Challenges in Cyber Security and Mitigating Strategies

Rafiqul Islam

Senior Lecturer, School of Computing and Mathematics, Charles Sturt University, Australia
Corresponding author's E-mail: mislam@csu.edu.au

Extended Abstract

A recent worldwide report by internet security software provider Symantec, suggests that the Cybercrime is likely to increase owing to factors such as attackers gaining greater sophistication over their targets, and leapfrogging their defences. Cybercrime in Australia costs consumers around $1.06 billion a year (ACSC, 2015) and this does not include the cost to business and government, with Dell reporting some 16 million types of malware programs present in its user base in 2013 (Ayrapetov, 2013). Cybercrime data shows a greater focus on extortion of consumers and organisations, demonstrated in a worldwide increase of 113% on ransom-ware demands, and that such attacks are now moving to mobile devices (Symantec, 2015). For the digital economy in Australia and worldwide this is an issue of grave concern, as trust and dealing with perceived risk are the major pillars supporting use in this sector (Moloney, 2009; Xia et al., 2003; Ward et al., 2005). To reduce the threats of cybercrime and to gain the trust of consumers, organisations have developed a range of security measures, most recently using biometric techniques (Kessler, 2006; Usman and Shah, 2013). However, such technological innovations are only as good as company (Ng et al., 2009) and consumer practices (Whitty et al., 2015) and do not take into account malware attacks, which occur in spite of diligent user behaviour (Dang-Pham and Pittayachawan, 2015). Authentication by traditional passwords suffers from several human factors: people have difficulty remembering a huge number of secure passwords. Often passwords are written down, reused and recycled, meaning that they are easily compromised (Prince, 2012).; conversely, system administrators tend to see only the cryptographic strength and other risk factors and ignore the vital issue of human mnemonic frailty. If strong passwords are enforced, or frequent changes are required, users take unsafe shortcuts. Biometrics may be used as part of a two phase approach to change security, but ideally require no new hardware, and are thus useable virtually anywhere. But strong passwords themselves may be stolen. Users may be induced to give them up to spam or phishing attacks, or their machines may get infected by malware such as keyloggers that grab keystrokes and leak passwords. Biometrics can solve the first of these, but malware requires a different approach, with software agents designed to seek out and kill malware. Malware detectors, such as virus scanners, tend to look for common patterns in malware code. This works because such code usually shares a common DNA (Islam et al., 2012; Islam et al., 2013). But malware is now more sophisticated, with a number of techniques to foil scanners (Acoca, 2008; Saleh et al. 2014). Users are thus engaged unwillingly in an unseen protection war against malware, whilst often engaging in risky security behaviours, compromising authentication. It is then important to develop better authentication and protection technologies with an understanding of consumer, administrative and employee security behaviour and their acceptance of new innovations in this area. Without such research and implementation of both an understanding of human behaviour and advances in technology, it is likely we will fall further behind in the arms race with cybercriminals and online malicious malcontents.

The talk will aim the following:

1. To determine current user, employee and system administrator security behaviour, practices and perceptions of risk and trust and to optimise new biometric and malware algorithms in the light of this behaviour.
2. To enhance password security with biometric authentication algorithms based on video fragments of short speech utterances.
3. To invent new algorithms to detect keystroke logging which do not require prior knowledge of malware structure and match their performance to user acceptable levels.

REFERENCES

Acoca B (2008). Online identity theft. OECD Observer: Organisation for Economic Cooperation & Development, p. 12-3.

ACSC (2015). Australian Cyber Security Centre (ACSC). The Australian threat environment. In: Australian Cyber Security Centre, editor. Canberra, Australia: Australian Government.

Ayrapetov D (2013). Cybersecurity challenges. CIO (13284045), 8.

Dang-Pham D, Pittayachawan S (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. Computers & Security, 48:281-97.

Islam R, Tian R, Moonsamy V, Batten L (2012). A comparison of the classification of disparate malware collected in different time periods. Journal of Networks, 7:946-55.

Islam R, Tian R, Batten LM, Versteeg S (2013). Classification of malware based on integrated static and dynamic features. Journal of Network and Computer Applications, 36:646-56.

Kessler J (2006). Banks are expected to use more behavioral biometrics technology. ABA Bank Marketing, 38, 5.

Moloney A (2009). Online banking security and consumer confidence. Credit Control, 30: 28-9.
Symantec (2015). Internet security report.

Ng B-Y, Kankanhalli A, Xu Y (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46:815-25.

Prince B. (2012). Yahoo confirms 400,000 passwords stolen in hack. eWeek. 2012:7.

Saleh M, Ratazzi EP, Xu S (2014). Instructions-based detection of sophisticated obfuscation and packing. Military Communications Conference (MILCOM), IEEE: IEEE; 2014. p. 1-6.

Usman AK, Shah MH (2013). Strengthening e-banking security using keystroke dynamics. Journal of Internet Banking & Commerce, 18:1-11.

Ward S, Bridges K, Chitty B (2005). Do incentives matter? An Examination of online privacy concerns and willingness to provide personal and financial information. Journal of Marketing Communications, 11:21-40.

Whitty M, Doodson J, Creese S, Hodges D (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. CyberPsychology, Behavior & Social Networking, 18:3-7.

Xia Y, Ahmed ZU, Ghingold M, Boon GS, Thain Su Mei GS, Lim Lee H (2003). Consumer preferences for commercial Web site design: An Asia-Pacific perspective. Journal of Consumer Marketing, 20:10-27.