On the Design of *Forgiving* Biometric Security Systems

Raphael C.-W. Phan, John N. Whitley, and David J. Parish

High Speed Networks Research Group*,
Department of Electronic and Electrical Engineering,
Loughborough University,
LE11 3TU, UK
{R.Phan,J.N.Whitley,D.J.Parish}@lboro.ac.uk

Abstract. This work aims to highlight the fundamental issue surrounding biometric security systems: it's all very nice until a biometric is forged, but what do we do after that? Granted, biometric systems are by physical nature supposedly much harder to forge than other factors of authentication since biometrics on a human body are by right unique to the particular human person. Yet it is also due to this physical nature that makes it much more catastrophic when a forgery does occur, because it implies that this uniqueness has been forged as well, threatening the human individuality; and since crime has by convention relied on identifying suspects by biometric characteristics, loss of this biometric uniqueness has devastating consequences on the freedom and basic human rights of the victimized individual. This uniqueness forgery implication also raises the motivation on the adversary to forge since a successful forgery leads to much more impersonation situations when biometric systems are used i.e. physical presence at crime scenes, identification and access to security systems and premises, access to financial accounts and hence the ability to use the victim's finances. Depending on the gains, a desperate highly motivated adversary may even resort to directly obtaining the victim's biometric parts by force e.g. severing the parts from the victim's body; this poses a risk and threat not just to the individual's uniqueness claim but also to personal safety and well being. One may then wonder if it is worth putting one's assets, property and safety into the hands of biometrics based systems when the consequences of biometric forgery far outweigh the consequences of system compromises when no biometrics are used.

1 The Case

The aim of this work is to put forth the case of *explicitly* designing biometric security systems with a *forgiving* feature; i.e. to be *forge-resilient*. To be more precise, we feel that biometric systems need to be able to recover from the incident that the underlying biometric characteristic type (e.g. fingerprint, face) becomes forgeable; or "cloneable" in biometric speak. Current biometric systems are designed without resilience to these incidents, i.e. security breaks down entirely when a characteristic becomes forgeable, with no option for incident recovery.

While *compromise-resilient* systems exist in cryptographic literature, e.g. intrusion-resilience [13, 10], key-insulation [11], leakage-resilience [21], key compromise-resilience, forward security [6, 7], or even fault-tolerance, we believe it makes sense even more so in the context of biometric systems to consider this resilience issue. The reason is this. It is common knowledge that biometrics while similar to more conventional authentication factors like passwords or chip cards, are *irreplaceable* and *irrevocable*. Thus, when a biometric characteristic of a legitimate party falls into the hands of an adversary in the forgeable sense, the legitimate party permanently loses the ability to use that characteristic in any biometric security system that authenticates using that type of characteristic. One may suggest to then replace the underlying characteristic type with another, e.g. using hand geometry instead of fingerprints; yet there is only a finite space of possible characteristic types on a human person that can be used. What is more, any evidence of the forged characteristic being found would non-repudiably bind to that party.

* Part of this work done over coffee.

2 Setting the Stage

2.1 Question Marks

Motivated by the case above, we feel therefore that one should treat forge-resilience from two perspectives: *forward security* and *convertibility*. This leads to the following questions.

Q1. Forward Security: Is there still any security that can be salvaged in the event that a characteristic type becomes forgeable with technology advances? If so, how can this remnant security be quantified?

Q2. Convertibility: Can biometric systems be designed such that the irrevocable feature is removed at the point when a characteristic type becomes forgeable? This notion could be compared with that of convertible digital signatures.

Thinking beyond forge-resilience towards a longer term goal of forge-resistance, we pose the following question that would be interesting to solve.

Q3. Ageing: can we design biometric systems with an *ageing* feature? i.e. where each subsequent sensing of a real (non-forged) biometric characteristic can be shown to be a more recent one compared to a previously sensed characteristic. In some sense, though not exactly identical, this feature could be compared to the notion of hash chains. Certainly, answering this question would make biometric systems resilient to characteristic forgery since a real one would then naturally post-date a forged one. In essence, an answer is not impossible because even if a forged characteristic appears identical to the real one, it is still an analog duplication (rather than digital) since it is physical in nature. The other distinguishing feature between a real and forged one is that the former is a physical biological characteristic that necessarily ages over time (e.g. skin cells are shed as a function of time), thus being able to capture this physical trait would aid in distinguishing between the two.

Finally, we believe that research into the above questions would progress well within a soundly defined framework that allows for rigour and unambiguity in the understanding of components that make up biometric systems, and all relevant properties that need to be captured. This raises the question below, the answer to which will cast research in this field into a strong setting.

Q4. Formal Models: can we rigorously model the security of biometric systems in the presence of forgeable biometric characteristics, and in the context of the above two main perspectives?

2.2 Moving Forward

To work towards solving the above open questions, immediate steps would naturally involve the following.

M1. Formal Models: Formalization of security in biometric systems to achieve forge-resilience: what security do we still want to uphold when the underlying biometric characteristic becomes forgeable with technological advances in physical or materials sciences?

M2. Forge-Resilience: Design of secure (in the reductionist security sense, with respect to the above formalization) biometric systems with forge-resilience, namely exhibiting either or both the following properties:

- Forward Security: systems that still offer some *remnant security* when a characteristic type becomes forgeable, and before the system (or more practically the relevant underlying component) is redesigned such that system security is recovered, i.e. it is no longer impacted by such forgery.
- Convertibility: systems such that upon the point of characteristic forgery, the non-repudiable binding of the characteristic to the party is removed, to prevent him being framed for crimes/actions he did not commit.

M3. It may be worth to design such systems using the ceremony approach [14], i.e. where humans are treated as network entities separate from the machines that they use; and taking human factors into consideration such as social and psychological issues. This is useful for instance since human tendency influences the captureability of biometric characteristics, which may impact unforgeability.

2.3 Biometric Security System

To kick off, it is worthwhile to treat a biometric security system with some notations.

Definition 1 [Matching]. Two biometric features F_1, F_2 are said to be *matching* (denoted $F_1 \leftrightarrow F_2$) if on input to a matcher algorithm $\mathcal{M}$ the output returns a "yes".

Definition 2 [Biometric System]. A biometric system $\mathcal{B} = (\mathcal{S}, \mathcal{E}, \mathcal{M})$ is a triple of the following algorithms:

sensor; $S \leftarrow \mathcal{S}(C)$**.** This senses the physical biometric *characteristic* C (sometimes used interchangeably with trait) of the human body e.g. fingerprint, iris, etc, and outputs a biometric *snapshot* S.

extractor; $F \leftarrow \mathcal{E}(S)$**.** This processes the biometric snapshot S and extracts at its output a biometric $feature$ F (sometimes also called a template), that is essentially a representation of the biometric characteristic.

matcher; $D \leftarrow \mathcal{M}(F, \mathtt{dB})$**.** This takes as input a biometric feature F and a database $\mathtt{dB}$ of stored biometric feature templates $\tilde{F}$; and via a matching process defined by some predetermined rules then outputs a *decision* $D \in \{$"*yes*", "*no*"$\}$ signifying the biometric authentication result, i.e. "yes" if F and at least one $\tilde{F}$ match and "no" otherwise.

3 Forge Resilience

Some kind of forge-resilient biometric systems have been proposed in literature that aim to differentiate between real and forged biometric characteristics by measuring the *liveness* property (sometimes called vitality) i.e. whether the characteristic is alive (real) or non-alive (forged), e.g. temperature under the skin, pulsation, perspiration [1], skin elasticity [2], skin odour [4], existence of blood veins [8], although it is not absolutely certain to what extent they can successfully solve this differentiation resolution problem [15].

In this paper, we propose another approach to achieving forge-resilient biometric systems, from the *temporal* (time-dependence) sense.

The forge resilience properties of forward security and convertibility are essentially functions of time. This is clear from their definitions, that they dictate different actions dependent on the point in time before or after a characteristic is forged. It turns out that we can achieve these forge resilience properties as a consequence of achieving age-dependent sensing of biometric characteristics.

More precisely, given that the underlying biometric characteristic type e.g. finger's bone density content [19], eye retina size [12, 16], ear size [22] vary as a function of time, this facilitates the additional sensing of the characteristic's age, thus allowing for age-dependent sensing. The gist of our approach is to design the sensing component as a function of time, such that it measures the age of the biometric characteristic in addition to the characteristic value itself. Then, upon forgery at time t', a subsequent snapshot $S_{t'}$ of the real characteristic is immediately sensed, and this is used as the reference point to outdate all sensed characteristics of an earlier age (note that this would include the forged one). This ability to differentiate between sensed characteristics as a function of time immediately implies forward security and convertibility. In more detail, since all snapshots $S_{\tilde{t}}$ (for $\tilde{t} < t'$) of an earlier age than that of $S_{t'}$ are obsoleted, the security of the biometric system after forgery no longer relies on them, and so this security is retained even after forgery. Convertibility is implied since the once binding and irrevokable snapshots $S_{\tilde{t}}$ are essentially revoked via obsoletion.

After all, ageing is very much an inherent property of the human body anyway, so it makes sense to directly use this to differentiate between the different sensed snapshots as a function of time (and more specifically the age of the sensed biometric characteristic).

4 Construction

A *forge-resilient* biometric system $\mathcal{B}' = (\mathcal{S}, \mathcal{E}, \mathcal{M}', \mathcal{R})$ is a 4-tuple of the following algorithms:

sensor; $S_t \leftarrow \mathcal{S}(C, t)$: This senses the physical biometric characteristic C of the human body, as well as senses the age t of the characteristic, and outputs an age-dependent biometric *snapshot* S_t.

extractor; $F_t \leftarrow \mathcal{E}(S_t)$: This processes the biometric snapshot S_t and extracts at its output an age-dependent biometric *feature* F_t, that is essentially a representation of the biometric characteristic.

matcher; $D \leftarrow \mathcal{M}'(F_t, \mathtt{dB})$: This takes as input a biometric feature F_t and a database $\mathtt{dB}$ of stored biometric feature templates $\tilde{F}$; and via a matching process defined by some predetermined rules then outputs a *decision* $D \in \{\text{“}yes\text{”}, \text{“}no\text{”}\}$ signifying the biometric authentication result, i.e. whether F_t matches to some $\tilde{F} \in \mathtt{dB}$.

resolver; $\theta \leftarrow \mathcal{R}(F^0, F^1)$: This takes as input two biometric features F^0, F^1 and then outputs a *verdict* $\theta \in \{0, 1\}$ signifying which feature is the outcome of a later snapshot, i.e. is more recent.

Forward (and Backward) Security. Forward (resp. backward) security refers to the system remaining secure for the time period *before* (resp. *after*) compromise; in our context compromise corresponds to characteristic forgery.

Let t' denote the age of the biometric characteristic at the point of forgery. Define an instance of the forge-resilient biometric system $\mathcal{B}'$ where its matcher $\mathcal{M}'$ algorithm is as follows:

- $D \leftarrow \mathcal{M}'(F_t, \mathtt{dB})$:
  1. Access from database $\mathtt{dB}$ the feature $F_{t'}$ corresponding to the point of forgery t'.
  2. Run $\mathcal{R}(F_t, F_{t'})$ to get the verdict θ. If $\theta = 0$, this indicates the characteristic feature F_t corresponds to an age after (or equal to) the forgery, and so output $D =$ “no” indicating that it should be disregarded, and quit. Otherwise, proceed to the next step.
  3. Run $\mathcal{M}(F_t, \tilde{F})$ for each of the features $\tilde{F}$ in the database $\mathtt{dB}$; to obtain the output D, which is returned as the final output.

The biometric system $\mathcal{B}'$ instantiated above achieves forward security since the matcher never passes any feature that is more recent than the one that was forged, yet features before the forgery incident remain passable even after this forgery incident. In the same vein, backward security can be achieved for a respectively defined matcher algorithm.

Convertibility. The notion of convertibility refers to the system removing the irrevocability property of biometric features that are more aged (or of the same age) as a forged feature. Define an instance of the forge-resilient biometric system $\mathcal{B}'$ where its matcher $\mathcal{M}'$ algorithm is as defined above and furthermore has an additional update $\mathcal{U}'$ algorithm defined as follows:

- $R \leftarrow \mathcal{U}'(\mathtt{dB}, F_{t'}, K)$: This algorithm takes as input the database $\mathtt{dB}$ of stored biometric features, a feature $F_{t'}$ corresponding to the point of forgery, and a secret key K known only to the administrator of the system.
  1. The key K is checked for correctness, upon which the algorithm proceeds to the next step.
  2. The feature $F_{t'}$ is entered into the database, overwriting any previous $F_{t'}$ value.
  3. A status reply R indicating successful or failure to update, is output.

The biometric system $\mathcal{B}'$ instantiated above achieves convertibility since the the most recently updated $F_{t'}$ would subsequently invalidate all features F_t aged after or equal to the forgery via the forge-resilient matcher algorithm $\mathcal{M}'$.

5 The Case of (In)Existence

With the discussions in the preceeding sections, it appears that the existence of forge-resilient secure biometric systems (in both the sense of forward-security and convertibility) relies fundamentally on the existence of age-dependent sensing technology and corresponding resolver technology within the field of physical and/or materials sciences.

Contrast this to conventional provably secure systems e.g. public key cryptography which rely on fundamental mathematical assumptions and correspondingly the existence of solving algorithms that can invalidate the assumptions.

6 Signposting

We draw on the main points to be derived from the above discussion in this paper.

† The security of a biometric system relies fundamentally on the underlying enabling technology, that of physical biometric sensing within the field of physical and materials sciences. In literature, one class of such sensors have been proposed to offer some form of forge resilience: liveness sensors. In this work, we have proposed another class: age-dependent sensors. It remains a constant open question if such sensors exist that resist forgeries, because advances in physical sciences lead to both an improvement in sensing technology as well as in forgery technology because they are essentially based on the same technology.

† We can only say so much about the actual security of a biometric system, because any security statement is necessarily relative; relative to the underlying enabling technology and relative to the unforgeability of the underlying sensing technology.

References

1. A. Abhyankar and S.A.C. Schukers, "Integrating a Wavelet based Perspiration Liveness Check with Fingerprint Recognition," *Pattern Recognition*, Vol. 42, No. 3, 2009, pp. 452-464.
2. A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," *IEEE Trans. Information Forensics and Security*, Vol. 1, No. 3, 2006, pp. 360-373.
3. D.A. Atchison, E.L. Maxwell, S. Kasthurirangnan, J.M. Pope, G. Smith and P.G. Swann, "Age-related Changes in Optical and Biometric Charateristics of Emmetropic Eyes," *Journal of Vision*, Vol. 8, No. 4, 2008, pp. 1-20.
4. D. Baldiserra, A. Franco, D. Maio and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis," *Proc. ICB '06*, LNCS 3832, 2006, pp. 265-272.
5. BBC, "Japanese Smokers to Face Age Test," last revised 12 May 2008. Available online at http://news.bbc.co.uk/1/hi/world/asia-pacific/7395910.stm, accessed 30 March 2009.
6. M. Bellare and S. Miner, "A Forward-Secure Digital Signature Scheme," *Advances in Cryptology - Crypto '99*, LNCS 1666, 1999, pp. 431-448.
7. M. Bellare and B.S. Yee, "Forward-Security in Private-Key Cryptography," *Topics in Cryptology - CT-RSA '03*, LNCS 2612, 2003, pp. 1-18.
8. BusinessWeek, "Biometrics: Vein Scanners Show Promise," 6 February 2007. Available online at http://www.businessweek.com/globalbiz/content/feb2007/gb20070206_099354.htm, accessed 30 March 2009.
9. R. Derakhshani, S.A.C. Schukers, L.A. Hornak and L. O'Gorman, "Determination of Vitality from a Non-invasive Biomedical Measurement for Use in Fingerprint Scanners," *Pattern Recognition*, Vol. 36, No. 2, 2003, pp. 383-396.
10. Y. Dodis, M.K. Franklin, J. Katz and M. Yung, "Intrusion-Resilient Public-Key Encryption," *Topics in Cryptology - CT-RSA '03*, LNCS 2612, 2003, pp. 19-32.
11. Y. Dodis, J. Katz, S. Xu and M. Yung, "Key-Insulated Public-Key Cryptosystems," *Advances in Cryptology - Eurocrypt '02*, LNCS 2332, 2002, pp. 65-82.
12. Andrew C. Gallager, "Determining the Age of a Human Subject in a Digital Image," US Patent Application, US Patent & Trademark Office, 2 March 2006.
13. G. Itkis and L. Reyzin, "SiBIR: Signer-Base Intrusion-Resilient Signatures," *Advances in Cryptology - Crypto '02*, LNCS 2442, 2002, pp. 499-514.
14. C. Karlof, J.D. Tygar and D. Wagner, "Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication," *Proc. NDSS '09*, to appear.
15. T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," *Proc. SPIE*, Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.
16. New Scientist, "Red-eye Age Checker," 27 April 2006. Available online at http://www.newscientist.com/blog/invention/2006/04/red-eye-age-checker.html, accessed 30 March 2009.
17. R.C.-W. Phan, K.-K.R. Choo and S.-H. Heng, "Security of a Leakage-Resilient Protocol for Key Establishment and Mutual Authentication," *Proc. ProvSec '07*, LNCS 4784, 2007, pp. 169-177.
18. D. Pointcheval and S. Zimmer, "Multi-Factor Authenticated Key Exchange," *Proc. ANC '08*, LNCS 5037, 2008, pp. 277-295.

19. RSA, "RSA Security and i-Mature Partner on Next-Generation Biometric Technology to Further Protect Children on the Internet," 7 February 2005.
20. Sankei Sport, "Magazine Bought Photos of ... Certain Loopholes in the Vending Machine," in Japanese, 24 June 2008. Available online at http://www.sanspo.com/shakai/news/080624/sha0806240502003-n1.htm, accessed 30 March 2009.
21. S. Shin, K. Kobara and H. Imai, "Leakage-Resilient Authenticated Key Establishment Protocols," *Advances in Cryptology - Asiacrypt '03*, LNCS 2894, 2003, pp. 155-172.
22. R. Tan, V. Osman and G. Tan, "Ear Size as a Predictor of Chronological Age," *Archives of Gerontology and Geriatrics*, Vol. 25, No. 2, 1997, pp. 187-191.