positive relationship between using a fingerprint and the level of security and usability and Table 3 show the mean values from the Likert scale for each method and it indicates that users feel that the finger method is most usable, the most secure and the most trustworthy. This means that, when the fingerprint was used, the level of usability and security increased. Regarding the last section of questions that asked the users to rank each method in terms of preference, ease of use, security and trustworthiness, the fingerprint was also most preferred by the users.

Table 3. Mean differences between methods

	usability	security	trustworthy
Fingerprint	**3.71**	**4.05**	**3.96**
Secure device	3.08	3.74	3.74
Card reader	3.46	3.78	3.85

6.3. Security Results

As mentioned previously, five criteria assessed the security level of the authentication process regarding the methods by examining the users' awareness and behaviour with the presented security indicators. During the experiment, regarding the observation of users' attention to the missing SSL and availability of a security icon and https in the address bar, none of the 100 users recognised the absence of SSL. However, 12 of the 100 users indicated they had experience in the domain of security, which revealed that the users' attention regarding the understanding the importance of an SSL connection is very low. Caution was measured by observing users' ability to type and provide an email address in an insecure page. During the experiment, all the participants provided and typed an email address in an insecure page without any concern, which also indicates their weak understanding of the harm that could happen as a result. Regarding motivation, which measure users' responses to the request for providing authentication methods, those who used the secure device were happy to use the method and complete the authentication process. Regarding those who used the card reader, 14 hesitated to use the original card. On the other hand, those who used the fingerprint seemed to enjoy the experience, while three out of 100 wondered whether their fingerprint would be saved in the website database, which indicated their caution to provide their fingerprint was not due to working in an insecure page but because of their wariness it would be used in other ways. Finally, wariness was measured by observing users' responses to the warning message that related to the missing security certificate. In this step, we obtained results from the table schema created to record responses and from the observation sheet. The results indicate that 85% of users pressed the OK button, which means they continued the process without any wariness, while 15% pressed cancel to avoid harm or danger. From the observation sheet, the experimenter was able to divide the participants' responses to the warning message into seven groups:

- Those who were confused after reading the message and decided not to go further (1 user).
- The group that read the message very carefully and tried to understand its content (f=16).
- Those who hesitated to proceed with the process (f=7).
- The group (f=5) that requested help from the observer.
- Two that decided to discontinue their work.
- One user who tried to find instructions to help him to decide.
- Finally, 68 users were not concerned and ignored the message.

Generally, the results indicate that the participants' level of attention, caution, wariness and motivation for security during the authentication is weak. In addition, it seems that their background regarding the security of online banking is very low; however, all of them are online banking users.

7. Conclusion

The presented study proposed an approach for evaluating different multifactor authentications by giving users the freedom to choose their preferred method to authenticate themselves while online banking. Our methodology that forces each user to use three different methods was successful and ended with an experiment that gives each user a realistic experience with each method in order to be able to rate each of them and get an accurate result. Moreover, the study's methodology suggested the integration of usability metrics with security metrics that related to the users' awareness of security indicators. The results from the experiment indicate that fingerprinting was the most usable and secure method from the users' point of view. Finally, the users' level of understanding security indicators is very low, based on observing their reaction to the security features presented in the study.

8. References

[1] Hyde, D. (2012). Hackers crack new online banking security putting 25 m people at risk. This is money. Available from: http://www.thisismoney.co.uk/money/saving/article2096060/Hackerscracknew-online. Available online. [Accessed on 13/12/2014].

[2] Nodder, C. (2005). Users and trust: A Microsoft case study. In: L.,Cranor, S.,Garfinkel, editors. Security and Usability. O'Reilly; pp. 589–606 [chapter 29].

[3] Whitten, A., and Tygar, J.D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, 99, McGraw-Hill.

[4] Computing Research Association (2003). " Four Grand Challenged In Trustworthy Computing", Final report of CRA Conference on Grand Challenged in Information Security and Assurance, Airlie House, Warrenton, Virginia, November 16 – 19.

[5] Piazzalunga, U., Savaneschi, P., and Coffetti, P. (2005). The usability of security devices. In: L.,Cranor, S.,Garfinkel, editors. Security and Usability. O'Reilly; pp. 221–42 [chapter 12].

[6] Weir, C.S., Douglas, D., Carruthers, M, and Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. Computer & Security, 28(1).

[7] Nielsen, J. (1993). Usability engineering. San Francisco: Morgan Kaufmann.

