

Maintaining The Security In Internet Marketing: Moving From Biometrics To Behaviometrics


S. Altan Erdem, University of Houston-Clear Lake, USA

ABSTRACT

While it is a rather common business practice, Internet marketing is still an area that continues to evolve and adapt. One of the everlasting challenges associated with this field is being able to insure that the online transactions take place in a secure setting. This construct of security appears to be multidimensional since it can include issues associated with secure ordering, hacker protection, firewalls, identity theft, etc. While the privacy of the online consumers has to be protected, it is important for the marketers to identify the users on the Internet to collect a profile of their interests so that they can adjust their site contents accordingly and deliver advertisements that appeal to their specific preferences. Whether the ultimate purpose is to custom-tailor the online messages or offer appropriate product/service options, it is imperative that the identity of the online consumers needs to be authenticated to make sure that there is no security breach in completing the online marketing transactions. This paper reviews some of the ongoing efforts in preventing the potential intrusions in online practices.

Keywords: Internet marketing; tracking; biometrics; behaviometrics

INTRODUCTION

nce an Internet user decides to spend some time on the Internet, it is just a matter of time before he/she is asked to create an account by providing a username and a password. Whether the user is a consumer purchasing an item on e-bay or casually viewing pictures sent from a friend through Snapfish, the internet site(s) will prompt the user to create a unique login identification and password. From a marketing standpoint, usernames and passwords, in addition to other tracking devices such as cookies, smart cards, tokens, and digital certificates, are useful approaches for gathering information about the potential consumers; however, there are limitations to this technology.

The market for technology used to track and capture individuals' interests in order to market to their tastes, often referred to as behaviorally targeted advertising, has been growing over the recent years (Holahan, 2006). Internet marketing, in particular is evolving into more personalized advertisement approaches for strategic placements of advertisements to appeal to users' preferences. However, as Internet marketing strategies move toward a more refined and personalized marketing approach, a better method of gathering user specific information is needed. One such method that has a potential of eliminating the need of coming up with usernames/passwords while securing the identity of online users is the use of biometric identification hardware/software.

Accordingly, the purposes of this paper are: 1) to review the current approaches of tracking online consumers and present some of problems associated with these approaches. 2) to review biometrics and its potential for identifying the individual users. 3) to examine a subset of biometrics - namely behaviometrics - and briefly highlight its potential use in ensuring that the users identified by biometric tools are the ones who end up by completing the final transactions.

TRACKING ONLINE USERS

Even though there have been many developments in this field over the years, it appears that cookies are still the most common tools to track online users. Cookies gather information on the specific behavior of users by tracking the users' mouse clicks and are generally hidden to the users. They are used to record and develop a profile of visitors' online habits for commercial solicitations (Furger, 2000). These profiles help advertisers deliver personally directed advertisements that appeal to the individual tastes of the consumer and help marketers tailor the ads to specific users (Holahan, 2006). The objective is the effective placement of advertisements to attract consumers to products for which they have a strong potential to purchase. However, this form of internet tracking has several shortcomings. First of all, cookies identify the computer but not necessarily the user (Jones, 2000). Since several users may access the same computer, Internet site owners will obtain only those mouse clicks specific to a computer, not to a specific user. With the indefinite accessibility of public computers with Internet access available in libraries, schools and other public venues, the information received from cookies can only yield a generally broad measurement of likes and dislikes as opposed to information specific to an individual. Additionally, some users may delete cookies from their computers or they may set their internet browser to block some or all cookies. These reasons decrease the accuracy of data received from cookies and limit the ability to market to users' individual tastes and preferences.

Usernames and passwords constitute another common method currently used to identify the users of websites and capture their activities. Unlike cookies, usernames and passwords are not hidden. They are created by the Internet user and held by their knowledge or possession. The advantage is that they are more effective than cookies in identifying the user on a computer in addition to tracking that particular user's activities every time he/she logs in. Therefore, usernames and passwords are more effective in identifying a specific user's activity on a particular website and developing a profile. On the other hand, having to keep track of multiple username and passwords for an indefinite number of websites, in addition to keeping them both accessible and private, can be rather frustrating for the user. Also, usernames and passwords can be passed to others, and can create discrepancies in the data gathered by marketers. Like cookies, there is still a possibility of tracking the shared activity of several individuals that are using the same username and password by happenstance instead of tracking the original user.

Other forms of measures such as smart cards, tokens, and digital certificates require physical possession and have the same drawbacks as cookies, usernames and passwords since someone other than the original user may be tracked. Additionally, credit cards and digital certificates are used during a transaction which limits the ability to link specific website activity to a particular consumer until the transaction is actually performed (Pons, 2006). Once again, these increase the uncertainty of identifying the computer user and his/her tastes and preferences for marketing purposes.

So it appears that one thing common among cookies, usernames/passwords, smart cards, tokens, and digital certificates is that they all are useful for tracking computers used by the online consumers but they all fall short in their abilities to track specific users for individual target marketing. Accordingly, one needs a method to properly identify the user on a particular computer without making this process cumbersome for the consumer. Some suggest that biometric technology offers such a method.

DEFINITION OF BIOMETRICS

The word "Biometrics" derives from the Greek word "bios" (life) and "metron" (measure) (Koltzsch, 2007). As stated by Corcoran, Sims, and Hillhouse (1999), biometrics is used to measure something unique about individuals and eventually use those unique clues to identify them. Specifically for this article, the term biometrics refers to the use of electronic hardware/software to verify the identity of a person by using human characteristics. Some of the common methods currently used include facial recognition, fingerprint pattern recognition, iris recognition, voice recognition and signature recognition (Albrecht et al., 2003; Nanavati et al., 2002).

The advantages of using biometric technology for identification are numerous. First, biometric technology is much more secure than common methods such as PIN numbers, passwords or security codes that are based on knowledge or possession. While these can be lost or stolen, biometric recognition relies on unchangeable

characteristics instead of knowledge and it cannot be lost or stolen (Koltzsch, 2007). Secondly, biometric identification is more convenient and it is always accessible. After all, one does not have to remember to “carry” biometric identification. It is simply a part of the user. Finally, biometric characteristics are rather difficult to forge or replicate. Even though there are ways to duplicate these characteristics, they are not only very difficult but also very costly. Considering these advantages, it is obvious how using biometric technology can be more effective and efficient for Internet users as well as online service providers.

Globally, the biometric market is already established in places such as Europe and South America. It is stated that most European Union nations include a biometric fingerprint on their national drivers’ licenses. As Europe and other countries move through the developments of biometric technology, this will inevitably result in the United States investigating and possibly being more open to this technology. With the heightened security from the September 11th attacks, acceptance of biometrics in the American market now has a great potential. With strong congressional interest, press coverage and public attention, biometrics has emerged as an item of interest in public and private sectors of the market including financial services and health care.

For instance, the growing number of identity theft and online fraud cases has been forcing financial institutions, governments and other organizations to strengthen their Internet security for a long while. On October 12, 2005, the Federal Financial Institutions Examination Council (FFIEC) released updated guidance on the risks and risk management controls needed to authenticate customers accessing Internet-based financial services. Their guidance stated that single-factor authentication (username/password) as the only control factor was inadequate for identification purposes for transactions involving access to customer information and the movement of funds. They stated that “financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks” (Authentication in an Internet Banking Environment, 2005). Biometric identification technology was stated in the guidance provided by the FFIEC as a control to strengthen online authentication. This indicated that there was already a potential demand for biometric technology for security purposes, even back in 2005. As financial institutions seek stronger security measures for online transactions and as marketing firms seek more specific data on users for marketing purposes, biometric recognition potentially gives online companies the edge they need to provide security and help them identify their users’ preferences for personalized marketing.

An Example of Biometric Technology

Biometric technology is still in the early stages of its commercial development. Currently, one device that has been gaining attention in the market and becoming more available to businesses and individuals is a fingerprint reader. The fingerprint recognition devices currently available to the general public are composed of a device that is similar to a mouse and connects to a personal computer generally via USB ports. Some examples are of such a device is DigitalPersona’s U.are.U 4500 Reader by DigitalPersona, TouchStation by LathemTime, and Secure Finger Scanner by KeyTronic. There are also PC keyboards and mouse with built-in fingerprint scanners.

Several advances have been made over the years to improve the effectiveness of these fingerprint reader devices such as matching fingerprints successfully even if a finger is placed in a different angle than the one when it was originally scanned, or if the fingerprint used is smudgy. Interestingly, it appears that most of these fingerprint readers are marketed as convenience tools to identify a user logging into a personal computer or to store usernames/passwords for logging into a website. That is, they are still used primarily for convenience, as opposed to security reasons.

On the other hand, it is unfortunate that with the emergence of new technologies there are new crimes that develop and evolve to circumvent the controls that protect the consumer. Regrettably, some crimes can become very violent and gruesome. For example, in March of 2005, a story from the United Kingdom’s BBC reported that some car thieves in Malaysia, armed with machetes, chopped off the finger of the owner of a Mercedes S-class that was protected with a fingerprint recognition system (Malaysia Car Thieves Steal Finger, 2005). They did this after they were unable to bypass the immobilizer which required the owner’s fingerprint. Although this case is extreme, it illustrates a challenge to owners of fingerprint recognition devices. As with all new technologies, companies will need to consider crimes such as this one when developing this new technology.

While we can use biometric technology to ensure that the right person is logging on to a particular computer, we cannot be sure that an intruder ends up by operating the same computer which was logged on by that “right” person. This is when the term of *behaviometrics* comes into a play.

DEFINITION OF BEHAVIOMETRICS

The word “*Behaviometrics*” derives from the terms “*behavioral*” and “*biometrics*.” In this context, *behavioral* mainly refers to a way a person behaves while *biometrics* refers to the technologies discussed above. Accordingly, *behaviometrics* focuses on behavioral patterns, instead of physical attributes, to verify the identity of an individual. So, in essence, it is behavioral biometrics (Ahmed and Traore, 2004).

One’s behavioral pattern consists of several unique “*semi-behaviors*” which are influenced by his/her social considerations as well as psychological variables. When these semi-behaviors are combined, they create a very unique behavioral profile for that individual. This profile is so multifaceted that it is practically impossible for others to replicate it.

BehavioSec, one of the most innovative security companies, has a very innovative “*continuous authentication and verification technology*” in the market (*Behaviometrics AB*, 2011). *Behavio*, one of the security software packages developed by *BehavioSec*, continuously verifies that the person sitting at the computer is indeed the intended user. In order to do that *Behavio* monitors the ways that users interact with their computers by examining their typing rhythms (keyboard strokes), mouse patterns (acceleration times, click frequencies), and graphical user interface (used programs). If these interactions do not match the users stored profiles, the program alarms or shuts down the system. Similarly, *BehavioWeb*, another package developed by *BehavioSec*, monitors the ways that the users interact with websites, compare those interactions with the profiles, and assign similarity ratios to transactions that are completed by those users. By including these ratios to the transactions, *BehavioWeb* helps the parties who are associated with those websites with their risk assessment.

Plurilock Security Solutions, Inc., another institution that is on the leading edge of the *behaviometric* technology, has similar authentication applications. The first one, *BioTracker*, measures individuals’ mouse and keystroke patterns while they are working and checks whether they are the same people they claimed to be at login or not. So even if a hacker were to phish account credentials of the person who originally logged in, he/she would still be detected and logged off the network. The second one, *PluriPass*, measures an individual’s typing patterns as he/she is typing usernames and/or passwords and checks if they match the account credentials of the user. Since both of these applications are designed to provide continuous authentication (that is, positively verifying the identity of a user in a repeated manner throughout a computing session by using *behaviometrics*), instead of static authentication which is based on having a simple username and a password, they are able to protect the online access from login to logoff (*Plurilock Security Solutions*, 2011).

While *behaviometrics* is a very promising field, it is rather new, especially when it comes to its use in this particular field. There are many studies currently underway by various parties, ranging from the Department of Homeland Security to IT specialists and academicians. It is hoped that some of these ongoing studies will result in additional tools that can supplement the options discussed above.

CONCLUDING REMARKS

While the basic components of online transactions have been improved significantly over the years, they are still far from perfect. It is imperative for information technology experts to examine the biometric technology for its incorporation, not only into hardware and/or software that are relevant, but also into commercial websites. Only when that is done properly, marketers can interact with the right individuals in their target market and worry about collecting the relevant data about these users. While this paper briefly reviewed biometric recognition tools, the author recognizes the fact that the entire spectrum of *biometrics* deserves an in-depth look in terms of its applications in various parts and aspects of online practices. Once that is done, one still needs to go beyond this particular spectrum and incorporate *behaviometrics* into the online business settings. Even though we can try to make sure that the right person is the one who initiates the online interactions, it is equally important to know that

the same “right” person is the one who continues them over time. By using biometric tools in intrusion detection applications, we may be able to focus on the areas which may not have been covered adequately by biometrics.

The research is currently underway to explore what else biometrics has to offer in this context. It is hoped that the exploratory studies, such as this one, would provide the researchers with added incentives to discover additional alternatives and help to improve this field even more...

AUTHOR INFORMATION

Dr. S. Altan Erdem earned his Ph.D. at the University of North Texas in 1991. Currently he is a Professor of Marketing and Marketing Program Chair at the University of Houston-Clear Lake. E-mail: aerdem@gmail.com

REFERENCES

1. Ahmed, Ahmed Awad E., and Traore, Issa, “Detecting Computer Intrusions Using Behavioral Biometrics,” *System Administrator: Admin*, Pages 1-8, 2004.
2. Albrecht, A., Behrens, M., Mansfield, T., McMeechan, W., Rejman-Greene, M., Savastano, M., Statham, P., Schmidt, C., Schouten, B., Walsh M., “Roadmap to Successful Deployments from the User and System Integrator Perspective,” *Biovision*, D2.6 / Issue 1.1., 2003.
3. “Authentication in an Internet Banking Environment,” October 12, 2005, http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/ots-ceo-ltr-228.pdf
4. “Biometrics AB,” May 20, 2011, <http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=40423100>
5. “Biometrics,” http://www.indexbiometrics.com/physiological_or_behavioral.htm
6. “Biometrics: Foundation Documents,” <http://www.biometrics.gov/documents/biofoundationdocs.pdf>.
7. Corcoran, David, Sims, David, and Hillhouse, Bob, “Smart Cards and Biometrics: The Cool Way To Make Secure Transactions,” *Linux Journal*, Issue 59, Article No. 7, 1999.
8. Furger, Roberta, “Who’s Watching You on the Web?” *PC World*, Vol. 18, No. 3, Pages 33-34, 2000.
9. Holahan, Catherine, “Taking AIM at Targeted Advertising,” *Business Week Online*, p. 26, 2006.
10. Jones, Mitt, “Web Privacy: How the Cookie Crumbles,” *PC World*, Vol. 18, No. 3, p. 49, 2000.
11. Koltzsch, Gregor, “Biometrics – Market Segments and Applications,” *Journal of Business Economics and Management*, Vol. 8, No. 2, Pages 119-122, 2007.
12. “Malaysia Car Thieves Steal Finger,” March 31, 2005, <http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>
13. Nanavati, S., Thieme, M., Raj, N., Navanati, R., *Biometrics: Identity Verification in a Networked World*. John Wiley and Sons, Inc., New York, 2002.
14. Pons, Alexander, “Biometric Marketing: Targeting the Online Consumer,” *Communications of the ACM*, Vol. 49, No. 8, Pages 61-65, 2006.
15. “The Business Case for Behavioral Biometric Authentication,” May 19, 2011, <http://www.plurilock.com/blog/business-case-behavioral-biometric-authentication>
16. “The Key to Biometrics Success,” http://www.checcoservices.com/publications/2005_IWA_interview.pdf
17. “University Uses Behavioral Biometrics for Online IDs,” May 9, 2010, <http://finance2business.com/business-articles/university-uses-behavioral-biometrics-for-online-ids/>
18. “Using Biometry for Security and Identification” Nov. 5, 2010, <http://www.brighthub.com/computing/smb-security/articles/63325.aspx>

NOTES