**Mobile Phishing**

According to the 2004 CSI/FBI Computer Crime and Security Survey [1], the unauthorized use of computer systems is on the decline in the USA. This may be true for reported intrusions, but a significant growth may be experienced in unreported intrusions, especially the intrusions related to financial institutions as reporting intrusions may lead to negative publicity.

The growth in the use of the Internet and the World Wide Web has lead to new types of security risks. From the moment a business obtains a web presence, there is the potential for the business systems in the organization to be exposed to security and confidentiality breaches across the entire Internet [2]. Any link to the Internet makes a business vulnerable and creates a potential intrusion risk.

Historically most of the crimes committed over the Internet were either the result of curiosity or malicious technical attack, performed by crackers. A cracker is the person who breaks security on a system. The immense growth of the Internet population using financial applications led to the introduction of two other computer criminals, called spammers and fraudsters [3]. Spam is defined as “Unsolicited commercial e-mail messages” [4] and is created by a spammer. Fraudsters are people involved in Internet fraud, a practice used by individuals who spam potential victims. These criminals cause significant damage to different role players. In 2003 alone, there were more than 200 million dollars of personal losses due to fraudulent intrusions [5]. In recent years spammers and fraudsters were joined by phishers. A phisher is involved in a fraud activity called phishing or spoofing, where phishing is defined as luring of sensitive information and spoofing is creation of a replica of an existing web page to fool a user into submitting personal, financial, or password data [4].

Phishing was first reported when America Online users were lured in the mid 1990’s by phishers to part with their user names and passwords. One intrusion technique used by phishers is the deployment of worms [6]. The W32.Mimail.I and W32.Mimail.S worms attempted to fool users into handing over credit-card information while posing as either a PayPal application or Microsoft Windows expiration notice [3].

According to a report issued by the Anti-Phishing Working Group [7], 1974 unique phishing attacks were reported to the anti-phishing organization for the July 2004 period. The organization that was targeted the most was Citibank with 682 attacks. In South Africa, eBay was targeted in July 2004. A database was discovered with more than 1000 active logins, passwords, and credit card information that could be used to purchase items on eBay’s site [8]. These kinds of attacks are categorized as identity theft [9], where the phisher may, after stealing the personal information, use this information for ‘account takeover’ or ‘application fraud’ [10].

Traditionally, Short Message Service (SMS) communication was limited to personal communication between two mobile phone users. However, this is no longer the only use of SMS technology. It is already possible to use a mobile phone to pay for parking services [11] or to transfer money from an existing contract phone to a pre-paid phone [12]. Furthermore, Ovum [13] predicts that by 2005, twenty percent of all Internet advertising will be wireless. The benefit businesses see in sending SMS’ to potential customers is that this kind of marketing is not easily ignored by the recipient.

Using SMS technology for financial transactions and marketing purposes introduce a number of security risks. Due to increasing publicity of spamming and phishing victims and advancing spam filters, the risk of being a victim of an e-mail phishing activity is decreasing. The average user is becoming more careful about clicking links included in incoming e-mails. We do believe that phishers, sooner or later will utilize SMS based phishing activities to keep their fraudulent activities continuing. One of the reasons that SMS can be a powerful tool in phishing activities is that SMS is still perceived as a more personal medium of communication when compared to e-mail. Our goal is to make stakeholders in mobile technology more aware of this threat so that in the unlikely event, they are not as vulnerable to a phishing attack as they would be if they were not informed.
There are a number of combinations by which phishing can take place via mobile technology. These combinations are based on the mediums from which the SMS messages originate and at which the information provided by potential victims is harvested. For example, an SMS message may be created and sent using an existing pre-paid account or from a web service provided by the mobile service provider (the phisher can take advantage of the convenience of a computer keyboard in sending and receiving SMS messages). Although the former case may seem inconvenient for phishing due to lack of a web interface, the existing technologies such as Bluetooth™ allow integrating cell phones with computers. The phishers may harvest the information in the same environment from which the messages originated. Alternatively, phishers can choose to harvest the information from a web server to which a user is directed for the sake of acquiring sensitive information. When a prepaid package is used for sending SMS messages, the pre-paid package (SIM card) can be discarded after a phishing activity is complete and a new service option can be acquired at minimal prices.

It is reported that, despite the widespread awareness, classical phishing activities that take place via e-mail have a success rate of 5% [7]. If a phisher can establish a feasible way to utilize mobile technology for phishing activities, one can anticipate the success rate (from a phisher's perspective) to be higher. This is because the users are not as aware of existence of such dangers in mobile technology and still perceive mobile technology as a personal means of communication.

For the future, it is necessary to research the techniques that could be used to detect a phishing attack in mobile technology. Monitoring the SMS message traffic and taking action based on the number of SMS messages having the same content may be helpful. However, such an approach needs to be backed with additional constraints to distinguish marketing (e.g. advertisement) messages from the fraudulent ones. Some distinction mechanisms can be based on calculating the distance between contents of SMS messages and keywords included in a table which contains the trusted sources.

Mobile phishing may not be a major threat for the current user, but we believe that the immense growth in applications using mobile technologies create new security threats, which the stakeholders involved in planning futuristic applications, should be aware of.

A. J. Van der Merwe (University of South Africa)    R. Seker (Texas Tech University)
School of Computing      Computer Science Department

5. FTC, Total Number of Fraud Complaints & Amount paid. 2003.