publications [8][9][10][11][12][13] (Table II). In the case of a compromised transformation key, the other literatures [8]-[13] showed some accuracy drops while still remaining close to the accuracy of the biometric system only (upper six rows in Table II). Hisham Al-Assam, et al. [16] showed that in such a scenario, the same Operating Point (OP) setup to operate at a zero EER caused the False Acceptance Rate (FAR) of the system to reach unacceptable levels: FAR of 56.67% for Fingerprint and FAR of 66.69% for Face (last two rows in table II).

TABLE II Authentication results

source	Biometric Type	Biometric only	Two-Factor (secure)	Two-Factor (insecure)
[8]	Fingerprint	EER=5.66	EER=0	N\A
[9]	Iris	EER=3.2	EER=0	EER=8.6
[10]	Fingerprint	FAR=1 at FRR=7	EER=0	FAR=1 at FRR=7
[11]	Face	EER=15.63	EER=0	EER=16.21
[12]	Palm	EER=2.75	EER=0	N\A
[13]	Face	EER=7.19	EER=0	EER=7.19
[16]	Fingerprint	FAR=0.1 at FRR=16	EER=0	FAR=56.67 at FRR=0
	Face	FAR=0.67 at FRR=21.5	EER=0	FAR=66.69 at FRR=0
EER: Equal Error Rate; FAR: False Acceptance Rate; FRR: False Rejection Rate				

The main reason behind the biased evaluation of a compromised key is due to the simulation which is performed at operating point(s) whose values are completely different from the operating point(s) in the case of a secure key. This assumption is totally unrealistic, as it implicitly assumes that the biometric system knows it is a compromised key and automatically changes its OP. However, note that there is no way to distinguish a genuine key from a compromised key.

VI. Conclusions

Multi-factor authentications have been proposed with the purpose of strengthening security in authentication systems. However, the effect of multi-factor authentications should be considered carefully, as security could be greatly weakened if not properly set and used. In this paper, we present several examples of multi-factor authentications which misbehave, compared to the initial expectations. From these examples, we extract some guidelines for future works.

1) As a general rule, that can be extracted from examples I and II and III, an open and standard cryptographic primitive such as a protocol, a block cipher or a hash function, should be preferred to any special or hidden design.

2) Through Example I, we emphasize the need for the client to be simpler in the client-server applications. Compared to the server, usually handled by security specialists, common clients have less insight on the security of their environment. Thus the secure solution should be obvious to the common client, like the Page-Two jumping up with the special message in Fig. 2. Note especially that the client may be even the attacker. Hence the special software downloaded in client environment is more vulnerable, ruining the security of the whole authentication process.

3) Example III and IV highlight the fact that in multi-factor authentication, all the factors must be independent; that is: password, token key and biometric transformation key must be independent. Indeed if a factor is compromised, it does not influence the others, ruining the whole security. In turn the independence of the factors forces the attacker to break every single component, making it much harder.

Acknowledgment

The authors would like to deliver special thanks to Manuel Charlemagne for his helpful proofreading work.

References

[1] L. Lamport：Password Authentication with Insecure Communication, In: Comm. ACM, vol. 24, No 11, 1981, pp. 770-772

[2] RSA SecurID - Two Factor Authentication, Security Token – EMC, http://www.rsa.com/node.aspx?id=1156

[3] Kensuke Sawada: Authentication System, US8074075, Dec. 2011.

[4] Zhou Lu, HuaZhang Yu: One time password generating method and apparatus, US8184872, May 2012.

[5] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen: HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2005, http://tools.ietf.org/html/rfc4226.txt

[6] N. Haller, C. Metz, P. Nesser, M. Straw: A One-Time Password System, Feb. 1998, http://www.ietf.org/rfc/rfc2289.txt

[7] RSA Laboratories - OTP-PKCS #11: PKCS #11 mechanisms for One-Time Password tokens, Dec. 2005, http://www.rsa.com/rsalabs/node.asp? id=2818

[8] Teoh, A.B.J., Ngo, D.C.L, Goh, A. 2004. BioHashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition. Vol. 37(11), pp. 2245-2255.

[9] Lumini Alessandra and Loris Nanni. 2006. Empirical tests on BioHashing. Neurocomputing. Vol. 69, pp. 2390-2395.

[10] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar. 2008. Biometric Template Security. EURASIP Journal on Advances in Signal Processing. pp. 1-17.

[11] Andrew B. J. Teoh, Kar-Ann Toh, and Wai K. Yip. 2007, 2^N Discretisation of BioPhasor in Cancellable Biometrics. Advances in Biometrics. pp. 435-444.

[12] Connie, T. and Teoh, A. and Goh, M. and D. Ngo. 2004, PalmHashing: a novel approach for dual-factor authentication. Pattern Analysis & Applications. Vol. 7(3),pp. 255-268.

[13] Wang, Y. and Plataniotis, KN. 2007, Face Based Biometric Authentication with Changeable and Privacy Preservable Templates. Biometrics Symposium. pp. 1-6.

[14] A. Biryukov, J. Lano, and B. Preneel. Recent attacks on alleged securid and their practical implications. Computers & Security, 2005. pp. 304-370

[15] Ian Molloy, and Ninghui Li. Attack on the GridCode One-Time Password, AsiaCCS2011, Hongkong, China. pp. 306-315

[16] Hisham Al-Assam, Harin Sellahewa, and Sabah Jassim. Multi-Factor Biometrics for Authentication: A False Sense of Security, MM&Sec2010, Roma, Italy. pp. 81-87.