Challenging USB fingerprint scanner security protocol: a methodology using casting agents to capture digit and latent ridge detail to enable access

Samuel McKenna and Mark Butler*

School of Science and Engineering,
Teesside University,
Middlesbrough, TS1 3BA, UK
Email: M2160163@tees.ac.uk
Email: M.Butler@tees.ac.uk
*Corresponding author

Abstract: Fingerprint scanners are used as a form of control with access limited to the beholder of the ridge detail. However, to what extent these devices are capable of providing that control has not been fully explored. This study tested the reliability of a fingerprint scanner in accessing enrolled fingerprint data, when faced with the challenge of fake fingerprints. Ridge detail casts were crafted from moulds, with gelatine and silicone being applied as casting agents. The second stage required participants to place fingerprints on a bottle or tile; these latent impressions were subsequently powdered using Magneta Flake. Provil, a forensic casting material was applied directly onto the powder, creating simulated fingerprints from a latent print. Each of the produced fingerprints then went through a scanning process. All materials tested were able to gain access through the participants' enrolled data. This suggests potential unreliability of the fingerprint scanner in storing pertinent data.

Keywords: biometrics; fingerprints; scanner; cyber; crime; fingerprint data; identification; digital; verification; theft; cryptography; security; hacking.

Reference to this paper should be made as follows: McKenna, S. and Butler, M. (xxxx) 'Challenging USB fingerprint scanner security protocol: a methodology using casting agents to capture digit and latent ridge detail to enable access', *Int. J. Biometrics*, Vol. X, No. Y, pp.xxx–xxx.

Biographical notes: Samuel McKenna is a BSc (Hons) graduate in Crime Scene Science. His work experience is in the field of mobile communication retail and business audits.

Mark Butler is a Senior Lecturer in Crime Scene Science at the Teesside University. He is a former Crime Scene Investigator and National Instructor. He obtained his BSc (Hons) in 1995, MSc in 2007, PhD in 2014. His research interests are in crime scene performance and intelligence analysis.

1 Introduction

With ever-increasing technological capabilities and a shift to a digital world, the need to protect individual security online has become essential. Identifying individuals from their fingerprints has been a work-stream of law enforcement agents for over a hundred years; however, this capability has evolved and migrated into other areas of security. The possibility to digitise fingerprints has resulted in a spread of this technology, for use by anyone with a desire to restrict access to digital devices (Sten et al., 2003). The use of fingerprints (ridge detail) as a method to successfully identify an individual forms just one part of biometrics, however, it is argued as being the most common (Uz et al., 2009). Its presence within the global market has seen significant growth within the last decade, highlighting its importance (PR Newswire, 2014). This popularity is largely based on fingerprints uniqueness, with not one holding the same ridge detail as another (Wang and Bhanu, 2007).

Biometric tools can be classified under two wide categories, physiological and behavioural. Physiological characteristics are unchanging physical features such as fingerprints, retinal, pattern or facial features. Behavioural characteristics pertain to a person's psychological standing and are subject to changes as a consequence of environmental factors on the body. These include ailments such as stress or illness (Jamieson et al., 2005).

Fingerprint scanners generally share a similar design, in that they contain a sensor which reads the fingerprint, converting this analogue data into a digital format utilising an analogue to digital (A/D) converter. This process is led by an interface module, which oversees the shift of data from the scanner itself into what is often a computer. The sensor is the most vital part of this process and comes in a number of forms. Optical sensors for example are popular and generally use light to make fingerprint ridges appear dark in order to gather their fine detail. Solid-state sensors use a number of small pixels and silicon surface on which the finger is placed. This type compares fingerprint images produced through either electrical charge or thermal recording of the print based on temperature. Ultrasound sensors examine the echo signals produced from ridge detail, creating a view of the fingerprint. Sweep sensors have come into place as a cheaper alternative; this type views and captures fingerprint sections, ultimately building a full finger view for identification (Maltoni et al., 2009).

Although still to be accepted by many, as industries have moved security to a virtual world consequently there has been a proliferation of biometric research (Mansfield-Devine, 2013). Some of these industries have adopted a return to existing methods of authentication, while others have explored fertile ground and created novel methods of verification using fingerprint scanners (Shrivastava and Srivastava, 2014). Ohana et al. (2013) provide an example of study which examined the growing use of biometrics within mobile technology. This is of particular significance as seen recently with the increase in biometric capabilities of cellular device such as the IPhone and its Touch ID technology (Goode, 2014). The findings from this study drew conclusions that the use of passwords and pins alone open devices up to greater vulnerability; offering an alternative choice of fingerprint biometrics provides a greater and alternative source of protection. The latter appears to be especially pertinent with the increasing use of such equipment. This study focuses solely on the use of mobile biometrics, whereas many consumers and industries do not utilise such forms of protection.

It is worth discussing at this juncture that fingerprint identification is perceived as being absolute, unquestionable and immune from persuasion. Dror and Mnookin (2010) scope the dangers of combining the work of automated fingerprint systems, evidencing that some bias exists by experts viewing fingerprints already run through automated platforms.

A shift to greater security can be said in large part, to have been stimulated by the ongoing threat of terrorism, and cyber-attacks, across the globe. A consequence of this has been an influx of biometric products for sale. The security concerns we occupy today were debated a decade ago with worldwide emphasis for officials to make steps to produce a biometric standard (Jamieson et al., 2005).

Research conducted into the use of biometrics has largely focused on the vulnerabilities of these products, with suggestions to improvements on the robustness of authentication processes (Nanni et al., 2015). Bowden-Peters et al. (2012) illuminate through use of live-detecting capacitive fingerprint scanners, the worrying ability to fool the biometric method through the manufacture of fake fingerprints. The fingerprints were created from clay moulds, acetate and PCB. Utilising polyvinyl acetate, silicone glue, silicone rubber, latex and fake skin, casts were created to act as imitation fingerprints. Interestingly, throughout each of the tests performed the chosen fingerprint scanner was fooled, allowing access by the newly created fake fingerprints. This finding remained true even with claims of liveness detection technology inbuilt in the scanner. It is clear that further work is needed to explore other ingredients in particular forensic casting agents and how well liveness detection is resisted. In addition to this is how well these materials are at capturing latent ridge detail marks, where the digit and casting agent do not need to come together for generating moulds.

Results from Bowden-Peters et al. (2012) align closely with Tan and Schuckers (2010) concerning the spoofing of fingerprints on fingerprint scanners. The approach here was to test the validity of a created anti-spoofing method based on fusing ridge signal and valley noise. This area of research builds towards potential industry standards that new devices would need to meet should they seek validation or accreditation. It is in this research vein that the first and second author feel that forensic casting agents in particular offer much to the community of practice regarding those concerned with spoof biometric fingerprint verification and validation. With further work proposed to explore the falsification of perspiration as an indicator of liveness (Parthasaradhi et al., 2005). These methods relied on using only one image as opposed to using two time-series images to highlight the ridge signal and valley noise produced by the moisture deposited by the perspiration of a dermal pore. Results indicated that the algorithms produced over a single image, combining ridge signal and valley noise, meant that an equal error rate (EER) of 0.9 was achieved. The EER conveys the rate when acceptance and rejections errors are equal in value. An EER of 0.9 indicates out of 100 individuals attempting to breach the fingerprint scanner less than one individual (0.9) can successfully gain access. This highlights a proven method of anti-spoofing in fingerprint scanners. Also of note is the use of a large dataset, wherein both live and spoof subjects were expected to complete a number of fingerprint scans; the increase of individuals in the dataset affords greater confidence. Although Parthasaradhi et al. (2005) aimed to test a new method for deterring spoof access; this initial outcome arguably cannot be used in high security scenarios simply because there is still the potential for access to pertinent information, albeit to a lesser degree. Its work, however, does improve on the study undertaken by

Bowden-Peters et al. (2012). This is evident through its creation of tried and tested software that can be used to develop a more secure and reliable fingerprint scanner. It does however connect with the study undertaken by Bowden-Peters et al. (2012), to develop a more secure and reliable fingerprint scanner by focusing on the software element of the device.

It is proposed that a wider engagement of materials used to capture ridge detail is necessary to determine those that are best suited to testing security and reliability against spoofing. To move beyond the mediums such as Play-Doh, gelatin and silicone as demonstrated by Tan and Schuckers (2010). This initial exploration was useful as it presents a landscape on products that are easily obtainable and could be defined as a rational choice for offenders.

The need to enhance the reliability of fingerprint technology on a wider scope is also an area for potential focus within the field of biometrics. This is evident through its growing use but its presence should never stand to replace the role of human experts in both confirming an identification and providing unbiased evidence in a court of law (Thompson et al., 2013). Furthermore, Haber and Haber (2014) indicated that whilst fingerprints have been used as evidence in criminal proceedings for over one hundred years, only in the last 20 has verification been implemented to test its reliability in the courtroom. As the use of digitised biometrics increases, both creators and users should remain wary of leaving a digital footprint that captures personal identification, since the potential for systems to be easily accessed by others is not only a reality but also requires little expertise. As the field expands, fingerprint experts should never depend wholly on results gained from automatic fingerprint recognition systems (AFRS), instead always confirming findings (Zhao et al., 2010). Although a separate issue it is recognised that since severe austerity measures within the UK policing, debates percolate on reducing secondary checks by recognising the computer database as an initial first check response. Dror and Mnookin (2010) concluded that even by using fingerprint identification systems, in this case AFIS (automatic fingerprint identification) opportunity existed for bias, as the generated 'possible' fingerprint matches are listed based on the number of points the identification assigns to each print. This, according to Dror and Mnookin (2010) is when bias may present itself, raising the question as to whether the experts view on the fingerprint is his or her own or whether is it based on the ranking provided by the fingerprint system? Subsequent research by Dror et al. (2012) found that examiners were affected by the location of prints from an automated fingerprint output, even to the extent to identifying incorrect fingerprints as matches when the correct fingerprint was present in the produced output list. Fingerprint identification has historically been seen as infallible, however an increasing number of studies have sought to test this theory and attempt to identify if and what error rates exist (Cole, 2005). Developing this further, a means to capture error rate of spoof fingerprints accessing devices is akin to a lock with published metrics of how long it can withstand damage from a variety of tools before access is gained. Being able to differentiate between fingerprint scanners and their ability to defend against spoofing should, it is argued, be made more transparent. In order to facilitate this demand, it is proposed research should continue to an end whereby a meta-analysis on what methods and materials should be used to form part of this testing process. This is of particular importance in line with the growing use of these devices; to be able to store fingerprint data in such a way that the systems on which they are integrated are robust enough to resist access, whilst still adhering to good ergonomic ubiquitous design (Furnell and Clarke, 2014).

2 Materials and methods

The following method outlines two approaches to spoofing a moderately priced fingerprint scanner. The first discusses moulds recording ridge detail taken directly from the digit. The second phase explores how some of these casting materials are sensitive enough to surface morphology that they are capable of recovering latent fingerprints after enhancement with Magneta Flake™ powder.

A pilot study, n = 5 participants were used, each agreeing to the ethical protocols of providing consent to allow capture of their ridge detail.

Two methods of fingerprint replication were used during the study to create spoof fingerprint ridge detail. The first was the manufacture of moulds directly from participants' fingerprints using two casting agents. The second and arguable the most controversial was the direct casting of participants' latent fingerprints. Since ridge detail characteristics are reported to be unique (Hsiao and Lee, 2015), it was explored whether the recovery of latent marks on surfaces could be used to gain access to the device.

Each participant provided two fingerprints each, to create two usable individual moulds (Tan and Schuckers, 2010). Ten moulds were created in total for use in the experimentation. The two materials were Play-Doh and Provil®. Provil is a trade name for a product that is often used as a forensic recovery agent of instrument marks at crime scenes [Pepper, (20100, p.60]. Its other uses include gathering dental impressions (Dentistry Today, 2010). Its chosen appeal is its sensitivity in being able to capture the microscopic striations left behind from an instrument after forced contact with a suitable surface. One kilogram of Play-Doh was chosen to create five of the ten moulds, one for each of the five participants. Play-Doh's properties enable it to be soft until hardened and contains a smooth surface. The fingerprints can be situated within the Play-Doh by each participant and remoulded several times if necessary, to gain the highest quality impression for each chosen finger. Participants placed their right index finger into a small circular ball of Play-Doh, with sufficient pressure to include the tip and down to the first flexure line. Once placed to an adequate depth, the finger was removed leaving behind an impression. The state of the impression at this juncture is that original ridges and furrows are reversed in the new medium.

Provil (vinyl polysiloxane) was then used to create another five of the ten moulds. This involved a 50 ml Provil Cartridge being loaded into a dispensing gun and applied directly onto the right hand index finger of each participant, enough to cover the fingertip. Prior to hardening, it was flattened with an acetate sheet leaving enough depth in the Provil to avoid damaging the ridge detail. Once dry, the acetate sheet was removed and the mould prepared for subsequent inspection. Moulds that had anomalies or damage were removed and new ones created prior to testing (Tan et al., 2010).

Each participant had two different moulding agents used on their right hand, resulting in a total of ten moulds for each participant. Play-Doh took longer to dry as it was air dried; Matsumoto et al. (2002) suggest this aids in avoiding any potential for distortion which can be attributed when using a kiln. The aim of quality controlling the manufacture of the moulds was to ensure sufficient and consistent detail was apparent for the scanning process. Once ten reviewed moulds had been created, casts were then prepared from these in order to reconfigure and correct the ridge and furrow reversal. Polycraft silicone mould making rubber was used to create the casts with both the orange curing agent and white base mixed to a ratio of 10:1 (Tan and Schuckers, 2010). The two were mixed until

a bright pink colour was produced; the aim of the mixing process was to remove any air bubbles. The prepared mixture was finally moved to a different container to fully remove any potential of the curing agent or white base to remain unmixed (MB Fibreglass, 2015). Silicone rubber was applied to the moulds through use of a syringe, filling them and then leaving them to harden overnight. This process was repeated four times to create a total of five casts.

3 Vahine gelatine powder

Gelatine powder was added slowly, one tablespoon of cold water whilst stirring, one 11 g bag could be sufficient enough to create 600 ml of gelatine, however, a ratio of 11 g gelatine to 100 ml water was used instead. This created greater firmness, producing a more suitable product for scanning. This mixture was set aside before 100 ml of water (70°C) was then added to the prepared mixture and stirred to remove any lumps. Once completed, the gelatine was cooled in ambient air and prepared for casting. Using a syringe the gelatine was applied to the moulds, again establishing five individual casts, one for each of the participants. These were then placed in the refrigerator for 30 minutes to avoid over-hardening as recommended (Sten et al., 2003).

Quality control vetting continued to ensure no blemishes led to inaccurate results (Espinoza et al., 2011). Due to the original cast bearing the negative values for the ridges and furrows any failed subsequent casts producing the positive values could be repeated.

Phase 2 focused on the recovery of ridge detail directly from a touched surface rather than the digit itself. Each participant provided four fingerprints each: thumb, index finger, middle finger and ring finger. The little finger was deselected as it was not possible to roll and provide sufficient detail. Each participant placed the thumb onto a curved bottle and each of the three remaining fingers onto a white tile as a latent print. Once positioned, these fingerprints were powdered with Magneta Flake, applied with a magnetic wand to enhance the ridge detail. With excess powder removed, Provil was then placed directly onto the enhanced ridge detail to a depth of 3 mm, a factor in ensuring durability (Ohana et al., 2013). Once dry, the cast was lifted. As a preliminary test one additional Provil cast was created, this was to test the stability of the powdered fingerprint now present on the Provil cast. After rigorous rubbing of the print, some of the Magneta Flake powder was removed however ridge detail features remained intact and unobliterated. These direct casts were then vetted using the same process as those created through moulding; identifying any areas of excessive powdering or air bubbles distorting the ridge detail and recreating where necessary.

Two scanners were preselected from the USB scanners currently available on the market (Bowden-Peters et al., 2012). Selection was based on their current price and, the latter graded from customer reviews (Ohana et al., 2013). Two pricing brackets were chosen, the first being from 0–20 GBP, the second from 21 GBP upwards. The fingerprint scanner chosen from the 0–20 GBP range was the Andoer Security USB Fingerprint Reader Scanner (sweep sensor) and the URU 5000 USB Biometric Fingerprint Reader Scanner (optical sensor) selected for the 21 GBP and above bracket (Maltoni et al., 2009).

To initially test the scanners reliability, one selected participant's results from the enrolment stage of scanning was recorded. This enrolment process involved the participant producing a reference for each subsequent identification

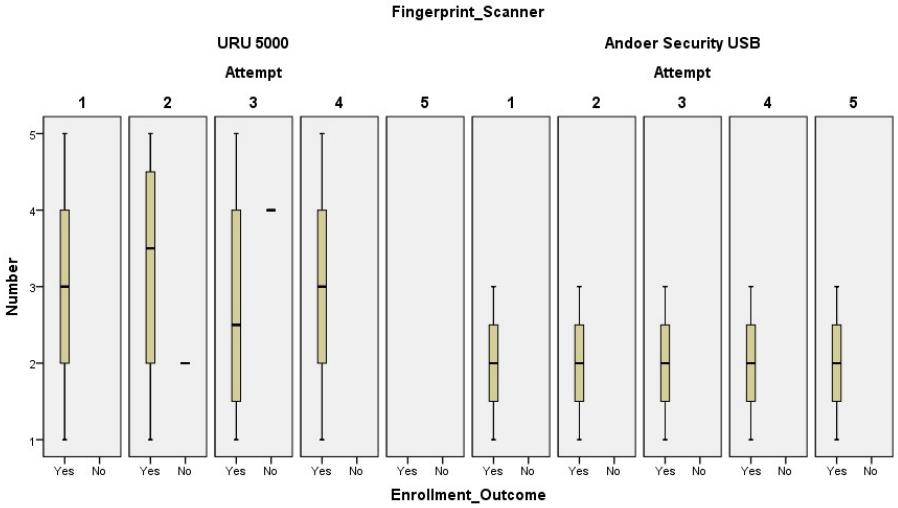
(Fernandez-Saavedra et al., 2013). Each cast was then tested 30 times per participant; in total 180 attempts were made. The result of each test was recorded contemporaneously, expressed through a series of yes or no's for each attempt. Further validity testing was also undertaken for each scanner. This involved using a known incorrect fingerprint cast being applied over 100 times to ascertain if consistent incorrect repetition resulted in access.

To confirm the results, this process was performed twice using two participant casts over two casting materials: Silicone and Provil. A success rate for the two fingerprint scanners was then established (Espinoza et al., 2011). An Acer Aspire 7750G laptop with a Windows 7 Operating System was used operate the fingerprint scanners.

4 Results

Figure 1 shows the enrolment results from participant 2's index finger on each of the two scanners.

Figure 1 Box plot showing enrolment results for participant 2 (see online version for colours)



Early scanning results illustrated that the Andoer Security USB Fingerprint Reader Scanner was intermittent in its functionality in confirming access once enrolled. This process reoccurred a number of times until access could not be gained at all. The scanner quickly failed to read fingerprints scanned however the results that were obtained showed that access was granted with the methods described. Due to its malfunction, the Andoer USB Scanner was not utilised further during the study.

The URU 5000 USB Biometric Fingerprint Reader Scanner was more durable and produced results showing that all three casting materials were able to gain spoof access as illustrated in Figure 2. From these casting materials used, the direct casting method using Provil performed most successfully in gaining, having succeeded 241 attempts from a total of 600 (40.16%) as shown in Table 2. This level of success is further evidenced by

the direct Provil casts gaining access for three participants (1, 2 and 4) above 27 attempts out of 30 for each individual (90%). Although able to gain access for two participants in 1 attempt out of a total of 30, Gelatine performed considerably less well from all casting materials as shown in Table 2. From all five participants used throughout experimentation, Table 3 shows that the casts from participants 1 and 2 who were both male were able to gain access most often with 118 and 89 successful entries respectively from a total of 180 attempts each, producing an average of 103.5. Furthermore, this is in comparison with participants 3, 4 and 5 who were female, male and female respectively who, although able to gain access using silicone and Provil, gained access considerably fewer times with an average of 22 successful attempts from a total of 180 each. Male participants gained access 41.85% of the time, with females at 13.05% over all casting mediums. The authors recognise this is a small sample size and it would be unwise to infer that vulnerability of a fingerprint scanner could be attributed to whether the user was male or female. However, for completeness, these results have been included as literature hints that this is worth exploring further.

Figure 2 Bar graph showing scanning results for each cast material per participant (see online version for colours)

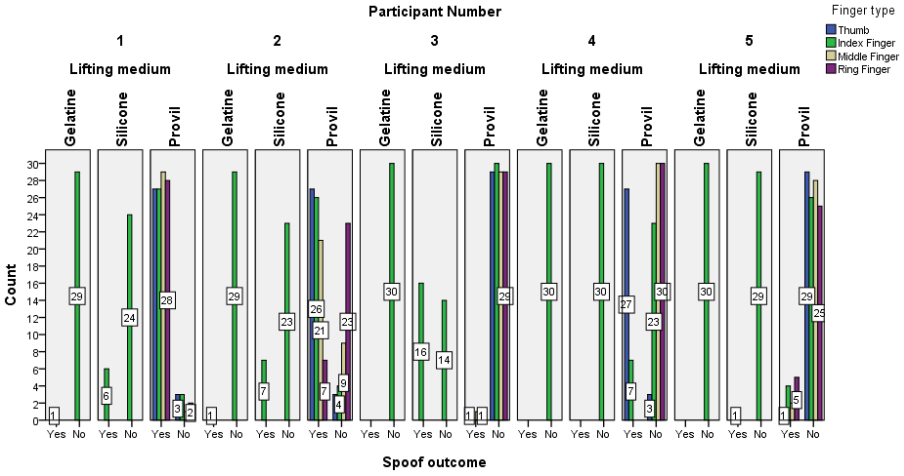


Table 1 Mould creation and direct casting lifting medium and spoof outcome cross-tabulation

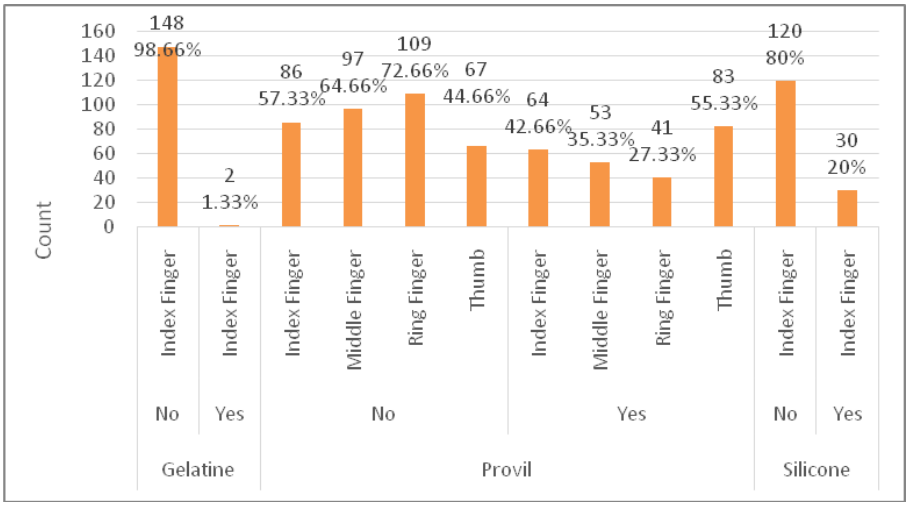
Count				
		Spoof_Outcome		*Total*
		Yes	*No*	
Lifting_Medium	Gelatine	2	148	150
	Silicone	30	120	150
	Provil	241	359	600
Total		273	627	900

The results indicate that when scanning using the direct casting method with Provil, the latent thumb mark taken from a curved surface proved the most successful in establishing access. Here, a total of 83 entries out of 241 resulted in authorised entry, making up 34.43% of the Provil success rate by gaining a 55.33% access rate as highlighted in Figure 3. Also of note is that whilst each of the fingers were able to gain entry via Provil direct casting, the index and ring finger casts provided by participant 3, along with the middle and ring finger casts provided by participant 4 were unable to breach the scanner. This might suggest that certain fingers provide better security measures, a proposal that warrants further investigation. This output is demonstrated in Figure 3.

Table 2 Mould creation and direct casting participant number and spoof outcome cross-tabulation

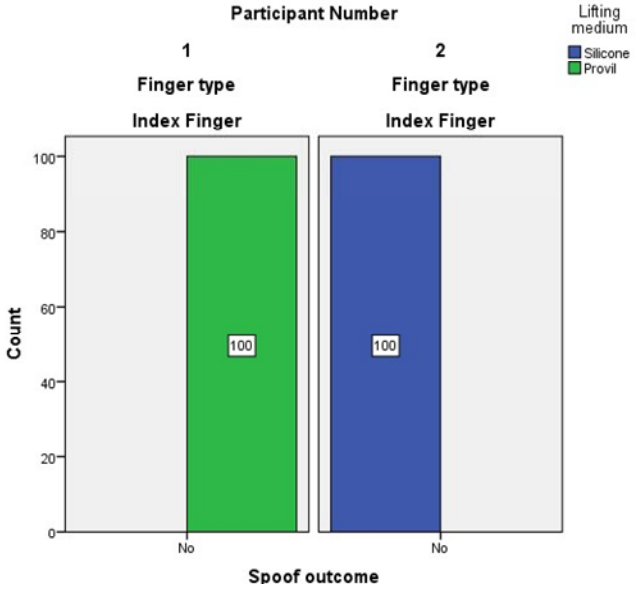
		Count		
		Spoof_Outcome		*Total*
		Yes	*No*	
Participant_Number	1	118	62	180
	2	89	91	180
	3	19	161	180
	4	34	146	180
	5	13	167	180
Total		273	627	900

Figure 3 Bar graph showing scanning results for each finger type as a total number for all participants with percentage of access rates (see online version for colours)



The reliability test results showed that from 100 attempts using two participant casts, the fingerprint scanner was able to prevent unauthorised access when a different digit cast was applied, as demonstrated in Figure 4.

Figure 4 Bar graph showing scanning results from reliability test for each cast material for each participant and cast material used (see online version for colours)



5 Discussion

This study examined the reliability of currently available fingerprint scanners, in storing fingerprint data. Key questions focused on the which replication method proved the most successful, in addition to scoping out future work in how fingerprint scanner security could be improved and the consequences of producing alternative or simulated ridge detail.

The presence of biometrics has continued to grow in line with development of the digital world and expanding security needs, as such the rising requirement for industries and society to protect information stored digitally has increased (Unar et al., 2014). As more pertinent details are stored online, the desirability for criminals to breach such systems proliferate (Jang-Jaccard and Nepal, 2014). Fingerprint identification is one of the most prominent sources of biometric security and storage and as such requires ever more attention to tackle the constant cyberattacks from individuals that seek access (Huang et al., 2007). As a wider range of online applications are created, the need for further research and development into these applications has become an urgent task (Bahaa-Eldin, 2013).

Section 4 provides a number of key outcomes pertaining to the current quality of finger scanner reliability. Five participants were used in the study, three males and two females. Results showed that two male participant casts were able to gain entry into the scanner considerably more than that of the third male and two females. This detection may be a product of the anatomy of the female fingerprint, where in general the friction ridge detail of the fingertip appears denser or more concentrate as demonstrated by

Oktem et al. (2015). This finding would, in this case, have an effect on the results after the replication process. To reiterate an earlier comment, it is too early to ascertain if male or female fingerprint biology is a variable in fingerprint scanner vulnerability, however it is suggested this is a theme which should be explored further.

Of importance was that all three casting agents, to varying degrees, were able to breach the fingerprint scanner used during the scanning stage. In some instances, this occurred up to 29 out of 30 attempts. This confirms the work performed by Bowden-Peters et al. (2012) in which access can be gained over multiple attempts using a range of casting materials. This discovery differs from the early established hypothesis in that it was assumed success rates would be much lower as seen by Sten et al. (2003) where 2% of attempts granted access.

A key reason for this difference could be the construction and quality of the casts produced as well as the scanners tested. Although strict quality control measures were implemented, exact duplication of cast composition could not be established. As a consequence, it is unknown whether any microscopic variations had an impact when products were compared. As a pointer for future researchers, it should be stated that the use of degraded fingerprint ridge detail or low-quality prints, has been explored at some level with attempts to reduce skewed results in fingerprint recognition, whilst maintaining a cost efficiency focus (Willis and Myers, 2001).

The results highlighted that direct casting using Provil, of a latent print achieved the highest success rate in obtaining access to the fingerprint scanner. Although the entries recorded from the mould production method is of importance the direct casting outcomes convey lessons which could shape future research in this domain. This discovery depicts the ease in which a user's latent fingerprint can be obtained even from a curved surface and used to spoof access. This conflicts at some level with work conducted by Ohana et al. (2013), wherein latent fingerprints were captured using Mikrosil, an alternative agent to Provil. Where the material was applied directly onto the finger, initial performances did not breach the tested fingerprint scanner as a stand-alone material, only when combined with moisture was access granted. Ohana et al. (2013) also tested using direct casting of a latent print, however, these produced negative results for spoofing as access was not granted using this approach. Differences in results could be due to a number of variables notably fingerprint scanner tested, ridge detail quality of the latent impression specifically depletion of fingerprints, casting agent as well as the enhancing fingerprint powder to name but a few.

What has been illuminated is that a method has been established which is capable of spoofing scanner access using a latent fingerprint. Moreover, this access was repeatable, signalling the need for manufactures to improve security capability and in the interim to provide more information to consumers. This finding has direct consequence on both the financial and ethical well-being of users employing such technology, in that the capability to impersonate or commit crime with only a few resources and little technical skill is a real phenomenon. The ability to operate with few safeguards to prevent such actions is not a new revelation (Monrose and Rubin, 2000). It is reported that a direct result of this is greater reluctance by consumers to use such technological methods as a means of identification and verification (Clodfelter, 2010). However, whilst this last point is made within the last decade it is important to consider that this is against a backdrop of a generation who are now familiar with this technology from accessing their smartphones to taking out a library book at school.

6 Conclusions and recommendations

Research is growing and diversifying, evidence falls to Yang et al. (2014) who investigated whether the characteristics of a finger vein can be applied as a unique biometric method, in essence a future verification tool. Furthermore, research conducted by Xu et al. (2015) examined the use of multibiometrics, combining both palm and finger ridge detail, as a means to enhance identification authenticity. It is envisaged research in this field will continue to grow, rectifying existing as well as exposing new vulnerabilities (Marasco and Ross, 2014).

However, this research wishes to acknowledge the average consumer and what fingerprint biometric security opportunities they have when they spend what is perceived to be a reasonable amount to make sure their data is safe whilst still benefiting from ease of access. To nourish this need, manufacturers should invest in systems that are capable at the very least to resist simulated ridges (Maltoni and Cappelli, 2009).

The authors acknowledge that a great range of participants and fingerprint scanning products are needed in order to solidify or challenge the results obtained as part of this study (Kärgel et al., 2012). That said it cannot be ignored that spoof access to a reasonably priced fingerprint scanning device from a latent fingerprint occurred more times than not, moreover, this proved to be the most reliable method of spoofing, even exceeding those where a cast was taken from a finger.

It is proposed that additional work be invested in to establish which materials are the best at providing spoof access, in this study, Provil was deemed to be a reliable agent. These should then be used to create a bench mark standard combining both technique and product in which fingerprint scanners should aim to resist. In addition to this, literature suggests that the ridge density on a fingertip is different between male and female users. Sample size was too small to explore this further although initial results deemed that it is a worthy research question. Moreover, questions also remain as to which fingers provide the best security provision. Additional comments to this work follows that novel methods of deterring access, such as odour (Baldisserra et al., 2006) and perspiration analysis (Parthasaradhi et al., 2005) along with further methods to garner consent (Yang et al., 2013), as a means of preventing unauthorised entry, are worth pursuing.

References

Bahaa-Eldin, A.M. (2013) 'A medium resolution fingerprint matching system', *Ain Shams Engineering Journal*, Vol. 4, No. 3, pp.393–408.

Baldisserra, D., Franco, A., Maio, D. and Maltoni, D. (2006) 'Fake fingerprint detection by odor analysis', *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Hong Kong, China; DEIS Università di Bologna, Bologna, Italy, 5–7 January, pp.265–272.

Bowden-Peters, E., Phan, R.C-W., Whitley, J.N. and Parish, D.J. (2012) 'Fooling a liveness-detecting capacitive fingerprint scanner', *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics (LNCS)*, Vol. 6805, pp.484–490.

Clodfelter, R. (2010) 'Biometric technology in retailing: will consumers accept fingerprint authentication?', *Journal of Retailing and Consumer Services*, Vol. 17, No. 3, pp.181–188.

Cole, S.A. (2005) 'More than zero: accounting for error in latent fingerprint identification', *Journal of Criminal Law and Criminology*, Vol. 95, No. 3, pp.985–1078.

Dentistry Today (2010) *Making a Great Impression* [online] http://www.dentistrytoday.com/impressions/4231-making-a-great-impression (accessed 21 April 2015).

Dror, I.E. and Mnookin, J.L. (2010) 'The use of technology in human expert domains: challenges and risks arising from the use of automated fingerprint identification systems in forensic science', *Law, Probability and Risk*, Vol. 9, No. 1, pp.47–67.

Dror, I.E., Wertheim, K., Fraser-Mackenzie, P. and Walajtys, J. (2012) 'The impact of human-technology cooperation and distributed cognition in forensic science: biasing effects of AFIS contextual information on human experts', *Journal of Forensic Sciences*, Vol. 57, No. 2, pp.343–352.

Espinoza, M., Champod, C. and Margot, P. (2011) 'Vulnerabilities of fingerprint reader to fake fingerprints attacks', *Forensic Science International*, Vol. 204, Nos. 1–3, pp.41–49.

Fernandez-Saavedra, B., Sanchez-Reillo, R., Liu-Jimenez, J. and Miguel-Hurtado, O. (2013) 'Evaluation of biometric system performance in the context of common criteria', *Information Sciences*, Vol. 245, pp.240–254.

Furnell, S. and Clarke, N. (2014) 'Biometrics: making the mainstream', *Biometric Technology Today*, January, No. 1, pp.5–9.

Goode, A. (2014) 'Bring your own finger – how mobile is bringing biometrics to consumers', *Biometric Technology Today*, No. 5, pp.5–9.

Haber, R.N. and Haber, L. (2014) 'Experimental results of fingerprint comparison validity and reliability: a review and critical analysis', *Science & Justice*, Vol. 54, No. 5, pp.375–389.

Hsiao, H. and Lee, J. (2015) 'Fingerprint image cryptography based on multiple chaotic systems', *Signal Processing*, Vol. 113, pp.169–181.

Huang, C., Liu, L. and Hung, D.C.D. (2007) 'Fingerprint analysis and singular point detection', *Pattern Recognition Letters*, Vol. 28, No. 15, pp.1937–1945.

Jamieson, R., Stephens, G. and Kumar, S. (2005) 'Fingerprint identification: an aid to the authentication process', *Information Systems Control Journal*, Vol. 1, pp.1–4 [online] http://www.isaca.org/Journal/archives/2005/Volume-1/Pages/JOnline-Fingerprint-Identification-An-Aid-to-the-Authentication-Process.aspx (accessed 14 October 2014).

Jang-Jaccard, J. and Nepal, S. (2014) 'A survey of emerging threats in cybersecurity', *Journal of Computer and System Sciences*, Vol. 80, No. 5, pp.973–993.

Kärgel, R., Hildebrandt, M. and Dittmann, J. (2012) 'An evaluation of biometric fingerprint matchers in a forensic context using latent impressions', *MM and Sec'12 – Proceedings of the 14th ACM Multimedia and Security Workshop*, Coventry, UK, 6–7 September, DOI: 10.1145/2361407.2361430.

Maltoni, D. and Cappelli, R. (2009) 'Advances in fingerprint modeling', *Image and Vision Computing*, Vol. 27, No. 3, pp.258–268.

Maltoni, D., Maio, D., Anil, K.J. and Prabhakar, S. (2009) *Handbook of Fingerprint Recognition*, 2nd ed., Springer Verlag, London.

Mansfield-Devine, S. (2013) 'Biometrics in retail', *Biometric Technology Today*, No. 9, pp.5–8.

Marasco, E. and Ross, A. (2014) 'A survey on antispoofing schemes for fingerprint recognition systems', *ACM Computing Surveys*, September, Vol. 47, No. 2, Article A.

Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S. (2002) 'Impact of artificial 'gummy' fingers on fingerprint systems', *Proceedings of SPIE – The International Society for Optical Engineering*, San Jose, California, 23–25 January, DOI: 10.1117/12.462719.

MB Fibreglass (2015) *Polycraft GP-3481-F General Purpose RTV Condensation Cure Mould Making Silicone Rubber* [online] http://www.mbfg.co.uk/rtv-silicone/gp-3481-f.html (accessed 10 October 2014).

Monrose, F. and Rubin, A.D. (2000) 'Keystroke dynamics as a biometric for authentication', *Future Generation Computer Systems*, Vol. 16, No. 4, pp.351–359.

Nanni, L., Lumini, A., Ferrara, M. and Cappelli, R. (2015) 'Combining biometric matchers by means of machine learning and statistical approaches', *Neurocomputing*, Vol. 149, No. PB, pp.526–535.

Ohana, D.J., Phillips, L. and Chen, L. (2013) 'Preventing cell phone intrusion and theft using biometrics', *Proceedings – IEEE CS Security and Privacy Workshops, SPW 2013*, San Francisco, California, 23–24 May, DOI: 10.1109/SPW.2013.19.

Oktem, H., Kurkcuoglu, A., Pelin, I.C., Yazici, A.C., Aktaş, G. and Altunay, F. (2015) 'Sex differences in fingerprint ridge density in a Turkish young adult population: a sample of Baskent University', *Journal of Forensic and Legal Medicine*, Vol. 32, pp.34–38.

Parthasaradhi, S.T.V., Parthasaradhi, S.T.V., Derakhshani, R., Derakhshani, R., Hornak, L.A., Hornak, L.A., Schuckers, S.A.C. and Schuckers, S.A.C. (2005) 'Time-series detection of perspiration as a liveness test in fingerprint devices', *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, Vol. 35, No. 3, pp.335–343.

Pepper, I.K. (2010) *Crime Scene Investigation: Methods and Procedures*, 2nd ed., Open University Press, Maidenhead.

PR Newswire (2014) *World Fingerprint Sensors Market Growth Driven by Smartphones, Mobile Commerce* [online] http://www.prnewswire.com/news-releases/world-fingerprint-sensors-market-growth-driven-by-smartphones-mobile-commerce-272736351.html (accessed 7 April 2015).

Shrivastava, A. and Srivastava, D.K. (2014) 'Fingerprint identification using feature extraction: a survey', *Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014, SJCEMysuru*, India, Institute of Electrical and Electronics Engineers Incorporated, 27–29 November, pp.522–525.

Sten, A., Kaseva, A. and Virtanen, T. (2003) 'Fooling fingerprint scanners – biometric vulnerabilities of the precise biometrics 100 sc scanner', *Proceedings of 4th Australian Information Warfare and IT Security Conference 2003*, Helsinki University of Technology: Telecommunication Software and Multimedia Laboratory, Adelaide, Australia, 20–21 November, pp.333–340.

Tan, B. and Schuckers, S. (2010) 'Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise', *Pattern Recognition*, Vol. 43, No. 8, pp.2845–2857.

Tan, B., Lewicke, A., Yambay, D. and Schuckers, S. (2010) 'The effect of environmental conditions and novel spoofing methods on fingerprint anti-spoofing algorithms', *2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010*, Seattle, Washington, USA, 12–15 December, DOI: 10.1109/WIFS.2010.5711436.

Thompson, M.B., Tangen, J.M. and McCarthy, D.J. (2013) 'Expertise in fingerprint identification', *Journal of Forensic Sciences*, Vol. 58, No. 6, pp.1519–1530.

Unar, J.A., Seng, W.C. and Abbasi, A. (2014) 'A review of biometric technology along with trends and prospects', *Pattern Recognition*, Vol. 47, No. 8, pp.2673–2688.

Uz, T., Bebis, G., Erol, A. and Prabhakar, S. (2009) 'Minutiae-based template synthesis and matching for fingerprint authentication', *Computer Vision and Image Understanding*, Vol. 113, No. 9, pp.979–992.

Wang, R. and Bhanu, B. (2007) 'Predicting fingerprint biometrics performance from a small gallery', *Pattern Recognition Letters*, Vol. 28, No. 1, pp.40–48.

Willis, A.J. and Myers, L. (2001) 'A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips', *Pattern Recognition*, Vol. 34, No. 2, pp.255–270.

Xu, Y., Fei, L. and Zhang, D. (2015) 'Combining left and right palmprint images for more accurate personal identification', *IEEE Transactions on Image Processing*, Vol. 24, No. 2, pp.549–559.

Yang, K., Du, E.Y. and Zhou, Z. (2013) 'Consent biometrics', *Neurocomputing*, January, Vol. 100, pp.153–162.

Yang, L., Yang, G., Yin, Y. and Xi, X. (2014) 'Exploring soft biometric trait with finger vein recognition', *Neurocomputing*, July, Vol. 135, pp.218–228.

Zhao, Q., Zhang, D., Zhang, L. and Luo, N. (2010) 'High resolution partial fingerprint alignment using pore-valley descriptors', *Pattern Recognition*, Vol. 43, No. 3, pp.1050–1061.