2000

A Tutorial on Web Security for E-Commerce

Robert J. Boncella
Washburn University, zzbonc@washburn.edu

A Tutorial on Web Security for E-Commerce

Dr. Robert J. Boncella, Computer Information Science Department, Washburn University
zzbonc@washburn.edu

Abstract

This tutorial will be an overview of the major categories of web site attacks, their effects and their possible countermeasures. The overview will have as its focus the web security necessary for a reasonable guarantee of secure e-commerce.

This tutorial is intended for those who have little or no knowledge of web security and its importance to e-commerce. At the conclusion of this tutorial attendees will have a basic understanding of the needs and techniques of web security as it applies to e-commerce.

Introduction

The world wide web (WWW or web) is an interconnection of networks of computer systems that provides information and services to users of the web. Computer systems in this interconnection of networks that provide services and information to other computer systems are called Web Servers. Computer systems that request services and information are call Web Browsers. The communication channel between the web browser (client) and web server (server) is established by an Internet Service Provider (ISP) that allows access to the web for both the server and client. The communication of the client with server follows a request/response paradigm. The client, via the communication channel makes a request to a server and the server responds to that request via a communication channel.

The web is a two way network composed of three components: web servers, web users, and a communication path connecting the servers and browsers. As such, web security requirements will be more extensive than a multi-user computer system or stand alone local area network.

Web Security

A general definition of web security is provided by Garfinkel and Spafford 1997.

"… (W)eb security is a set of procedures, practices, and technologies for protecting web servers, web users, and their surrounding organizations. Security protects you (the user) against unexpected behavior."

Users and providers of web services have a set of assumptions regarding expected behavior of the web with regard to security.

From the users' perspective their expectation is the service being provided is legitimate, safe, and private; legitimate in the sense the services or information being supplied by the web server is the web server the user expects to provide those services or information; safe in the sense that the services or information being provide will not contain computer viruses or content that will allow the user's computer system to be used for malicious purposes. And finally, respecting the client's privacy, the provider of the requested information or services will not record or distribute any information the user may have sent to the provider in order to request information or services.

From the server's perspective their expectation is the requestor of the information or services is legitimate and responsible; legitimate in the sense the user has been accurately identified; responsible in that the user will not attempt to access restricted documents, crash the server, or use the server computing system as means of gaining illegal access to another computer system.

From the perspective of both the server and the user, they have an expectation that their communications will be free from eavesdropping and reliable in terms that their transmissions will not be modified by a third party.

Risks to Avoid

The purpose of web security is to meet the security expectations users and providers. To that end, web security is concerned with client-side security, server-side security and secure transmission of information.

Client-side security is concerned with the techniques and practices that protect a user's privacy and the integrity of the user's computing system. The purpose of client-security is to prevent malicious destruction of a user's computer systems; e.g. by a virus that might format a user's fixed disk drive and to prevent unauthorized of use of a user's private information; e.g. use of a user's credit card number for fraudulent purposes.

Server-side security is concerned with the techniques and practices that protect the web server software and its associated hardware from break-ins, web site vandalism, and denial of service attacks. The purpose of server-side security is to prevent modification of a web site's contents, prevent use of the server's hardware, software, or databases for malicious purposes, and to ensure reasonable access to a web site's services i.e. to avoid or minimize denial of service attacks.

Secure transmission is concerned with the techniques and practices that will guarantee protection from eavesdropping and intentional message modification.

The purpose of these security measures is to maintain the confidentiality and integrity of user and server information as it is exchanged through the communication channel

Web Security and E-Commerce

With respect to e-commerce web security has as its main focus web sever security and secure transmission. There is some concern with client-side security. However the client can be greatly assured that the client's security expectations will be met if the web server and transmission channel are secure in the sense suggested above.

The reason for this focus is the nature of e-commerce. E-commerce can be simply defined as the exchange of goods and services for money. This exchange is transacted electronically generally via the web. Buyers - clients - seek out reliable providers of the goods and services they require.

Web server security is concerned with preventing attacks on web sites. There are several ways to classify attacks on web sites in order to understand their nature. The classification used in this tutorial partitions web site attacks into two broad categories: attacks on web site information and web site accessibility. Within attacks on web site information an overview of threats on a web site's information integrity and confidentiality will be given. Within attacks on a web site's accessibility overview of denial of service and invalid authentication threats will be presented.

Overview of Web Site Attacks

The following outline presents a summary of possible web site attacks. This outline is a slight modification of information presented in Rubin et al. 1997. For each of the two broad categories of information and accessibility attacks the outline presents an overview of the threats, consequences, and prevention that are relevant for web security and e-commerce. The tutorial is loosely organized around the information presented in the following outline.

I. Attacks on Web Site Information
   A. Integrity of Information Attacks
      1. Threats
         a. Modification of user data
         b. Trojan Horse browser
         c. Modification of memory
         d. Modification of message traffic in transit
      2. Consequences
         a. Loss of information
         b. Compromise of machine
         c. Vulnerability to all other threats
      3. Countermeasures - cryptographic checksums
   B. Confidentiality of Information Attacks
      1. Threats
         a. Eavesdropping on the Net
         b. Theft of info from server
         c. Theft of data from client
         d. Info about network configuration
         e. Info about which client talks to server
      2. Consequences
         a. Loss of information
         b. Loss of privacy
      3. Countermeasures
         a. Encryption
         b. Web proxies

II. Attacks on Web Site Accessibility
   A. Denial of Service Attacks
      1. Threats
         a. Killing of user threads
         b. Flooding of machine with bogus requests
         c. Isolating machine by DNS attacks
      2. Consequences
         a. Disruptive
         b. Annoying
         c. Prevent user from getting work done
      3. Countermeasures - difficult to prevent
   B. Authentication Attacks
      1. Threats
         a. Impersonation of legitimate user
         b. Data forgery
      2. Consequences
         a. Misrepresentation of user
         b. Belief that false information is valid
      3. Countermeasures - cryptographic techniques

Tutorial Outline

The following is a brief and somewhat tentative outline of the tutorial. A general review of the networking concepts necessary for e-commerce will be presented. These concepts are used to implement web security measures to counter the risks of conducting business using the web.

I Review of Web Concepts for E-Commerce
   A. Client/Server Applications
   B. Communication Channels
      1. Internets and Intranets
      2. TCP/IP Protocol - language of the Internet

II. Typical E-consumer to E-business Transaction.
   A. Web Security Threats in these Transactions
   B. Security Threats Not Handled by Encryption

III. Security Threats and their Countermeasures
- A. Information Security Threats Countermeasures
  - 1. Internet Cryptography Techniques
  - 2. Transport Layer Security
    - a. SSL (Secure Sockets Layer)
    - b. TLS (Transport Layer Security)
  - 3. Application Layer Security
    - a. SET (Secure Electronic Transaction)
    - b. PGP (Pretty Good Privacy)
  - 4. Web Proxies and Firewalls
- B. Access Security Threats Countermeasures
  - 1. Denial of Service
    - a. Types of DOS attacks
    - b. Preventive measures
  - 2. Authentication (Access Control)
    - a. Username/Password authentication
      - i. Password Creation
      - ii. Kerberos
      - iii. Smart Cards
    - b. Alternative Authentication - Biometrics

After August 15, 2000 this tutorial presentation will be available at

http://www.washburn.edu/cas/cis/f_bob.html.

Bibliography

Atkins, D., Buis, P., Hare, C., Kelley, Nachenberg, C., Nelson, A.B., Phillips, P., Ritchey, T., Sheldon, T., and Snyder, J., *Internet Security Professional Reference Second Edition*, New Riders, Indianapolis, IN, 1997.

Denning, D., and Denning, P.J., *Internet Besieged Countering Cyberspace Scofflaws*, ACM Press, New York, NY, 1998.

Drew, G. *Using SET for Secure Electronic Commerce*, Prentice-Hall, Upper Saddle River, NJ, 1999.

Garfinkel, S. and Spafford, G. *Web Security & Commerce*, O'Reilly and Associates, Cambridge, MA, 1997.

Rubin, A., Geer, D., and Ranum, M., *Web Security Sourcebook*, Wiley, New York, NY, 1997

Smith, R.E., *Internet Cryptography*, Addison-Wesley, Reading, MA, 1997.

Stallings, W., *Network Security Essentials: Applications and Standards*, Prentice-Hall, Upper Saddle River, NJ, 2000.

Stein, Lincoln D., *Web Security: A Step-by-step Reference Guide*, Addison-Wesley, Reading, MA, 1998.