

Major Security Issues in E-Commerce

Eamonn O'Raghallaigh MSc, BSc(Hons)

Executive Summary

E-commerce is defined as the buying and selling of products or services over electronic systems. A wide variety of commerce is conducted via e-commerce, including electronic funds transfer, supply chain management, online transaction processing, electronic data interchange (EDI) and automated data collection systems. US online retail sales reached \$175 billion in 2007 and are projected to grow to \$335 billion by 2012.

Any secure e-commerce system must meet four integral requirements: a) privacy – information exchanged must be kept from unauthorized parties, b) integrity – the exchanged information must not be altered or tampered with, c) authentication – both sender and recipient must prove their identities to each other and d) non-repudiation – proof is required that the exchanged information was indeed received. The financial services sector still bears the brunt of e-crime, accounting for 72% of all attacks. But the sector that experienced the greatest increase in the number of attacks was e-commerce. Attacks in this sector have risen by 15% from 2006 to 2007.

Privacy now forms an integral part of any e-commerce strategy and investment in privacy protection has been shown to increase consumer's spend, trustworthiness and loyalty. Another key development in e-commerce security and one which has led to the widespread growth of e-commerce is the introduction of digital signatures as a means of verification of data integrity and authentication.

Technical attacks are one of the most challenging types of security compromise an e-commerce provider must face. Perpetrators of technical attacks, and in particular Denial-of-Service attacks, typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, large online retailers and popular social networking sites. Technical attacks include Denial of Service (DoS), Distributed Denial of Service (DDoS) and Brute Force Attacks. Non-Technical attacks also are challenging to the security professional as they are difficult to detect and can involve 'human factors' which are difficult by nature to correct. Non-technical attacks include Phishing and Social Engineering.

In conclusion the e-commerce industry faces a challenging future in terms of the security risks it must avert. With increasing technical knowledge, and its widespread availability on the internet, criminals are becoming more and more sophisticated in the deceptions and attacks they can perform. Novel attack strategies and vulnerabilities only really become known once a perpetrator has uncovered and exploited them. In saying this, there are multiple security strategies which any e-commerce provider can instigate to reduce the risk of attack and compromise significantly. Awareness of the risks and the implementation of multi-layered security protocols, detailed and open privacy policies and strong authentication and encryption measures will go a long way to assure the consumer and insure the risk of compromise is kept minimal.

Table of Contents

1. Introduction	3
2. Privacy	4
3. Integrity, Authentication & Non-Repudiation	5
4. Technical Attacks	7
<i>Denial of Service Attacks</i>	7
<i>Distributed Denial-of-Service Attacks</i>	9
<i>Brute Force Attacks</i>	9
5. Non-Technical Attacks	10
<i>Phishing Attacks</i>	10
<i>Social Engineering</i>	10
6. Conclusions	11

1. Introduction

E-commerce is defined as the buying and selling of products or services over electronic systems such as the Internet and to a lesser extent, other computer networks. It is generally regarded as the sales and commercial function of eBusiness. There has been a massive increase in the level of trade conducted electronically since the widespread penetration of the Internet. A wide variety of commerce is conducted via eCommerce, including electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. US online retail sales reached \$175 billion in 2007 and are projected to grow to \$335 billion by 2012 (Mulpuru, 2008).

This massive increase in the uptake of eCommerce has led to a new generation of associated security threats, but any eCommerce system must meet four integral requirements: a) privacy – information exchanged must be kept from unauthorized parties, b) integrity – the exchanged information must not be altered or tampered with, c) authentication – both sender and recipient must prove their identities to each other and d) non-repudiation – proof is required that the exchanged information was indeed received (Holcombe, 2007). These basic maxims of eCommerce are fundamental to the conduct of secure business online.

Further to the fundamental maxims of eCommerce above, eCommerce providers must also protect against a number of different external security threats, most notably Denial of Service (DoS). These are where an attempt is made to make a computer resource unavailable to its intended users through a variety of mechanisms

discussed below. The financial services sector still bears the brunt of e-crime, accounting for 72% of all attacks. But the sector that experienced the greatest increase in the number of attacks was eCommerce. Attacks in this sector have risen by 15% from 2006 to 2007 (Symantec, 2007).

2. Privacy

Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for eCommerce providers. According to Consumer Reports Money Adviser (Perrotta, 2008), the US Attorney General has announced multiple indictments relating to a massive international security breach involving nine major retailers and more than 40 million credit- and debit-card numbers. US attorneys think that this may be the largest hacking and identity-theft case ever prosecuted by the justice department. Both EU and US legislation at both the federal and state levels mandates certain organizations to inform customers about information uses and disclosures. Such disclosures are typically accomplished through privacy policies, both online and offline (Vail et al., 2008).

In a study by Lauer and Deng (2008), a model is presented linking privacy policy, through trustworthiness, to online trust, and then to customers' loyalty and their willingness to provide truthful information. The model was tested using a sample of 269 responses. The findings suggested that consumers' trust in a company is closely linked with the perception of the company's respect for customer privacy (Lauer and Deng, 2007). Trust in turn is linked to increased customer loyalty that can be

manifested through increased purchases, openness to trying new products, and willingness to participate in programs that use additional personal information.

Privacy now forms an integral part of any e-commerce strategy and investment in privacy protection has been shown to increase consumer's spend, trustworthiness and loyalty. The converse of this can be shown to be true when things go wrong. In March 2008, the Irish online jobs board, jobs.ie, was compromised by criminals and users' personal data (in the form of CV's) were taken (Ryan, 2008). Looking at the real-time responses of users to this event on the popular Irish forum, Boards.ie, we can see that privacy is of major concern to users and in the event of their privacy being compromised users become very agitated and there is an overall negative effect on trust in e-commerce. User comments in the forum included: "I'm well p*ssed off about them keeping my CV on the sly"; "I am just angry that this could have happened and to so many people"; "Mine was taken too. How do I terminate my acc with jobs.ie"; "Grr, so annoyed, feel I should report it to the Gardai now" (Boards.ie, 2008).

3. Integrity, Authentication & Non-Repudiation

In any e-commerce system the factors of data integrity, customer & client authentication and non-repudiation are critical to the success of any online business. Data integrity is the assurance that data transmitted is consistent and correct, that is, it has not been tampered or altered in any way during transmission. Authentication is a means by which both parties in an online transaction can be confident that they are

who they say they are and non-repudiation is the idea that no party can dispute that an actual event online took place.

Proof of data integrity is typically the easiest of these factors to successfully accomplish. A data hash or checksum, such as MD5 or CRC, is usually sufficient to establish that the likelihood of data being undetectably changed is extremely low (Schlaeger and Pernul, 2005). Notwithstanding these security measures, it is still possible to compromise data in transit through techniques such as phishing or man-in-the-middle attacks (Desmedt, 2005). These flaws have led to the need for the development of strong verification and security measurements such as digital signatures and public key infrastructures (PKI).

One of the key developments in e-commerce security and one which has led to the widespread growth of e-commerce is the introduction of digital signatures as a means of verification of data integrity and authentication. In 1995, Utah became the first jurisdiction in the world to enact an electronic signature law. An electronic signature may be defined as “any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with the intent to authenticate a writing” (Blythe, 2006).

In order for a digital signature to attain the same legal status as an ink-on-paper signature, asymmetric key cryptology must have been employed in its production (Blythe, 2006). Such a system employs double keys; one key is used to encrypt the message by the sender, and a different, albeit mathematically related, key is used by the recipient to decrypt the message (Antoniou et al., 2008). This is a very good

system for electronic transactions, since two stranger-parties, perhaps living far apart, can confirm each other's identity and thereby reduce the likelihood of fraud in the transaction.

Non-repudiation techniques prevent the sender of a message from subsequently denying that they sent the message. Digital Signatures using public-key cryptography and hash functions are the generally accepted means of providing non-repudiation of communications

4. Technical Attacks

Technical attacks are one of the most challenging types of security compromise an e-commerce provider must face. Perpetrators of technical attacks, and in particular Denial-of-Service attacks, typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, large online retailers and popular social networking sites.

Denial of Service Attacks

Denial of Service (DoS) attacks consist of overwhelming a server, a network or a website in order to paralyze its normal activity (Lejeune, 2002). Defending against DoS attacks is one of the most challenging security problems on the Internet today. A major difficulty in thwarting these attacks is to trace the source of the attack, as they often use incorrect or spoofed IP source addresses to disguise the true origin of the attack (Kim and Kim, 2006).

The United States Computer Emergency Readiness Team defines symptoms of denial-of-service attacks to include (McDowell, 2007):

- Unusually slow network performance
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received
-

DoS attacks can be executed in a number of different ways including:

ICMP Flood (Smurf Attack) – where perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination

Teardrop Attack – A Teardrop attack involves sending mangled IP fragments with overlapping, over-sized, payloads to the target machine. A bug in the TCP/IP fragmentation re-assembly code of various operating systems causes the fragments to be improperly handled, crashing them as a result of this.

Phlashing - Also known as a Permanent denial-of-service (PDoS) is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. Perpetrators exploit security flaws in the remote management interfaces of the victim's hardware, be it routers, printers, or other networking hardware. These flaws leave the door open for an attacker to remotely 'update' the device firmware to

a modified, corrupt or defective firmware image, therefore bricking the device and making it permanently unusable for its original purpose.

Distributed Denial-of-Service Attacks

Distributed Denial of Service (DDoS) attacks are the greatest security fear for IT managers. In a matter of minutes, thousands of vulnerable computers can flood the victim website by choking legitimate traffic (Tariq et al., 2006). A distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. The most famous DDoS attacks occurred in February 2000 where websites including Yahoo, Buy.com, eBay, Amazon and CNN were attacked and left unreachable for several hours each (Todd, 2000).

Brute Force Attacks

A brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, a large number of the possible keys in a key space in order to decrypt a message. Brute Force Attacks, although perceived to be low-tech in nature are not a thing of the past. In May 2007 the internet infrastructure in Estonia was crippled by multiple sustained brute force attacks against government and commercial institutions in the country (Sausner, 2008). The attacks followed the relocation of a Soviet World War II memorial in Tallinn in late April made news around the world.

5. Non-Technical Attacks

Phishing Attacks

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing scams generally are carried out by emailing the victim with a 'fraudulent' email from what purports to be a legitimate organization requesting sensitive information. When the victim follows the link embedded within the email they are brought to an elaborate and sophisticated duplicate of the legitimate organizations website. Phishing attacks generally target bank customers, online auction sites (such as eBay), online retailers (such as amazon) and services providers (such as PayPal). According to community banker (Swann, 2008), in more recent times cybercriminals have got more sophisticated in the timing of their attacks with them posing as charities in times of natural disaster.

Social Engineering

Social engineering is the art of manipulating people into performing actions or divulging confidential information. Social engineering techniques include pretexting (where the fraudster creates an invented scenario to get the victim to divulge information), Interactive voice recording (IVR) or phone phishing (where the fraudster gets the victim to divulge sensitive information over the phone) and baiting with Trojans horses (where the fraudster 'baits' the victim to load malware onto a system). Social engineering has become a serious threat to e-commerce security since it is difficult to detect and to combat as it involves 'human' factors which cannot

be patched akin to hardware or software, albeit staff training and education can somewhat thwart the attack (Hasle et al., 2005).

6. Conclusions

In conclusion the e-commerce industry faces a challenging future in terms of the security risks it must avert. With increasing technical knowledge, and its widespread availability on the internet, criminals are becoming more and more sophisticated in the deceptions and attacks they can perform. Novel attack strategies and vulnerabilities only really become known once a perpetrator has uncovered and exploited them.

In saying this, there are multiple security strategies which any e-commerce provider can instigate to reduce the risk of attack and compromise significantly. Awareness of the risks and the implementation of multi-layered security protocols, detailed and open privacy policies and strong authentication and encryption measures will go a long way to assure the consumer and insure the risk of compromise is kept minimal.

REFERENCES

- ANTONIOU, G., BATTEN, L. & PARAMPALLI, U. (2008) A Trusted Approach to E-Commerce. *Secure Data Management*.
- BLYTHE, S. E. (2006) Cyberlaw Of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality, And Controlling Computer Access. *Journal of Internet Law*, 10, 20-26.
- BOARDS.IE (2008) Jobs.ie Security Breached.
<http://www.boards.ie/vbulletin/showthread.php?p=55521004>.
- DESMEDT, Y. (2005) Man-in-the-Middle Attack. *Encyclopedia of Cryptography and Security*.
- HASLE, H., KRISTIANSEN, Y., KINTEL, K. & SNEKKENES, E. (2005) Measuring Resistance to Social Engineering. *Information Security Practice and Experience*.
- HOLCOMBE, C. (2007) *Advanced Guide to eCommerce*, LitLangs Publishing.
- KIM, B.-R. & KIM, K.-C. (2006) Improved Technique of IP Address Fragmentation Strategies for DoS Attack Traceback. *Computer Science – Theory and Applications*.
- LAUER, T. & DENG, X. (2007) Building online trust through privacy practices. *International Journal of Information Security*, 6, 323-331.
- LEJEUNE, M. A. (2002) Awareness of Distributed Denial of Service Attacks' Dangers: Role of Internet Pricing Mechanisms. *NETNOMICS*, 4, 145-162.
- MCDOWELL, M. (2007) Cyber Security Tip ST04-015. IN TEAM, U. S. C. E. R. (Ed.) *United States Computer Emergency Readiness Team*.
- MULPURU, S. (2008) B2C eCommerce Expected To Top \$300B In Five Years. *Forrester Research*, 1-7.
- PERROTTA, N. (2008) Be on guard for ID-theft schemes. *Consumer Reports Money Adviser*, 5, 2-2.
- RYAN, E. (2008) DPC urges Jobs.ie customers to be wary. *ENN*.
<http://www.enn.ie/story/show/10124134> ed.
- SAUSNER, R. (2008) Could the U.S. Be the Next Estonia? *Bank Technology News*. SourceMedia, Inc.
- SCHLAEGER, C. & PERNUL, G. (2005) Authentication and Authorisation Infrastructures in b2c e-Commerce. *E-Commerce and Web Technologies*.
- SWANN, J. (2008) Beware of Disaster Phishing Scams. *Community Banker*, 17, 15-15.
- SYMANTEC (2007) Attacks rise as e-tailers lag finance sector on security. *Computer Weekly*, 4-4.
- TARIQ, U., HONG, M. & LHEE, K.-S. (2006) A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques. *Advanced Data Mining and Applications*.
- TODD, B. (2000) Distributed Denial of Service Attacks.
http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-whitepaper.html.
- VAIL, M. W., EARP, J. B. & ANTAN, A. L. (2008) An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies. *IEEE Transactions on Engineering Management*, 55, 442-454.