State-of-the-Art Identity Integrity Safeguard Approach in e-Commerce

Han-Foon Neo[1]*, Chuan-Chin Teo[1], Ong Thian Song[1], Devinaga Rasiah[2] and David Yoon Kin Tong[2]

Brick-and-mortar business activities are gradually being replaced by e-commerce worldwide. The number of transactions and revenue should be correspondingly higher but due to the increase in the number of fraudulent cases, especially unauthorised use of credit cards, the record remains unbreakable. The use of biometrics is an optimal solution to safeguard the online user's identity integrity. However, the best practicable way onimplementing biometrics with e-commerce is still in progress. The online user's identity integrity is important because a secure transaction that increases user confidence will directly encourage more business. Motivated by the idea "Attack is the best form of defence", hackers and imposters should be misled, traced and penalised accordingly in a proactive approach. In this paper, an intelligent state-of-the-art identity integrity safeguard framework encompassing fingerprint technology, a hiddenrisk analysis agent mechanism and real-time reporting is proposed. Since e-commerce is ubiquitous, it is possible to determine online users' attitudes from different countries which enables collaboration with a French research unit. The findings would be significant to cyberlaw makers and e-commerce merchants to promote a secured e-commerce application from the online user's perspective and consequently extend the findings to the m-commerce platform.

Key words: e-commerce; identity integrity safeguard; fingerprint; proactive; risk agent

INTRODUCTION

Electronic commerce (e-commerce), the act of virtual purchasing and trading via the Internet has transformed the way we live today. Online users have been able to buy apparels, books, music, coupons and gadgets through e-commerce portals and make instant payments with a click of a button. Examples of popular e-commerce merchants include Amazon, Cdiscount, Fnac and eBay (Statista, 2016). In Malaysia, the e-commerce market size has increased from RM 1.8 billion in 2010 to RM 5 billion in 2014 (Get Ranked, 2015). The recent #MyCyberSale 2015 campaign which generated a revenue of RM118 million (MDEC, 2016) and a record of 25 transactions per second was similar to e-commerce websites in France (Ecommerce News, 2016) proving the increasing reliance of online shopping behaviour exacerbated by the advent of the Internet.

Several innovations have been made available for online users to purchase virtually via desktops, laptops, tablets or smart phones. Online users are assured by the third party verification qualified by e-commerce merchants to ensure payment integrity. As such, encyption and digital watermarking methods have been used to enhance online transactions security and reliability. Recently, Google proposed a hands-free payment method that utilised facial verification where users did not need to take theirsmartphones out from the pocket (The Star, 2016a). Similarly, Amazon and Alibaba have integrated gesture recognition with face recognition for e-commerce activities (The Star, 2016b). Apply Pay has used near-field communication technology to transmit data between the Apple device and a contactless reader forpayment (The Star, 2016c). These methods unabashedly provide easier and convenient methods for effortless e-payment.

[1]Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
[2]Faculty of Business, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
*Corresponding author (Han-Foon Neo, e-mail: hfneo@mmu.edu.my)

Online banking, one of the most active e-commerce activities, hasvarious sensitive transactions such as money transfer and electronic fixed deposits. To ensure the security of online banking transactions, two-factor authentications (2FA) that involve password/CVC codes and SMS token/security devices have been used to prevent fraud. For instance, online banking users need to login as the first layer of authentication, followed by a security fob to further authenticate certain activities such as fund transfer and bill payments as implemented by DBS Singapore (Paul, 2016). This method is secured yet the credit card information and handphone details could be obtained bytrusted parties such as family members, friends or executers.

Technology proliferation has created critical exposures especially in monetary transactions such as identity spoofing, repudiation issues and credit card fraud. Various works have been proposed to protect e-commerce merchants from phishing, espionage, denial-of-service and malware attacks, but little attention has been given to online users (Turban *et al*., 2015). Although secured e-commerce websites with the strongest antivirus programmes, SSL certificate encryptions, public key infrastructures, intrusion detections and firewalls have been implemented, they are still in "defensive" mode. Security solutions in “defensive” mode block hackers and imposters, herein denoted as cybercriminals, and gradually become more vulnerable and susceptible to attack. Therefore,new “defensive” solutions have to be updated from time to time. As a result, the cost fore-commerce transactions have been increased which is a burden for the online user. Hence, the focus of this paper is to safeguard the user’s identity integrity in an e-commerce environment proactively as opposed to the existing “defensive” solutions.

Motivated by the idea “Attack is the best form of defence”, cybercriminals should be misled, traced and penalised accordingly. In this paper, an intelligent state-of-the-art identity integrity safeguard (IIS) framework in e-commerce based on a proactive approachhas been proposed. By building on top ofe-commerce websites, cybercriminals with stolen details would still be granted access to proceed with payments. Consequently, a hidden risk analysis agent mechanismwould be triggered to analyse users’ details such as location and fingerprint authenticity to determine the genuity of the transaction. Additionally, keystrokes would be recorded to identify the risk levels in order to generate real-time reports to notify genuine users, banks and police enforcement units. By implementing an intelligent proactive security framework from the online user’s perspective, it raises the confidence of the online user to continue promoting e-commerce transactions whererepeat purchases would lead to an increase of the nation’s GDP and prosperity.

Online users’ attitudes and intention to use the proposed IIS should be solicited from both Malaysians and French for further analysis based on the renowned Unified Theory of Acceptance, and Use of Technology 2 (UTAUT2) (Venkatesh *et al*., 2012). The purpose is to determine if there exists any cultural differences that prevent the successful use of the IIS. Hence, the findings would be significant tocyberlaw makers to refine legislations that uphold online users’ identity integrity. At the same time, the findings could educate and raise awareness on the importance of identity integrity toonline users. Moreoever, it could also provide an insight on the benefits of using the IIS to e-commerce merchants.

LITERATURE REVIEW

E-commerce provides a gateway for online users to purchase goods virtually,pay with the click of a button and have the goodsdelivered to the door step without any hustle. When a user purchases online, the conventional payment method is by credit card, which discloses the secret code (CVC) together with an SMS token or security device. Consequently, the transaction is considered successful.

However, various exposures exist in the conventional e-commerce payment method which leads to an increase of fraud cases yearly. One of the weaknesses of e-commerce activities is identity spoofing (Dinev, 2006). Identity spoofing is prevalent especially in family members and fraternalrelationships. This occurs because some websites fail to restrict access controls which areset loose to allow anyone to buy online. This vulnerability enables anyone to impersonate an authorised user with all the relevant details such as user name, password, credit card information and other credentials to successfully participate in the online transaction.

Credit card fraud is the next most common type of weakness for e-commerce (Banerjee & Karforma, 2008). Credit card fraud is defined as a wide-ranging term for theft and fraud committed involvingpayment cards, such ascredit or debit cards, as fraudulent sources of funds in a transaction. This usually happens among close friends or

family members when the unauthorised userobtained permission to use the genuine user's credit card. Credit cards, similar to all smart cards, areeasily stolen when the user forgets or misplaces the card. Additionally, unauthorised users could obtain the genuine user's credit card details easily especially when a user makes payment at physical stores such as restaurants or hotels where the card is taken and kept for some time. As a result, these exposures have led tothird party abuse of unauthorised credit cards.

Last but not least,repudiation issues might occur if the user denies and loses, or the unauthorised user misuses, steals and double spends(Song & Korba, 2004). This is due to the vulnerability of the integrity and origin of the data which reflects on the confidentiality of a user where such information could be exploited in many e-commerce websites through man-in-the-middle attacks.

In order to combat e-commerce fraud, biometric technology has beenproposed to be integratd withconventional e-commerce transactions. This is because biometrics are unique, universal, permanent and measurable (Jain et al., 2006). Vangala & Sasi (2004) and Rahimi *et al*. (2009) proposed the encryption of iris attributes in credit cards so that when an online user made a purchase, the identity could be verified by the embedded biometric feature. However, Meng (2008) argued that a single biometric feature was insufficient to cope with fraud in e-commerce because it was easy to be spoofed. Hence, he proposed the use of multi-modal biometrics, which consisted of more than one biometric feature for user verification such as a combination of finger and palm print images; and voice and signature recognition. Dhamija & Dhamija (2015) proposed a three-tier approach, involving biometrics, password and one-time-password to verify the online user's identity. Their proposed solution required e-commerce merchants and online users to have separate biometric devices.

It has been recognised that the use of biometric technology in e-commerce activities to verify an online user's identity was robust, yet it was passive which enabled hackers to manipulate biometric features via the replication of synthetic fingerprints or the fabrication of facial images. Moreover, it appeared to be selective as hackers could simply avoid attacking the e-commerce website if the payment implementation involved biometric technology. In addressing this gap, an intelligent proactive state-of-the-art identity integrity safeguard (IIS) framework has been proposed which would solve the above-mentioned problems holistically by misleading, tracing and penalising cybercriminals.

PROPOSED CONCEPTUAL FRAMEWORK

The evolvement of using credit cards forsecured online payment transactions to the implementation of 2FA with the integration of SMS tokens or security devices are common. Recently, this has progressed to involve biometric technology such as fingerprint or facial verification for online user authentication. This method lacksintelligence as it is passive and appears selective for cybercriminals. Cybercriminals could simply avoid attacking e-commerce websites which were secured with biometric technology if identity verification was required before making e-payments. Therefore, the next generation ofsecured e-commerce websites should incorporate proactive approaches which would encourage cybercriminals to engage in the transactions. A series of intelligent actions will then be executed to block their retreat.

Figure 1 illustrates a scenario and process flow of impersonation by a cybercriminal to an e-commerce website with subscription to the identity integrity safeguard (IIS) service. Since biometric authentication does not appear at the beginning of the transaction, it thus encourages the cybercriminal to complete the transaction by complying with the conventional security requirements. Upon confirmation, the transaction would appear to be successful.

As a surprise step,, an optional fingerprint authentication would emerge which leaves no means for the cybercriminal to cancel the transaction. At this stage, any delay or failure to perform identity verification would increase the risk levels in which the risk analysis agent hidden mechanism would then be executed. Additionally, the risk analysis zone would also capture keystrokes and data such as user IP, location, historical data, and correlated events to determine the risk level. For instance, if the impersonator's IP address was detected from France but the goods were to be delivered to Malaysia, this would increase the risk weight. As a proactive scheme, IIS would delay a transaction's completion time in order to trace the source and identity of the impersonator by analysing the risk ratio based on various inputs.

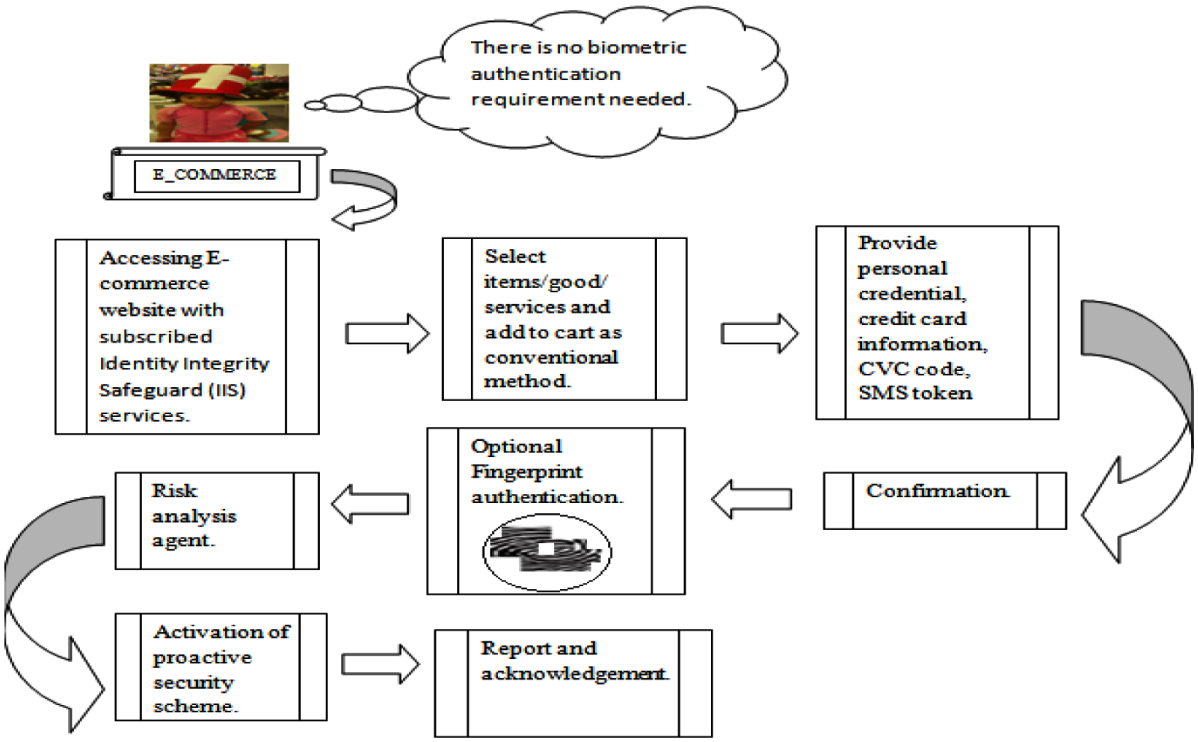

Figure 1. Process Flow of Identity Integrity Safeguard (IIS)

The concept of misleading comes in when the cybercriminal is lured into the e-commerce engagement and given notice of the successful transaction. Tracing is embedded in the IIS from the first click of the impersonator in the e-commerce website where all relevant inputs areanalysed by the risk analysis agent's hidden mechanismwhich intelligently categorises the risk levels. Last but not least, the impersonator would be penalised. IIS would generate a real-time fraud report which includes logs, trails and acknowledgements to be sent to enforcement authorities, banks and genuine users for immediate action.

CONCLUSIONS

E-commerce has transformed the traditional method of purchasing and trading for both online users and organisations. Muchattention has been given to detect and prevent cyber fraud from the organisation's perspective. However, theonline user's identity integrity is equally important. If the identity integrity awareness instilled in the online user is high, the greater the possibility that the online user would uphold and safeguard his identity from being spoofed and masqueraded. Hence, this paper proposes an intelligent proactive approach, the state-of-the-art identity integrity safeguard framework which would be capable of misleading, tracing and penalising cybercriminals. The first principle could be achieved by a conventional e-commerce portal whereby users could browse, select, checkout, and make an e-payment. The transaction would appear successful to all online users. Subsequently, the fingerprint authentication wouldbe executed after the transaction has been made. Tracing would be executed by triggering the risk analysis agent's hidden mechanismto identify the user's IP, location, credit card and credentials in this zone. A high risk weight indicates that the online user is an imposter and as a result, logs, reports, and acknowledgements would be sent to enforcement authorities, bank and genuine user for immediate action as a means of penalty. The overall concept of the proposed framework is based on the idea "Attack is the best form of defence". In the future, the IIS framework should be studied rigorously to include aspects such as an enhanced risk analysis agent which could analyse input data in depth and the implementation of IIS which does not deprive the online user of his privacy.

ACKNOWLEDGEMENTS

The authors would like to thank the French Embassyand Multimedia University, and the Mini Fund Grant (MMU/RMC/MiniFund/FIST/2015-2016/05) for the financial support provided.

REFERENCES

Banerjee, S & Karforma, S 2008, 'A prototype design for DRM based credit card transaction in e-commerce', ACM Ubiquity, vol. 9, issue 18, pp. 1-9.

Dhamija, A & Dhamija, D 2015, 'A three tier novel approach for secure user authentication and online payments', Journal of Basic and Applied Engineering Research, vol. 2, no. 2, pp. 112-116.

Dinev, T 2006, 'Why spoofing is serious internet fraud?', Communications of the ACM, vol. 49, no. 10, pp. 77-82.

Ecommerce News 2016, 2015 started better than 2014 for ecommerce in France, viewed 16 February 2016, <http://ecommercenews.eu/2015-started-better-than-2014-for-ecommerce-in-france/>.

GetRanked 2015, E-Commerce in Malaysia, viewed 16 February 2016, <http://www.getranked.com.my/e-commerce-in-malaysia/>.

Jain, A, Ross, A, & Pakanti, S 2006, 'Biometrics: a tool for information security', IEEE Transactions on Information Forensics and Security, pp. 125-143.

MDEC 2016, Malaysia's Biggest Online Sale, #Mycybersale Is Back This Year, viewed 14 February 2016, <http://www.mdec.my/media-centre/news-releases/malaysia%E2%80%99s-biggest-online-sale-mycybersale-back-year>.

Meng, X 2008, 'Study on the model of e-commerce identity authentication based on multi-biometric features identification', ISECS International Colloquium on Computing, Communication, Control, and Management, pp. 196-200.

Paul, M 2012, 'How DBS bank implements two-factor authentication', viewed 10 May 2016, < http://www.techrepublic.com/blog/asian-technology/how-dbs-bank-implements-two-factor-authentication/>.

Rahimi, A, Mohammadi, S, & Rahimi, R 2009, 'An efficient iris authentication using chaos theory-based cryptography for e-commerce transactions', International Conference for Internet Technologyand Secured Transactions, pp. 1-6.

Song, R & Korba, L 2004, 'How to make e-cash with non-repudiation and anonymity', Proceeding of the International Conference on Information Technology, pp. 1-6.

Statista 2016, Ranking of e-commerce websites in France as of first quarter of 2015, by unique visitors (in thousand of visitors), viewed 28 April 2016, <http://www.statista.com/statistics/384688/most-visited-e-commerce-websites-in-france/>.

The Star 2016a, Google testing digital wallets, viewed 4 March 2016.

The Star 2016b, Selfie for shopping, viewed 21 March 2016.

The Star 2016c, Apple pay rolls out in Singapore, viewed 21 April 2016.

Turban, E, King, D, Lee, JK, Liang, T-P, Turban, DC 2015, E-commerce security and fraud issues and protections, Electronic Commerce, part IV, pp 457-518, Springer International Publishing.

Vangala, R, & Sasi, S 2004, 'Biometric authentication for e-commerce transaction', International Workshop on Imaging Systems and Techniques, pp. 113-116.

Venkatesh, V, Thong, JYL & Xu, X 2012, 'Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology', MIS Quarterly, vol. 36, no. 1, pp. 157-178.