South African Journal
of Information Management
[DoE accredited]

Student Work

Vol.2(2/3) September 2000

Web site security? Is the threat real?

J. Schoeman
mwmachan@mweb.co.za

Contents

1. Introduction
2. What is Web security and why is it necessary?
3. Terms associated with Web site security
4. Dimensions of Web site security
5. How can Web sites be secured?
6. Conclusion
7. References

1. Introduction

With more than 80 million users in over 200 countries, the Internet has very rapidly grown in size and status to become the world's most universal IT resource, and an indispensable business tool.

Everyone is eager to use it: Consumers like its convenience and the opportunity to 'window-shop' right around the globe. Merchants appreciate its low-cost, high-yield global market reach. Corporates like the opportunity for faster, more effective communication with staff, customers, suppliers, banks and other business associates. And, of course, everyone likes the wealth of information it puts right at his or her fingertips.

But for all its undoubted strategic merit, the Internet remains an open, public network that offers users no guarantee of information security, privacy or integrity. For competitive businesses large and small, this is very much its shadow aspect and a major cause for concern.

But is the Blade Runner-esque world of cybercrime, hackers and computer viruses the creation of slick marketing, merely preparing the world for an array of security products or is Web site security a grossly neglected aspect of users and corporations' interface with the Internet? Is the threat real?

top

2. What is Web site security and why is it necessary?

According to Stein (1998:1), Web security is different things to different people. For some, it's the ability to browse the Web in peace, knowing that no one is looking over their shoulders. For others, it’s the ability to conduct financial and commercial transactions safely. For the operators of Web sites, it’s confidence that their sites will not be vandalized by pranksters or used as a gateway to break into their local area network.

There are a number of reasons why protection is required when connecting to the Internet or to any other external network. It is firstly important to remember that security is not built into the Internet itself and the security of external networks cannot be guaranteed as they can be compromized themselves. Most of the host operating systems on the Internet have ineffective integral security measures. The large number of Internet users means that there are many possible sources of abuse. Socially irresponsible users, competitors, disgruntled employees and ex-employees who have access to the Internet may compromise security where there is a loophole to exploit and motivation to attack (Doddrell, 1996:6).

This type of attacks can take various forms and include passive attacks active attacks, and denial of service attacks (MacGregor, Aresi and Siegert., 1996:3)

2.1 Passive attacks

In a passive attack, the perpetrator simply monitors the traffic to try to learn secrets. Such attacks can be either network based (tracing the communication links) or system based (replacing a system component with a Trojan Horse that captures data insidiously). Passive attacks are the most difficult to detect.

2.2 Active attacks

In these the attacker is trying to break through the defences. There are several types of active attack such as system access attempts, spoofing and cryptographic attacks.

2.3 Denial of service attacks

In this case the attacker is not so much trying to learn the secrets as to prevent operation, by re-directing traffic or by bombarding a user with so-called 'spam'.

top

3. Terms associated with Web site security

3.1 Firewalls

Firewalls are software programs that are the cornerstone of network security infrastructure (Middleton, 2000:1). Doddrell (1996:7) describes these as 'a logical barrier which provides some protection for corporate information from the Internet or other networks'. The main operation of firewalls has not changed much over the years. Development is geared towards firewalls inter-operating with other products to provide a wider, more complete solution. Firewalls are installed at the gateway between the company network and the Internet. They are good at preventing unwanted access but cannot, for example, stop viruses entering the network.

3.2 Authentication and/or authentication servers

Authentication in a digital setting is a process whereby the receiver of a digital message can be confident of the identity of the sender and/or the integrity of the message (Forcht and Fore, 1995:28). Authentication of users is a difficult task. Using simple password schemes is no longer viable to secure access to a system. Increased sophistication of security devices such as strong authentication via Biometric scanners offers a variety of solutions to the problem of ensuring only authorized users gain access to a system. Public Key Infrastructure (PKI) and encryption are both increasingly being used by large organizations. Mobile computing compounds the problem of authentication. Companies with remote users, such as employees who work from home, need additional authentication mechanisms, such as digital certificates or tokens, to secure their networks.

3.3 Viruses and virus scanners

Viruses are programs that have the ability to destroy computer data files, programme files, entire disk surfaces, and sometimes even computer hardware (Howard, 1995:107). Virus scanners are therefore necessary, as viruses have caused a lot of damage over the past few years. They tend to attack weaknesses in operating systems or working practices. Viruses can easily be transported from one system to another, which makes controlling them difficult (Van der Merwe, 2000a:1). According to various experts, viruses represent a much bigger problem than hackers – it is therefore critical to ensure that content is virus-protected.

top

4. Dimensions of Web site security

According to Ellis (2000:1), data transfers are typically secured using a firewall, strong encryption technology, digital certification, and either SSL (secure sockets layer) or SET (secure electronic transactions) channel support.

MacGregor *et al.* (1996:2) place security objectives into one or more of the following five categories: Access control, authentication, integrity, accountability and privacy.

Middleton (2000:1) is of the opinion that networks must be adequately protected from both external and internal security threats. In this regard four distinct areas of concern can be delineated:

The first is *infrastructure*, where firewalls and authentication products protect the network against intruders.

The second concerns the *security of content*, for example from viruses.

Then comes the area of *operational compliance*, where security involves audit, assessment and intruder detection.

The final category is *application security*, which is security developed specifically to protect individual applications.

top

5. How can Web sites be secured?

Van der Merwe (2000b:1) offers various guidelines which could be employed to protect Web sites and to reduce unauthorized access. These include:

- Build a wall. If you have not yet installed a firewall to protect the Web service running your site, do so immediately. This is the first line of defence against hackers.
- Separate the public and the private. Make sure that the Web servers running your public Web site are physically separate and individually protected from your internal

corporate network. If someone were to hack into your Web site, you would want to prevent that person from having a point of entry into your corporation's sensitive data.
- Do it right the first time – configure properly. It is believed that 70% of sites with certified commercial firewalls are still vulnerable to attacks because of misconfiguration and improper deployment.
- Poke holes before the bad guys do. Use scanning tools to determine the potential vulnerabilities associated with all of your systems that are Internet accessible.
- Watch traffic like a hawk. Put host-based intrusion-detection agents on your Web servers and monitor activity, looking for any irregularities.
- Issue licences to buy. If you are conducting e-commerce on your Web site, secure your transactions with digital certificates.
- Develop Web content off-line. Set up a staging area internally where relatively important data is held and reviewed before being posted to your Web site. Make this area password-protected and enforce the password component.
- Protect your database. If your Web site retrieves dynamic content from a database, consider putting that database behind a second interface on your firewall, with tighter access rules that interface to your Web server.
- Do not forget your trading partners. If you have an extranet site for dealing with your business partners, create extra security for it. Because you are communicating across the Internet, you are only as strong as your weakest link. Trading partners need to put firewalls in place and should conduct security audits, just as you are doing.
- Harden your Web server. If you are extremely security conscious, consider a 'hardened' Web server product, which comes with a locked-down OS and compartmentalized networking subsystem.

top

6. Conclusion

Considering the evidence in hand, one has to come to the conclusion that the violation of Web site security is a very real (and potentially damaging) threat to Web sites on the Internet.

'There is, after all, very little business benefit in being able to transfer vital company data thousands of kilometres in seconds via Internet-enabled e-mail, if that information can be just as quickly and easily intercepted, used and abused by competitors', comments Tim Ellis, MD at the South African Certification Agency (SACA).

The problem facing electronically accessible companies today is the conflict between the demand for wider access to information and the need to protect that information from misuse. In the past, the majority of companies grossly under-estimated the complexity of issues to be considered in implementing an information security (infosec) solution. Doddrell (1996:5) rightly remarks that information security is often given a low priority because the business impact potential is not fully appreciated.

Part of the problem has been that Web site security has traditionally been seen as an IT and not as a management responsibility. Management conveniently forgets that, in the final instance, it is still people using or abusing the technology and an effective information security policy therefore has to be formulated, applicable to both individuals inside the company as well as to individuals interacting with the company by electronic means. Security should also be seen as an ongoing process, requiring constant auditing and review.

Security is, without a doubt, going to feature heavily in computer systems of the future. Protecting Internet content has unleashed a business whose value will rise to US$952 million in 2004 from US$66 million in 1999, according to market researchers International Data Corporation (IDC) (Anon., 2000:1). With the e-commerce industry on the increase, secure payment systems will become the driving force and ensure the success of this industry.

top

7. References

Anon. 2000. $1 billion to be spent coping with e-mails, Net – IDC.

[Online] Available WWW: http://196.36.119.109/sections/monitor/2000.

Doddrell, G.R. 1996. Information security and the Internet. Internet Research, 6(1): 5–9.

Ellis, T. 2000. The Internet – your business ally only if it is secured! [Online] Available WWW: http://196.36.119.109/sections/techforum/2000.

Forcht, K.A. and Fore R.E. 1995. Security issues and concerns with the Internet. Internet Research, 5(3): 23–31.

Howard, G.S. 1995. Introduction to Internet security: from basics to beyond. Rocklin, Calif.: Prima Publishing.

MacGregor, R.S., Aresi, A. and Siegert, A. 1996. WWW.SECURITY: How to build a secure World Wide Web connection. Upper Saddle River, N.J.: Prentice-Hall.

Middleton, G. 2000. Firewalls only the start of effective corporate security. [Online] Available WWW: http://196.36.119.109/sections/techforum/2000.

Stein, L.D. 1998. Web security: a step-by-step reference guide. Reading, Mass.: Addison Wesley.

Van der Merwe, J. 2000a. Keeping it safe: the future of information security. [Online] Available WWW: http://196.36.119.109/sections/techforum/2000.

Van der Merwe, J. 2000b. Ten tips to protect your Web site. [Online] Available WWW: http://196.36.119.109/sections/techforum/2000.

Disclaimer

Articles published in SAJIM are the opinions of the authors and do not necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user’s use of the Website.

ISSN 1560-683X

Published by InterWord Communications for the Centre for Research in Web-based Applications,
Rand Afrikaans University