5. Defeating the Greatest Masquerade

Identity theft, phishing, identity fraud, criminal identity theft and payment instrument frauds are all examples of malicious activity that requires a successful masquerade. Even confidence fraud is a masquerade, of a criminal who claims to be an honest person in a particularly difficult or powerful situation. Why networks and databases have made it more difficult to maintain privacy, these technologies have also conversely made masquerade attacks easier. An examination of masquerade attacks can illuminate the importance of credentials, the threats that together create identity theft, and the relationship between privacy and security.

In the real-world context, an individual evaluates the amount of perceived risk in a specific context through familiarity of social and physical context. People infer knowledge about someone's "values and moral commitments on the basis of their clothing, behavior, general demeanor … or a common background". (Kim & Prabhakar 2002) An individual will trust another individual or a merchant if the other person is significantly similar to them; the similarity and hence perceived familiarity "triggers trusting attitudes". (Kim & Prabhakar 2002; Kalakota et. al., 1997) Online, those social cues are absent.

Web Spoofing and Scams

Following is a false PayPal Web page. This type of masquerade attack is called phishing. Phishing is possible because, despite the efforts in identifying consumers to merchants, there is less information for consumers to identify the merchants in return.

The lack of a proper Internet address may identify this as a scam, yet in the email the link to the address will say http://www.paypal.com. And of course a higher quality fraud would add the image of the lock and the image of the correct URL.

Note that a core part of the business plan of PayPal is to avoid the cost of fraud implemented over its payment system. For example, by using bank accounts rather than credit cards, PayPal makes disputing fraud more difficult and pays less overhead for fraud management. Thus risk is shifted to the consumer.

Unlike PayPal, this website requests a Social Security Number. Of course, one should never ever provide a Social Security Number over email or web pages. This masquerade attack is taking advantage of the fact that PayPal has convinced its customers to enter their banking information. By obtaining access to a bank account through the PayPal password, the attacker

can transfer funds to his or her own account. Unlike with credit card theft, the victim loses those funds forever. By obtaining a SSN, the attacker can implement another set of masquerade attacks.

First the attacker masquerades as PayPal to the customers of PayPal. Second, the attackers use the information from the phishing attack to obtain new accounts in false names. The individuals who fall for this attack are victimized at least twice. First the victims lose access to established accounts. Second, the victims may be held responsible for accounts opened in their names by the attackers.

The ability to misuse individual information and the importance of never sharing a SSN underscore that fact that privacy is security.

Figure 1: An Attack on PayPal Customers Using Identity Confusion

The belief that lack of privacy will make us more secure is the underlying mechanism that allows these frauds to succeed.

Notice that there is no browser lock, indicating that SSL is not in use. Therefore, in addition to the criminals implementing the masquerade attacks, all information entered on this web page is transmitted unprotected. Therefore any group of criminals (they need not be affiliated with the phishing attack) could read the information from the Web form as it crosses the network.