

E-Commerce/Network Security Considerations


Carl S. Guynes, University of North Texas, USA
Yu 'Andy' Wu, University of North Texas, USA
John Windsor, University of North Texas, USA

ABSTRACT

E-Commerce security issues can be grouped under the categories of system availability, data integrity, and data privacy. System availability means that all necessary components are available to support a given users transmission requirements. Data integrity means that all valid messages that are sent are received, messages are not altered in such as way as to make them invalid, and unauthorized messages are not introduced and transmitted over the network. Data privacy means that transmitted messages contain only 'need to know' information and are seen only by their intended audience. Enterprise network security is typically reactive, and relies heavily on host security. This approach creates complicated interactions between protocols and systems that can cause incorrect behavior and slow response to attacks. Network security at both the e-commerce and customer sites must be constantly reviewed and suitable countermeasures must be planned. The security of a site depends on the security of the internal systems and the security of external networks.

Keywords: E-commerce Security; Denial of Service; Enterprise Networks; Visualization

INTRODUCTION

 -commerce security deals with two strategic issues; i.e., protecting the integrity of the business network and its internal systems and accomplishing transaction security and privacy between the customer and the business. E-commerce security needs to be addressed not only at the business site with its servers/network, but also on the client side, which includes direct connection to home computers. It is this group of computers that are most vulnerable to attacks because of its low level of user security training or awareness.

Transaction security is important in order to support customer confidence in a particular e-commerce site. It depends on the organization's ability to ensure privacy, authenticity, integrity, availability and the blocking of unwanted intrusions. Transaction privacy can be threatened by unauthorized network monitoring by software devices called sniffer programs. Transaction privacy has become one of the most well-known security issues replacing theft and fraud as top concerns in e-commerce.

Transaction confidentiality requires the removal of any trace of the actual transaction data from intermediate sites. Encryption techniques, such as secret-key, public-key and digital signatures, are the most common method of ensuring transaction privacy, confidentiality and integrity. The common weakness of these techniques is that they depend on the security of the endpoint systems to protect the keys from modification or misuse. Transaction integrity requires methods that prevent the transactions from being modified in any way while it is in transit to or from the customer.

E-COMMERCE SECURITY ISSUES

E-Commerce security issues can be grouped under the categories of system availability, data integrity, and data privacy. System availability means that all necessary components are available to support a given users transmission requirements. Data integrity means that all valid messages that are sent are received, messages are not

altered in such a way as to make them invalid, and unauthorized messages are not introduced and transmitted over the network. Data privacy means that transmitted messages contain only 'need to know' information and are seen only by their intended audience.

Threats to systems availability include accidental or intentional destruction of hardware, software, or transmission media, and the malfunction of any of the e-commerce components. Some of the risk reduction measures for systems availability are environmental monitoring, network component monitoring, physical access control, and such basic measures as having a business contingency plan and cross-training personnel.

Efforts must be made to reduce the risks of integrity problems by implementing physical access controls, software controls, and message authentication controls. The security system must perform recurring verification of data completeness and accuracy, and have built-in hardware and software error detection and correction routines. More traditional security measures such as separation of duties, formalized operating procedures, and adequate training can also reduce losses due to integrity problems.

Privacy threats facing an e-commerce system include unauthorized access and inappropriate disclosure of private information. This unauthorized disclosure can result in invasion of privacy litigation being brought against a company. Risk reduction measures in the area of privacy involve such actions as the encryption of sensitive data, restricting the access to personal data, physical shielding of transmission of facilities, and establishing a policy addressing the confidentiality of corporate data. Even though early security techniques utilized a strategy of simply limiting access to corporate data, today's client's demands for data availability create a new subset of related security issues. To successfully manage an e-commerce environment, there must be a balance between cost, security, risk, performance, and connectivity. The spiraling increase in technological complexity, especially in networks, and the evolving view of information as an asset that must be protected have brought the concept of network security to the forefront.

There are numerous network security and access control issues to be considered when implementing an e-commerce system. As the server is usually the central location for critical data, adequate physical security and operational security measures need to be taken to insure the safety of the data. Although there are a large number of tools available to perform security and control functions on mainframe systems, there are significantly less tools available that are designed specifically for e-commerce systems. Until these tools are developed, companies must exercise extreme caution when placing mission critical applications on an e-commerce system. The end-user computing evolution provided computing power at the workplace, and resulted in end-user demand for access to corporate data with little regard for the security of that data.

DENIAL OF SERVICE ATTACKS

Denial of service attacks pose a serious challenge to networks as a whole and especially to the Internet. In addition to the strategies in place to control the attack, preventing the attack helps in saving essential network resources [10]. Businesses that completely rely on web-based transactions will continue to be vulnerable to Denial of Service (DoS) attacks. DoS attack scripts are the most common, effective and easiest to implement attacks available on the WEB. No actual damage is done to the victim site instead the access paths to it are simply weighed down with incoming packets. The Distributed Denial of Service (DDoS) attacks are the latest evolution of DoS attacks and their success depends on the inability of intermediate sites to detect, contain and eradicate the penetration of their network. The more intermediate sites compromised, the more sites are available to launch a DDoS attack against a victim site. Internet sites are vulnerable if site managers do not perform standard patch maintenance and do not monitor their systems regularly with any intrusion detection tools. DDoS attacks worked because sites failed to detect the initial compromise of their systems. The compromises could have been prevented if standard system maintenance had been performed. Proper system administration training is the easiest method of countering this and other types of attacks. The Distributed Denial of Service (DDoS) attacks demonstrate that business sites do not maintain adequate security protection and intrusion detection measures. Some sites do not detect compromise, which can occur months before an actual DDoS attack. Automated security updates are another feature that could be used to help limit the scope of these attacks. The security of a site depends on the security of the internal systems and the security of external networks. Software developers need to design software that is engineered for safety and security [11].

CLIENT RESPONSIBILITY

Cable modems, DSL connections and other high speed direct connect mechanisms for connecting to the Internet has created an entirely different set of security issues. The migration of DDOS attack tools to the Windows OS now allows a hacker to use these direct connect systems as another base of operation. The ISP's responsibility to maintain network integrity and create a model for containing any attack with their domain is important. The client's main responsibility deals with the requirement of e-commerce sites to acknowledge the rights of the customer, to examine their credit history and to be provided with information about who gets the information. E-commerce businesses should develop orientation programs for their customers that teach about basic security practices. This will help to ensure confidence in the business's ability to secure and protect the customer information.

ENTERPRISE NETWORK SECURITY MEASURES

Enterprise network security is typically reactive, and relies heavily on host security. This approach creates complicated interactions between protocols and systems that can cause incorrect behavior and slow response to attacks. One solution is to imbue the network layer with mechanisms for dynamic access control by using a system for securing enterprise networks, where the network elements themselves enforce dynamic access control policies based on both flow-level information and real-time alerts. One such systems, Resonance, uses programmable switches to manipulate traffic at lower layers; these switches take actions to enforce high-level security policies based on input from both higher-level security policies and distributed monitoring and inference systems [9].

Evaluating the security of a computer network system is a challenging task. Configurations of large systems are complex entities in continuous evolution. The installation of new software, a change in the firewall rules, or the discovery of software vulnerability can be exploited by a malicious user to gain unauthorized control of the integrity, availability and confidentiality of the assets of an organization [7].

Network security at both the e-commerce and customer sites must be constantly reviewed and suitable countermeasures must be planned. The security of a site depends on the security of the internal systems and the security of external networks. The majority of security breaches on the Internet occur at the endpoints, i.e., the local network, rather than on the main "backbone" of the Internet [2]. The most commonly used e-commerce security measure is the use of access limitation procedures. These procedures can be divided into the categories of network access, data access and client access. Network access deals with enabling the system to recognize that a user exists and has usage rights. This is facilitated by employing user profiles which include passwords, user IDs and specify which parts of the mainframe database are accessible to the user. The user profile resides in the file server or mainframe side of a network transmission. At the conceptual micro/user end of the message, physical terminal restrictions should be used. When the application of user profiles on an individual basis creates an undesirable amount of overhead, some companies move to the use of heterogeneous group access. Lower-level groups of people with similar access needs get the same access allocations. This compromise position, while easier to implement, increases access risks.

Data access procedures specify and limit the number of individuals who can view a file, can change a file, or can copy a file. The file access system should provide multiple combinations of read, write and delete privileges which can be set at the file, record, or field level. Prerequisite to determining file parameters, all information should go through data classification, with appropriate restrictions determined for each class. Typical classes would be non-critical data, critical corporate data, and personally sensitive data. Many of today's network products provide security utilities that help identify potential security problems.

Client access can be challenging for secure e-commerce because companies cannot control what users do with their web browsers, which is the interface between the user and e-commerce sites. A good example is SQL injection. Programmers often obtain textual information users enter into textboxes on Web pages, such as user names, account numbers, order numbers, etc. These pieces of textual input are then intermixed with programming code to create SQL statements that query or update databases. An enterprising user may append to the normal input some extra text that bears syntactical meaning in SQL. If programmers fail to write code to prevent such malicious input, the resulting SQL statements can be much more powerful than intended for normal e-commerce. They can return

information that should not be disclosed to a remote, regular user. This can include sensitive columns in database tables (e.g., passwords), administrative tables, metadata about the database, etc.

A fundamental tool for security is encryption. Modern cryptography implements sophisticated algorithms to transform plain text with processes such as permutation and substitution of bits. Today's computing power allows the processes to be performed in large number of iterations within a split second, hence scrambling the plain text into something beyond recognition unless the encryption key is available. Most of the time, the attacker is left with brute force attack as the only option, i.e., to exhaust all possible combinations of characters allowed by the length of the key. Specifically for e-commerce, the Secure Socket Layer (SSL) technology takes advantage of encryption to secure the information exchange between a client (user's browser) and the server. The two go through a process known as SSL handshake to arrive at an agreement on what encryption algorithm and key to use for encrypting the communication session. The session then proceeds with text exchanged only in scrambled form. Another important function of SSL uses the public key infrastructure so that a client can verify the true identity of the server before it decides to trust the server for conducting the transaction. Server identity validation is mandatory in SSL. Optionally, if the environment requires added security, SSL can be configured to require client identity validation.

One of the more neglected technical procedures is traditionally backup and recovery. Even though users are aware of the fact that systems fail, they are not always willing to prepare for the eventuality of its failure. A positive suggestion for keeping a system up is to perform the necessary backups. An effective backup plan should recognize the entire data flow, from information origin through processing. Backup procedures must be set for both daily activities and for exceptions. The main goal of periodic file backup is to minimize recovery requirements. A vast majority of this effort is at the server level. Therefore the most exposure is left at the client level. This is primarily because periodic backup often depends on user discipline. A client's upload capability is an advantage in this case because the client can make use of standardized server backup procedures. Periodic tests of the backup plan are essential to continually determine if the plan fits with the changing company.

Another security tool is the use of firewalls. A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. Firewall policies are needed to conduct performance testing as well as configuration analysis. They are mainly used to protect the internal network of businesses. The original design of a firewall was supposed to allow only specific services (e.g., email, web access) between the Internet and the internal network but have now become a major point of defense in the e-commerce security architecture [12]. However, just because a firewall is in place does not mean that the site is secure. Installation of firewalls can bring about a false sense of security, if no efforts are spent to ensure that they are configured correctly and that logs from the firewalls are constantly monitored, analyzed, and acted upon.

Network security decision-making is hard for both humans and machines. This is because security decisions are context-dependent, require highly dynamic, specialized knowledge, and require complex risk analysis. Multiple user studies show that humans have difficulty making these decisions due to insufficient information and bounded rationality. However, current automated solutions are often too rigid to adequately address the problem and leave their users more confused and inept when they fail. A mixed-initiative approach, in which users and machines collaborate to make security decisions and make use of complementary strengths rather than weaknesses, is a much better approach. [4]

Given the increasing dependence of our societies on networked information systems, the overall security of these systems must be continually measured and improved. Existing security metrics have generally focused on measuring individual vulnerabilities with minimal consideration of their combined efforts. Some network models incorporate temporal factors, such as the availability of exploit codes or patches to help provide both a theoretical foundation and a practical framework for continuously measuring network security in a dynamic environment. [3]

Network security is gravitating towards more centralized control. Strong centralization places a heavy burden on the administrator who has to manage complex security policies and be able to adapt to users' requests. To be able to cope, the administrator needs to delegate some control back to end-hosts and users, a capability that is missing in today's networks. Delegation makes administrators less of a bottleneck when policy needs to be modified and allows network administration to follow organizational lines. IT should use protocols to request information from end-hosts

and networks on the path of a flow, and one that allows users and end-hosts to participate in network security enforcement by providing information that the administrator might not have or rules to be enforced on their behalf. [8]

VISUALIZATION

Visualization is any technique for creating images, diagrams, or animations to communicate a message and for making data more comprehensible. Corporations are usually not able to react quickly enough toward security incidents because their security staffs are flooded by information difficult to interpret. A possible solution to this problem is to build efficient visualizations based on more pertinent information by having fewer but higher-level parameters collected on the endpoints and then centralized on the network [5].

The growth of the Internet has been accompanied by the growth of e-commerce. This proliferation of e-commerce has put large quantities of consumer private information in the hands of the service providers, who in many cases have mishandled the information, either intentionally or unintentionally, to the detriment of consumer privacy. As a result, government bodies have put in place privacy legislation that spells out a consumer's privacy rights and how consumer private information is to be handled. Providers are required to comply with such privacy legislation. IT management should use visualization as a tool that can be used by security or privacy analysts to understand how private information flows within and between provider organizations, as a way of identifying vulnerabilities that can lead to non-compliance [13].

The increasing availability of network test beds and the benefits of visualization-based security study call for the emergence of supporting tools for network security research. IT should consider using an integrated specification and visualization toolkit that supports network experimenters to conduct interactive experiments on network test beds. Some visualization toolkits feature a combination of topology-based network animation for global awareness and detailed data analysis support through a complete set of data conversion, data selection, and graphical analytical tools [6].

TECHNICAL CONSIDERATIONS

Technical knowledge requirements for security personnel have increased dramatically in the last decade. The software, involving operating security system, data validation software and security modules of the network programming, has become more sophisticated [1]. Signal interceptions are another technical consideration in any e-commerce environment and must be detected quickly. They are especially dangerous because hackers can intercept passwords, which usually precede transmissions. The fiber optics media is almost impossible to tap because it does not generate a magnetic field and any physical break-in will break the light beams, thus triggering an alarm.

Line media selection pre-determines some technical security measures. For instance, satellite channel detection is easy, so transmissions must be encrypted. However, this media covers long distances, so compared to multi-node land-based systems, it has fewer interception and repeater locations. Fiber optics cables are much more compact than copper wires, which makes them easier to conceal and, as mentioned before, are difficult to tap without detection. They are also relatively free from electrical interference, but are very difficult and expensive to install, repair, expand using existing lines. Wireless networks are especially vulnerable to security threats. With wireless technology data packets are in open air and susceptible to monitoring, spoofing, and even network impairment. Encryption schemes are a major solution to these risks.

DESIGN FOR SECURITY

In addition to the prevention of security breaches, security design must also facilitate evaluating violations and analyzing the degree to which data has been mis-handled. A primary tool to accomplish this is the extensive use of audit trails. These are especially valuable with undetected intruders. Another security design strategy emphasizes layers of redundancy, with each subsequent layer reducing the overall vulnerability of the system. Disk integrity, for example, can be achieved by using two copies of directories and files. Mirroring is the most basic disk redundancy design. This design simply utilizes two disks and all write commands are performed on both drives. Another disk integrity technology is called RAID (redundant array of inexpensive disks). RAID allows several disks to function as

one. This design breaks files into logical blocks and stores redundant copies of each block on two or more disks.

The trade off, of course, is that each new layer of security has a corresponding cost. The procedure for creating all of the newly needed control objectives is fairly straight-forward. First, develop a rationale for objectives, and then define the conditions under which the objectives are satisfied. In the user-oriented world, however, these have to be explained to and accepted by users. The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the e-commerce systems personnel to read and implement. Educating the consumer on security issues is an ongoing process but will prove to be the most critical element of the e-commerce security architecture.

CONCLUSION

Historically, information systems executives have had the technical knowledge required in the new world of security, but lacked the political clout and authority to make sure that daily use by end users is kept secure. It is essential to have a proactive attitude toward network crime rather than a reactive one. Effectively, a shift of responsibilities up the corporate ladder has occurred. There must be a changeover of what kind of manager is responsible for overall security of information. Concurrent with the changing face of security has been a changing view of what non-IS management must understand and take responsibility for. What used to be considered too technical for non-IS management is now often a part of its responsibilities.

AUTHOR INFORMATION

Dr. Carl S. Guynes is a Regents Professor of Information Systems at the University of North Texas. He received a doctorate in quantitative analysis from Texas Tech University. Dr. Guynes' areas of specialization are client/server computing, end-user computing, data administration, and information resource management. His most recent research efforts have been directed in the areas of client/server computing and data administration. Some of the journals in which Dr. Guynes has published include *Communications of the ACM*, *Information & Management*, *The Journal of Information Systems Management*, *Journal of Accountancy*, *Journal of Systems Management*, *The Journal of Database Management*, *The CPA Journal*, *The Journal of Computer Information Systems*, *Information Strategy*, *Computers and Security*, and *Computers and Society*.

Dr. Yu “Andy” Wu is an assistant professor in the Department of Information Technology and Decision Sciences, College of Business at the University of North Texas. He received a Ph.D. in Management Information Systems from the University of Central Florida, Orlando, FL, in 2007. His primary research interests include information security and social networks. His research papers appeared in various information systems journals and conferences. Before his academic career, Dr. Wu had experiences administering a corporate network. He has obtained network- and security-related certifications from Cisco, Microsoft, Novell, and CompTIA.

Dr. John C. Windsor is a professor of Information Systems and former Director of the Information Systems Research Center at the University of North Texas. He received his Ph.D. in Decision Sciences from Georgia State University. He has published six books and over 60 articles in such journals as *Data Base*, *IIE Transactions*, *Information & Management* and *Computers & Security*. His research interests include software and data engineering, systems security, collaborative computing, and the organizational impact of information technology.

REFERENCES

1. Al-Shaer, Ehab, Latifur Khan, and Mohammad Ahmed. “A comprehensive objective network security metric framework for proactive security configuration.” Proceedings of the 4th annual workshop on Cyber security and information intelligence research. Vol. 288 Article No. 42, (2008).
2. Al-Shaer, Ehab, Latifur Khan, and Mohammad Ahmed. “Dynamic security policy Learning.” Proceedings of the first ACM workshop on Information security governance, (2009):39-48.
3. Frigault, Marcel, Ling Wang, Anoop Singhai, and Sushil Jajodia. “Measuring network security using dynamic bayesian network.” Proceedings of the 4th ACM workshop on Quality of protection (2008): 23-30.

4. Greenstadt, Rachel, Sadia Afroz, and Michael Breenan. "Mixed-initiative security agents." Proceedings of the 2nd ACM workshop on Security and artificial intelligence (2009): 35-38.
5. Hertzog, Patrick. "Visualizations to improve reactivity towards security incidents inside corporate networks." Proceedings of the 3rd international workshop on Visualization for computer security (2006): 95 – 102.
6. Li, L., P. Liu, and G. Kesidis. "Visual toolkit for network security experiment specification and data analysis." Proceedings of the 3rd international workshop on Visualization for computer security. (2006): 7 – 14.
7. Montanari, Mirko, and Roy Campbell. "Multi-aspect security configuration assessment." Proceedings of the 2nd ACM workshop on Assurable and usable security configuration (2009):1-6.
8. Naous, Jad, Ryan Stutzman, Mazieres Mckeown, David Nick, and Nick Zeldovich . "Delegating network security with more information." Proceedings of the 1st ACM workshop on Research on enterprise networking. (2009):19-26.
9. Nayak, Ankur, Alex Reimers, Nick Feamster and Russ Clark. "Resonance: dynamic access control for enterprise networks." Proceedings of the 1st ACM workshop on Research on enterprise networking. (2009):11-18.
10. Padmanabhan, Jayashree, K. Easwarakumar, B. Gokul and S. Hanshankar. "Trust based traffic monitoring approach for preventing denial of service attacks." Proceedings of the 2nd international conference on Security of information and networks. (2009):200-206.
11. Parvin, Sazia, Shohrab Ali, Song Han, and Tharam Dillon. "Security against DoS attack in mobile IP communication." Proceedings of the 2nd international conference on Security of information and networks.(2009):152-157.
12. Samak, Taghrid, Adel El-Atawy, and Ehab Al-Shaer. "Towards network security policy generation for configuration analysis and testing." Proceedings of the 2nd ACM workshop on Assurable and usable security configuration. (2009):45-52.
13. Yee, George. "Visualization for privacy compliance." Proceedings of the 3rd international workshop on Visualization for computer security (2006): 117 – 122.

NOTES