Biometric authentication

Technology, Information Technology

Evaluation of the Viability of Biometric Authentication For Online Transactions Presented By: Computer Sciences and Information Technology

Lecturer’s Name

Institution’s Name

Location

Date

1. Viability of biometric authentication methods for online transactions

Biometric Authentication is generally a more secure means of optimizing data security on online transaction as it minimizes the risk of impersonation and identity theft. In essence, biometric identification implies that the owners of the information are present in person as it identifies unique features such as eyesight, fingerprint, and voice data (Oezcan 2003, p. 11). Unlike password and signatures which are easily stolen by third parties, biometric authentication relies on the actual data from the actual users, leaving minimal chances. Biometric methods are more reliable than other methods, but still faces various limitations and exposure to dynamic attacks.. The desirable processes of biometric authentication methods that make it reliable include verification, screening and identification.

1. 1. Verification

This is a test make sure that a person A is exactly the one he claims to be. The verification can be envisaged in two ways: using central storage or using distributed storage.

1. 2. Screening

This process makes use of a watch list or a database, containing data of people to be excluded. It has records containing only the biometric

information for specific individual (Ratha, Connell & Bolle 2001, p. 610). Every individual provides biometric samples to be checked to confirm if it matches the watch-list.

1. 3. Identification

This process is used in the discovery of an individual without the user's prior claim of identity. It checks the bio information against the contents of a central database without which it cannot operate.

2. Increased Potential Violence

In spite of the great success in biometric authentication, online transactions face exposure to possible attack such as risks of Man-in-the-Middle attack and bio phishing.

2. 1. Man-In-the-Middle Attack

This is the attack where a person pretends to be a genuine person or individual service provider and prompts a user to provide personal bio data. Once the data is available and has passed through verification, the perpetrator of the attack performs unauthorized transactions.

2. 2. Bio Phishing

The phishing attack is equally harmful and takes place with or without the knowledge of the owner of the bio data. For example, an individual gets into a banking hall, gets into a dust bin and collects half-filled customer vouchers containing handwritten signature or fingerprint. He or she scans the signatures and finger prints which are then used electronically for valid online transactions.

3. Success in Biometrics

3. 1. Security

Biometric methods are more secure in the performance of online transactions. The owner provides Unique biometric information only when required electronically, unlike in the use of ordinary identification numbers.

3. 2. Privacy

A biometric method provides a high degree of privacy to users and minimizes the exposure of information to unauthorized parties (Weaver 2006, p. 99). For example, for an iris scan to be done, a person must be physically available.

4. Failures of Biometric Methods

4. 1. Frauds and Forgeries

It is possible to fraudulently reproduce biometric data depending on the resources, modality, the application and availability bio-data being reproduced. This can take place with or without the co-operation of the owners of the biometric data. Before deciding on whether the biometric system should be used or not, the first question is whether the biometric information can be technologically reproduced artificially. Secondly, it is necessary to check the availability of the data. The last question is whether it is possible to use biometric sensors for detecting possible impostors or not.

4. 2. Low Efficiency (90%)

The efficiency of biometric data verification and authentication is only 90% (Jain, Hong & Pankanti 2000, p. 97). This means there is a 10% exposure to imposters, and risk of frauds. Regardless of the successes in biometric methods, it is important to sensitize users against the possible attacks on online transactions.

5. Conclusion

Biometric methods are indeed security improvements for online identification and transactions. For the threats of attacks in biometric information on internet transactions require application of stronger security involving a combination of multiple authentication stages. For example, safety can be improved by combining hand written signature, thumb print and iris or retina scan. In case a malicious attack perpetrator gains access to one of them, it is almost impossible that he or she will gain access to the other two, hence, the chances of attack are reduced.

References

Oezcan, V 2003, ‘ Germany Weighs Biometric Registration Options for Visa Applicants’, Humboldt University Berlin, p. 11.

Weaver, AC 2006, Biometric Authentication, Computer, 39 (2), p. 99.

Jain, A., Hong, L & Pankanti, S 2000, ‘ Biometric Identification’. Communications of the ACM, 43(2), p. 97.

Ratha, NK., Connell, JH and Bolle, RM 2001, ‘ Enhancing security and privacy in biometrics-based authentication systems’, IBM systems Journal, vol. 40, pp. 610–631.