoption," in *Workshop on Usable Security*, 01 2015.

[6] L. Lassak, A. Hildebrandt, M. Golla, and B. Ur, ""it's stored, hopefully, on an encrypted server": Mitigating users' misconceptions about fido2 biometric webauthn," in *USENIX Security Symposium*, 2021.

[7] A. Patrick, A. Burris, S. Das, and N. Noah, "Understanding user perspective in a university setting to improve biometric authentication adoption," in *Proceedings of the 9th Mexican International Conference on Human-Computer Interaction*, MexIHC '22, (New York, NY, USA), ACM, 2022.

[8] K. Cao and A. K. Jain, "Hacking mobile phones using 2 d printed fingerprints," tech. rep., Michigan State University, 2016.

[9] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Comput. Surv.*, vol. 47, nov 2014.

[10] H. Lee, S. Kim, and T. Kwon, "Here is your fingerprint! actual risk versus user perception of latent fingerprints and smudges remaining on smartphones," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, ACSAC '17, (New York, NY, USA), p. 512–527, ACM, 2017.

[11] A. Roy, N. Memon, and A. Ross, "Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2013–2025, 2017.

[12] A. Kruzikova and V. Matyas, "Fingerprint forgery training: Easy to learn, hard to perform," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, (New York, NY, USA), ACM, 2023.

[13] A. Jahan, J. Banks, and V. Chandran, "Fingerprint systems: Sensors, image acquisition, interoperability and challenges," *Sensors*, vol. 23, no. 14, 2023.

[14] M. Drahansky, M. Dolezel, J. Urbanek, E. Brezinova, and T.-h. Kim, "Influence of skin diseases on fingerprint recognition," *Journal of biomedicine & biotechnology*, vol. 2012, p. 626148, 05 2012.

[15] C. K. Lee, C. C. Chang, A. Johar, O. Puwira, and B. Roshidah, "Fingerprint changes and verification failure among patients with hand dermatitis," *JAMA Dermatology*, vol. 149, pp. 294–299, 03 2013.

[16] R. B. Steele, J. S. Taylor, and S. Aneja, *Skin Disorders in Athletes: Professional and Recreational Sports*, pp. 1–23. Cham: Springer International Publishing, 2018.

[17] J. Emer, R. Sivek, and B. Marciniak, "Sports dermatology: Part 1 of 2 traumatic or mechanical injuries, inflammatory conditions, and exacerbations of pre-existing conditions," *The Journal of clinical and aesthetic dermatology*, vol. 8, pp. 31–43, 04 2015.

[18] S. Sharma, R. Shrestha, K. Krishan, and T. Kanchan, "Sex estimation from fingerprint ridge density. a review of literature," *Acta bio-medica Atenei Parmensis*, vol. 92, p. e2021366, 11 2021.

[19] A. Sankaran, A. Malhotra, A. Mittal, M. Vatsa, and R. Singh, "On smartphone camera based fingerphoto authentication," in *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–7, 2015.

[20] C. Lee, S. Lee, J. Kim, and S.-J. Kim, "Preprocessing of a fingerprint image captured with a mobile camera," in *Advances in Biometrics* (D. Zhang and A. K. Jain, eds.), (Berlin, Heidelberg), pp. 348–355, Springer Berlin Heidelberg, 2005.

[21] A. Dabouei, S. Soleymani, J. Dawson, and N. M. Nasrabadi, "Deep contactless fingerprint unwarping," in *2019 International Conference on Biometrics (ICB)*, pp. 1–8, 2019.

[22] P. Wild, F. Daubner, H. Penz, and G. F. Domínguez, "Comparative test of smartphone finger photo vs. touch-based cross-sensor fingerprint recognition," in *2019 7th International Workshop on Biometrics and Forensics (IWBF)*, pp. 1–6, 2019.

[23] C. Lin and A. Kumar, "Matching contactless and contact-based conventional fingerprint images for biometrics identification," *IEEE Transactions on Image Processing*, vol. 27, no. 4, pp. 2008–2021, 2018.

[24] R. Carvalho and N. Tihanyi, "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)*, pp. 1–6, 2021.

[25] P. Burton, K. Cook, R. Kelley, J. Ivy, and K. Thomas, "Fingerprint spoofing: Exploring cybersecurity with limited technology," *Connected Science Learning*, vol. 4, no. 6, 2022.

[26] I. Goicoechea-Telleria, A. Garcia-Peral, A. Husseis, and R. Sanchez-Reillo, "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)*, pp. 1–5, 2018.

[27] R. Casula, G. Orrù, D. Angioni, X. Feng, G. L. Marcialis, and F. Roli, "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)*, pp. 3412–3418, 2021.

[28] R. Casula, M. Micheletto, G. Orrú, G. L. Marcialis, and F. Roli, "Towards realistic fingerprint presentation attacks: The screenspoof method," *Pattern Recognition Letters*, 2022.

[29] T. Ogane and I. Echizen, "Biometric jammer: Preventing surreptitious fingerprint photography without inconveniencing users," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 253–260, 2017.

[30] O. Buckley and J. R. Nurse, "The language of biometrics: Analysing public perceptions," *Journal of Information Security and Applications*, vol. 47, pp. 112–119, 2019.

[31] V. Zimmermann and N. Gerber, "The password is dead, long live the password – a laboratory study on user perceptions of authentication schemes," *International Journal of Human-Computer Studies*, vol. 133, pp. 26–44, 2020.

[32] F. Wolf, R. Kuber, and A. J. Aviv, ""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*, CHI '19, (New York, NY, USA), p. 1–12, ACM, 2019.

[33] E. Marasco, M. Albanese, V. V. R. Patibandla, A. Vurity, and S. S. Sriram, "Biometric multi-factor authentication: On the usability of the fingerpin scheme," *Security and Privacy*, vol. 6, no. 1, p. e261, 2023.

[34] T. Habibu, E. T. Luhanga, and A. E. Sam, "Assessment of how users perceive the usage of biometric technology applications," in *Recent Advances in Biometrics* (M. Sarfraz, ed.), ch. 3, Rijeka: IntechOpen, 2022.

[35] S. Hadzidedic, S. Fajardo-Flores, and B. Ramic-Brkic, "User perceptions and use of authentication methods: insights from youth in mexico and bosnia and herzegovina," *Information & Computer Security*, vol. ahead-of-print, 03 2022.

[36] D. Votipka, E. Zhang, and M. L. Mazurek, "Hacked: A pedagogical analysis of online vulnerability discovery exercises," in *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 1268–1285, 2021.

[37] V. Zimmermann and K. Renaud, "The nudge puzzle: Matching nudge interventions to cybersecurity decisions," *ACM Trans. Comput.-Hum. Interact.*, vol. 28, jan 2021.

[38] J. Mirkovic, M. Dark, W. Du, G. Vigna, and T. Denning, "Evaluating cybersecurity education interventions: Three case studies," *IEEE Security & Privacy*, vol. 13, no. 3, pp. 63–69, 2015.

[39] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, jun 2010.

[40] V. Švábenský, J. Vykopal, and P. Čeleda, "What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, SIGCSE '20, (New York, NY, USA), p. 2–8, ACM, 2020.

[41] V. Mdunyelwa, L. Futcher, and J. van Niekerk, "An educational intervention for teaching secure coding practices," in *Information Security Education. Education in Proactive Information Security* (L. Drevin and M. Theocharidou, eds.), (Cham), pp. 3–15, Springer International Publishing, 2019.

[42] D. Xiujuan and J. Zhigang, "Using achievement-based teaching interventions in network security course," in *2008 International Conference on Computer Science and Software Engineering*, vol. 5, pp. 129–132, 2008.

[43] J. Petelka, M. Finn, F. Roesner, and K. Shilton, "Principles matter: Integrating an ethics intervention into a computer security course," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1*, SIGCSE 2022, (New York, NY, USA), p. 474–480, ACM, 2022.

[44] NIST, "Nist biometric image software (nbis)." https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis, 2022. Online; accessed August 2, 2023.

[45] M. Peidro-Paredes, J. M. De Fuentes, L. González-Manzano, and M. Velasco-Gomez, "Characterizing the masterprint threat on android devices with capacitive sensors," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, (New York, NY, USA), ACM, 2023.

[46] "Utkarsh-deshmukh / fingerprint-enhancement-python." https://github.com/Utkarsh-Deshmukh/Fingerprint-Enhancement-Python, 2022. Online: accessed August 2, 2023.

[47] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777–789, 1998.

[48] NIST, "Biometric quality." https://www.nist.gov/programs-projects/biometric-quality. Online; accessed August 8, 2023.
[49] T. Kluyver, B. Ragan-Kelley, F. Pérez, B. Granger, M. Bussonnier, J. Frederic, K. Kelley, J. Hamrick, J. Grout, S. Corlay, P. Ivanov, D. Avila, S. Abdalla, C. Willing, and J. development team, "Jupyter notebooks? a publishing format for reproducible computational workflows," in *Positioning and Power in Academic Publishing: Players, Agents and Agendas* (F. Loizides and B. Scmidt, eds.), pp. 87–90, IOS Press, 2016.
[50] "Utkarsh-deshmukh / kruskal wallis scipy python." "https://docs.scipy.org/doc/scipy/reference/generate/scipy.stats.kruskal.html". Online; accessed August 8, 2023.
[51] "IBM SPSS Statistics for Windows, Version 27.0. Armonk," 2020.

ACKNOWLEDGMENT

We thank Karel Stepka from the CBIA lab at the FI MUNI for the photo processing script. We also thank students for their participation and seminar tutors for their help with realization. Agata Kruzikova was supported by Red Hat Czech. ChatGPT was used to polish some sentences.

AGATA KRUZIKOVA is a PhD candidate in the Centre for Research on Cryptography and Security at the Faculty of Informatics at Masaryk University, Brno, Czech Republic. She researches authentication with respect to both end-users and IT professionals in the field of usable security, often in collaboration with commercial companies.

ALESSIA MICHELA DI CAMPI Web Developer, Software Programmer, and currently a dedicated PhD Candidate in Authentication Security and Usability.

VASHEK MATYAS is a Professor at the Centre for Research on Cryptography and Security at the Faculty of Informatics at Masaryk University, Brno, Czech Republic. He researches usable security with respect to both end-users and advanced users, biometric authentication systems, outputs of crypto primitives, and the security of wireless sensor networks.

TOMAS CERNY is an Associate Professor of Systems and Industrial Engineering at the University of Arizona, Tucson. After earning Engineering and Masters's degrees from the Czech Technical University, FEE, and from Baylor University, he has served as an Assistant professor at the Science and Computer Department at the Czech Technical University, FEE since 2009. Soon after earning a Doctoral degree in 2016, he returned to Baylor University to join the Computer Science department. He was tenured in 2023 at Baylor and moved as Associate Professor of Systems and Industrial Engineering at the University of Arizona. His research focus is Software Engineering, Static Analysis, Cloud Computing Applications nd Architecture Degradation. He served 15+ years as the lead developer of the International Collegiate Programming Contest Management System. He authored nearly 200 publications, mostly relating to code analysis and aspect-oriented programming. Among his awards are the seven best papers, the 2023 Baylor Scholarship Award, the Outstanding Service Award ACM SIGAPP 2018 and 2015, and the 2011 ICPC Joseph S. DeBlasi Outstanding Contribution Award. He actively serves the scientific community and was on the organizing committee for IEEE SOSE, ESOCC, SANER, ACM SAC, ACM RACS, and ICITCS.