Biocryptographic Authentication

[Survey of recent advances in techniques that mix biometrics with cryptography]

Terrance E. Boult[a,b], R.C. Johnson[a,b], Walter J. Scheirer[b,c]
[a]Univ. of Colorado Colorado Springs; [b]Securics, Inc, ; [c]Harvard Univ.

1. Introduction

Strong authentication using biometric-based technologies have been deployed for decades, but as the use of biometrics becomes more wide-spread, the privacy concerns that stem from their use are becoming more apparent. Over the past decade there has been progress toward privacy-enhanced biometric-based technologies that can address the privacy concerns while maintaining the strong authentication properties of biometrics. Early work was not sufficiently accurate/secure, and some of these techniques have been "cracked"[11]. However, recent work has produced solutions that are sufficiently accurate and secure for broad usage. We will briefly review the state of privacy-enhanced biometrics and template protection techniques, and then dive deeper into the subclass called biocryptographic techniques – techniques which bind biometric data and key/token data such that biometric matching releases the key/token. The authors have a long history in this space, having produced the most accurate/secure template finger-print technology [3, 10, 5], the most accurate privacy-enhanced voice-base solutions[7, 6], as well as privacy-enhanced techniques that work with iris [14] and face[2, 13] and having provided many tutorials include an IEEE Expert tutorial on biometrics security and privacy[12]. We have pioneered how to use biocryptographic techniques to develop a wider range of authentication protocols [8, 9, 1], many of which fit naturally into today's public-key based solutions, providing for both key management and for advanced strong authentication.

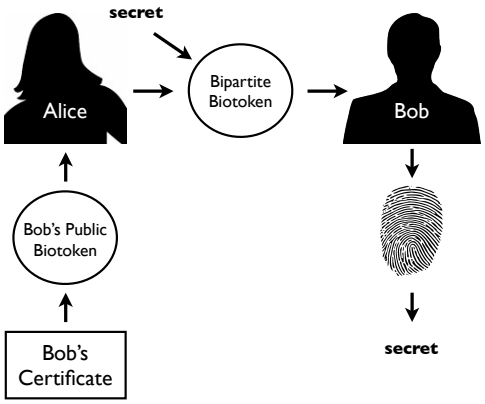

Figure 1: The Biocryptographic Key Infrastructure concept: the ability to securely store *public* biotokens in public digital certificates for use in a transaction. Any entity in the infrastructure can send secret data that only the owner of the biotoken can unlock. In this example, Alice wants to convey a secret message to Bob. Bob's public biotoken can be retrieved from his certificate, allowing Alice to transform it into a bipartite biotoken, which conveys an embedded secret. Alice has assurance that the identity must be present to unlock the secret – not just a key. Alice can also use it for her own private key for signing, or as part of a key-based authentication protocol, e.g. Kerberos or OAuth.

2. Biometric Security & Privacy

Traditional biometrics, once compromised, cannot be revoked. Even if stored encrypted, biometrics must be decrypted to match. Together these lead to the *biometric dilemma*, a biometrics become widely used they become more useless for security. In addition, traditional biometrics lead to various privacy concerns because traditional biometrics can be matched without user consent.

To add these issues research developed cancelable or revocable biometrics, wherein the raw biometric undergoes a secure transformation and then the data is matched in that transformed space. Some of these transformations are just security oriented, allowing matching without user involvement and others can involve users pass-phrases to control usage and hence have even greater privacy benefits. Some papers focus on non-invertibility, but this is red herring – being non-invertible is neither necessary nor sufficient for security/privacy [4]. The security and privacy also depend on how well the transformation protects the data from recovering data that could be used to launch an attack or violate privacy. A number of the early techniques, including those with "proven" security were later "cracked"[11], and we show an example of how this happens. We briefly review the top 10 state of the art techniques, their security standing, their known accuracy, known limitations and added benefits.

3. Biocryptographic techniques

Authentication is inherently an asymmetric problem – you want to prove your identity without giving someone the identify information that would allow then to impersonate you. Traditional biometric fail at that level – they are akin to symmetric encryption in that there is only one key. Public-key cryptography introduced an asymmetric model allowing sender and receiver to have different "keys". Biocryptographic techniques seek to do something similar for strong identity. By securely combining biometric data with crypto-

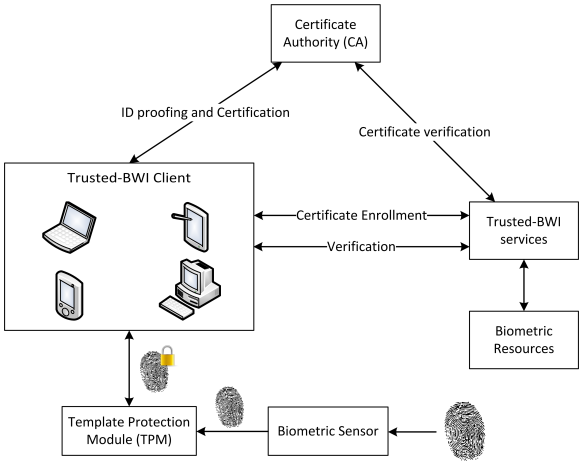

Figure 2: Overview of Trusted-BWI web services. An extended BKI uses a Template Protection Module (either software or hardware) which produces a Public Key/Private key and protects the private key, requiring biometric matching to use it. The CA does identity proofing with it, represented in the resulting certificate. The certificate can be enrolled in a Trusted-BWI server and used for later verification. The model allows trusting CAs for identity proofing; however, the Trusted BWI servers may also have their own CA. Privacy is maintained since traditional biometric data is not used outside the Template Protection Module while the certificate may have a pseudonym rather than traditional identity information. Stronger binding of digital certificates to identity, in a scalable manner, with privacy enhanced remote/client side matching, makes Trusted-BWI ideal for web-based applications needing trusted identities.

graphic keys in a way that support the approximate matching needed for biometrics, we can produce asymmetric identity tokens that the sender/challenger doee not have access to the receiver/user secret data. They allow the owner to release the key/message using their biometric (and possibly a password), all while ensuring an attacker cannot recover approximations to the biometric or the key in reasonable effort. We call the resulting object a biotoken. The key element here is defining a process by which the biometric is cryptographically mixed with key such that matching releases the key but such that neither the biometric or key can be meaningfully approximated from the data. While one can have an approach that converts a biometric into a fixed key, that returns to the problem of irrevocability. Rather, we seek a re-encoding property, which is essential for supporting a transactional/authentication framework - tokens with unique data must be generated quickly and automatically to support the transaction. By combining some types of revocable biometric templates with cryptographic functions, we can obtain biocryptographic tokens that can support a more general biocryptographic key infrastructure(BKI)[9], see figure 1, as well as privacy and security enhanced Trusted Biometric Web Identities[1], see Figure 2.

Our talk will review the state of the art in this emerging area including our recent work on fingerprint and voice-based solutions including the first challenge-response protocol for biometric biometric-based authentication where your biometric data never leaves your device.

4. References

[1] A. A. Albahdal, H. Alzahrani, L. P. Jain, and T. E. Boult. Trusted BWI: Privacy and trust enhanced biometric web identities. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Int. Conf. on*, pages 1–8. IEEE, 2013.

[2] T. E. Boult. Robust distance measures for face-recognition supporting revocable biometric tokens. In *Automatic Face and Gesture Recognition, 2006. Int. Conf. on*, pages 560–566. IEEE, 2006.

[3] T. E. Boult, W. J. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In *CVPR*. IEEE, 2007.

[4] T. E. Boult and R. Woodworth. Privacy and security enhancements in biometrics. In *Advances in Biometrics*, pages 423–445. Springer, 2008.

[5] L. Jain, M. J. Wilber, and T. E. Boult. Issues in rotational (non-) invariance and image preprocessing. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2013 IEEE Conf. on*, pages 76–83. IEEE, 2013.

[6] R. Johnson and T. E. Boult. With vaulted voice verification my voice is my key. In *Technologies for Homeland Security (HST), 2013 IEEE Int. Conf. on*, pages 453–459. IEEE, 2013.

[7] R. Johnson, T. E. Boult, and W. J. Scheirer. Voice authentication using short phrases: Examining accuracy, security and privacy issues. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Int. Conf. on*, pages 1–8. IEEE, 2013.

[8] W. Scheirer and T. Boult. Bio-cryptographic protocols with bipartite biotokens. In *Biometrics Symposium, 2008. BSYM'08*, pages 9–16. IEEE, 2008.

[9] W. J. Scheirer, W. Bishop, and T. E. Boult. Beyond PKI: The Biocryptographic Key Infrastructure. In *Security and Privacy in Biometrics*, pages 45–68. Springer, 2013.

[10] W. J. Scheirer and T. E. Boult. Bipartite biotokens: Definition, implementation, and analysis. In *Advances in Biometrics*, pages 775–785. Springer, 2009.

[11] W. J. Scherier and T. E. Boult. Cracking fuzzy vaults and biometric encryption. In *In Proc. of the 2007 Biometrics Symposium, held in conjunction with the Biometrics Consortium Conf. (BCC 2007)*, 2007.

[12] W. J. Scherier and T. E. Boult. Biometrics: Privacy and social acceptance. IEEE Expert Now Series, online course material available in the IEEE eLearning Library, Dec. 2010. `http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&mdnumber=EW1198`.

[13] M. J. Wilber and T. E. Boult. Secure remote matching with privacy: Scrambled Support Vector Vaulted Verification. In *Workshops on the Applications of Computer Vision (WACV)*, 2012.

[14] M. J. Wilber, W. J. Scheirer, and T. E. Boult. PRIVV: Privae remote iris-authentication with vaulted verification. In *IEEE Computer Vision and Pattern Recognition (CVPR) Workshop on Biometrics*, 2012.