Information Security Threats to Network Based Information Systems

Sumeet Gupta
National University of Singapore, Singapore

INTRODUCTION

While Internet has opened a whole new world of opportunity for interaction and business by removing many trade barriers, it has also opened up new possibilities and means of criminal acts altogether unheard of in the off-line world. Why do people commit crimes online? Perhaps, some of them attempt to gain unauthorised access to other's money. Some people have fun doing so and there are others who do it to take revenge or to harm others. While the motivation of conducting criminal acts may be the same as in the off-line world, the manner of such criminal acts is unique to the Internet. The vulnerability of the information transmitted over Internet is the root cause of the sprawling of criminal acts over Internet. Both users and vendors become vulnerable to criminal acts that undermine security due to easy accessibility of Internet and easy exploitation of security loopholes in the Internet. These criminal acts can adversely affect Internet users, particularly online vendors and customers. Therefore, it is important that Internet users not only become conversant of such criminal acts but also take suitable measures to counter and avoid becoming victims of these criminal acts. In this article we examine some of the major information security threats to Internet users with particular emphasis on electronic commerce and propose plausible solutions for a safer online experience.

The information security threats can be categorised into threats to the users, threats to the vendors, and threats to both users and vendors. Electronic embezzlement, sniffing and spoofing, and denial-of-service attacks are examples of threat to the vendor. Credit card frauds and malicious codes are examples of threats to the users. Cybervandalism and phishing are examples of threats to both users and vendors.

CYBERVANDALISM

Cybervandalism is defined as an act of intentionally disrupting, defacing, or even destroying a site (Laudon & Traver, 2003). Hacking and cracking are two common forms of cybervandalism. Hacking is an act of unauthorised access to computer systems and information (Laudon & Traver, 2003). Hackers, in general, are computer aficionados excited by the challenge of breaking into corporate and government Web sites. There are three types of hackers, namely, white hats, black hats, and grey hats. White hat hackers are good hackers and are employed by the firms to locate and fix security flaws in their systems. Grey hat hackers are people who think that they are doing some greater good to the society by exposing security flaws in the systems. Black hat hackers are the one with criminal intent. Also known as crackers, black hat hackers pose the greatest threat and act with the intention of causing harm. Sometimes such hackers are merely satisfied by breaking into the files of a Web site. However, some of them a have more malicious intention of committing cybervandalism by intentionally disrupting, defacing, or even destroying the site.

Hacking is widely prevalent in the cyber industry. Recently, the publication of cartoons of Prophet Mohammed in a Danish newspaper angered hackers who then defaced the homepages of hundreds of Danish Web sites on a Saturday (Reddy, 2006). The hacking of Macs' platform is quite common (Patricks, 2006). Once the intruder gets into the system, the intruder will then be able to cause great damage to the network and its enterprise. This makes the loss of millions of dollars in a split second a high possibility. One such example is that of Network Associates (www.nai.com.br and www.mcafee.com.br), an Internet security firm whose Web sites were defaced by hackers recently. The intruders spattered cyber-graffiti over the Brazilian-based Web sites. They gained access to the Web sites by hacking

the company's host Internet service provider (ISP). But luckily none of the company's systems or information were damaged.

In e-commerce, information security and privacy are two major threats for a customer to engage in online transactions (Hoffman, Novak, & Peralta, 1999). Currently, most sites that require user login have password protection. However, passwords have many disadvantages (Conway & Koehler, 2000). They are generally chosen poorly, managed carelessly, and often forgotten. This definitely aids hackers who use these shortcomings of users to hack into accounts.

CREDIT CARD FRAUD/THEFT

A common form of hacking is credit card fraud, whereby credit card information is stolen and used (Laudon & Trevor, 2003). Credit card fraud is the most high profile e-commerce crime which compromises nonrepudiation and confidentiality of the customers. Vendors are affected the most while customers are generally insulated. This is because, while credit card companies ensure that card owners are only liable for the first 50 dollars, vendors are liable for everything they ship in unsanctioned transactions. Losses for vendors can include cost of goods, cost of shipping, administrative cost of dealing with fraudulent transactions, 'charge-back' fees that banks demand to offset their own administrative costs, and orders that online merchants reject in their determination to prevent fraud. Losses for vendors are estimated to be as much as $60 billion in 2005, according to Financial Insights (Louvel & Capachin, 2005). Stolen credit card numbers may be used by hackers to assume a new identity. Users end up paying for items that they did not purchase. Vendors in turn may have delivered the product but payment will not be made, since it is a case of stolen identity and the credit card issuers will not honor vendor's sales. For instance, Vladimir Levin broke into Citibank's system and downloaded customers' passwords, transferring $3.7 million into his account. Both Citibank and users were affected.

DENIAL-OF-SERVICE ATTACK

Denial-of-service (DoS) attack is another kind of cybervandalism. It is an attack on a computer system or a network in which the attacker floods a Web site with useless traffic to inundate and overwhelm the network (Laudon & Traver, 2003). Such an attack may cause a network to shut down, making it impossible for users to access the site. Typically, the attack consumes the bandwidth of the victim's network or overloads the computational resources of the victim's system. It tends to cause inconvenience and annoyance to the users as the network stops responding to normal traffic and service requests from clients. In addition, prolonged shutdown of the vendors' server and systems will also lead to great losses in money and reputation, as transactions with customers are paralysed. The economic damage from DoS attacks in 2004 was estimated to be around $30 billion and $37 billion worldwide (Content Wire, 2004).

Typically, in establishing a connection with the vendors' site, the user sends a message asking the vendor's server to authenticate it. The server returns the authentication approval to the user. The user acknowledges this approval and then is allowed onto the server. In a denial-of-service attack, the attacker sends several authentication requests to the server, thus filling up the server. All requests have false return addresses, so the server cannot find the user when it tries to send the authentication approval. The server waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again, tying up the service indefinitely and thus hanging up the server[1]. When such an attack is made from different computers, it is known as distributed denial-of-service.

Yahoo!, eBay, and Amazon.com are examples of such victims that were attacked in February 2002 by a Canadian teenager, resulting in huge losses (Laudon & Traver 2003).

MALICIOUS CODES

Malicious code, such as virus or Trojan horse, is software specifically designed to damage or disrupt a system. The term malware is an acronym for malicious software which are designed to infiltrate or damage a computer system, without the owner's consent. Malware generally upsets the integrity of the Internet system as it impedes the networks of both the users and the vendors. Computer viruses, worms, and Trojan horses are