IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Internet Security against Hacking System

Ms. Pooja D. Jaiswal[1], Dr. Harshalata J. Petkar[2]

Student, Dept. of Computer Science, Dr. Babasaheb Nandurkar College of Physical Education Yavatmal[1]

HOD, Dept. of Computer Science, Dr. Babasaheb Nandurkar College of Physical Education Yavatmal[2]

Abstract: The internet has been a wide usage in all the fields in the present competitive world. It is used in education, business, research and everything. So it provides security for user's information or transactions or any other data in every field. In other words, the security attacks are made either by the hackers or the intruders, the ways how they attack and exploit to illegitimate means.This paper is an overview of the security and privacy concerns based on the experiences as developers of E-commerce.E-commerce is a business application that is used to do transaction between the retailers to the customer.And also it is used to do trading between manufacture and supplier. Here we present you the better ways of how to defend from the attacks and protect your personal data without depending on the network provider's security with the help of personnel firewalls and honey pots.

Keywords: Network security, Hacking, Authentication, Authorization, Encryption, Decryption

1. INTRODUCTION

E-Commerce is use to exchange the goods and services over the internet. All major retail brands have an online presence, and many brands have no associated traditional paves. E-Commerce also applies to business to business transactions.E-Commerce provides an integrated platform that runs both their customer facing online shopping sites, and their internal distributor or supplier portals as shown in Figure.

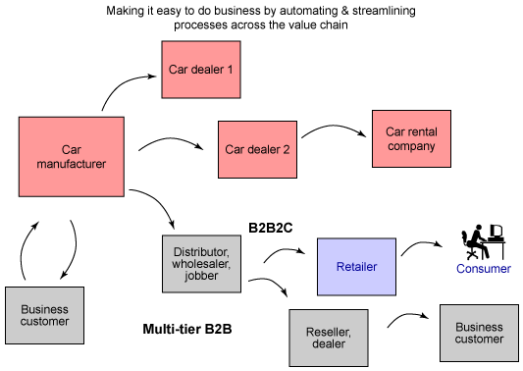

Fig:-1 making it easy to do business by automating & streamlining processes across the value chain

E-Commerce systems are relevant for the services industry. For example, online banking and services allow customers to retrieve bank statements online, transfer funds, pay credit card payment, buy and sell securities, and get financial guidance and information.

2. SECURITY OVERVIEW AND ITS FEATURES

A secure system accomplishes its task with no unintended side effects. Using the equivalence of a house to represent the system, you decide to carve out a piece of your front door to give your pets' easy access to the outdoors. However, the hole is too large, giving access to housebreakers. You have created an unintended implication and therefore, an insecure system. While security features do notgain guarantee to provide secure system, they are necessary to build a secure system. There are four categories:

- Authentication: Verify the user is authentic. It enforce that only one can logon on to specific account.
- Authorization: Only you can manipulate your resources to make ways.
- Encryption: Mapping the original contents,with releases.
- Auditing: Keeps a record of operations.

3. THE VICTIMS AND THE ACCUSED (THE PLAYERS)

In a typical e-Commerce experience,A shopper visit to web site and browse a catalog and make a purchase. There areat mostfour major players in e-Commerce security. One player is the shopper who uses their own browser to locate and relocate the site and the same is usually operated by a merchant, players, whose business is to sell merchandise to make a profit. As the merchant business is selling services and goods, not build software, he usually purchases most of the software to run his site from other-party software vendors. The software vendor is the last of the three legitimate players

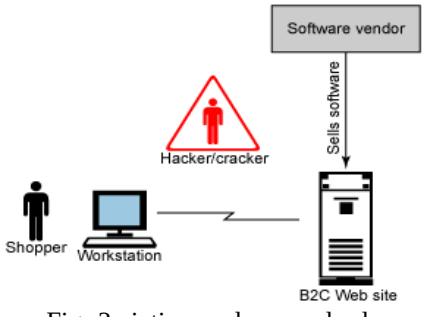

Fig:-2 victims and accused role

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

A threat is a possible to attack on the system. It does not mean that the system is vulnerable to the attack.But it is not necessarily be known by the attacker. Vulnerabilities is an entry and exit points to the system. In a house, the vulnerable points are the windows and door. As Figure shows, there are following points that attacker can target:

- Shopper
- Shopper' computer
- Network connection between shopper and Web site's server
- Web site's server
- Software vendor

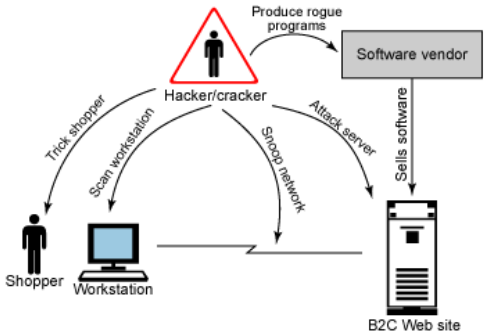

Fig: 3 tricking the shopper

3.1 Tricking the shopper:

It is also known as social engineering techniques, some are easiest and most profitable attacks are based on tricking the shopper. These attacks involve surveillance of the shopper's correlated tasks, collecting information to use against the shopper. For example, a mother maiden name is a common challenge question used by most of the sites. If one of these sites is tricked into giving away a password once the challenge question is provided, then not only has this site been compromised, but it is most likely to have that shopper used the same credentials on other sites. Snooping the shopper's computer: Millions of computers are added to the network every month. Almost every users' knowledge regarding security, is vulnerable of their systems is vague at best. A popular technique for gaining entry into the shopper's system is to use a tool, such as SATAN, to perform port scans on a computer that detect entry points into the machine. Based on the opened ports found, the attacker can use numerous techniques to gain entry into the user's system. Upon entry, they scan your lotdata for personal information, such as passwords. A user that purchases firewall software to protect his computer may find there are conflicts with other software on their system. To resolve the conflict, the user disables enough capabilities to render the firewall software useless.

3.2 Sniffing the network:

In this scheme, the attacker monitorsto the data between the shopper's computer and the server. There are enormous points in the network where this attack is more conscious than others. If the attacker sits in the middle of the network, then within the scope of the Internet, this attack becomes impractical. A request from the client to the server computer is broken up into small pieces known as packets as it leaves the client's computer and is fabricated at the server. The packets of request are sent through different ways. The attacker cannot access all the packets of a request and cannot decipher.

3.3 Guessing passwords:

Another common technique is to guess a user's password. This style of attack is traditional or automated. Traditional attacks are laborious, and only successful if the attacker knows something about the shopper. For example, if the shopper uses their Favorite color as the password.

Using server root exploits: Root exploits refer to techniques that gain super user access to the server. This is the most coveted type of exploit because the possibilities are limitless. When you attack a shopper or his computer, you can only affect specific individual. With a root exploit, you gain control of the merchants and all the shoppers' information on the site. There are two main types of root exploits:

- Buffer overflow attacks
- Executing scripts against a server

4. DEFENSE

Despite the survivals of hackers and crackers, e-Commerce remains a safe and secure activity. The resources available to large companies involved in e-Commerce are enormous. These companies will pursue every legal route to protect their customers. Figure represent a high-level illustration of defenses available against attacks.

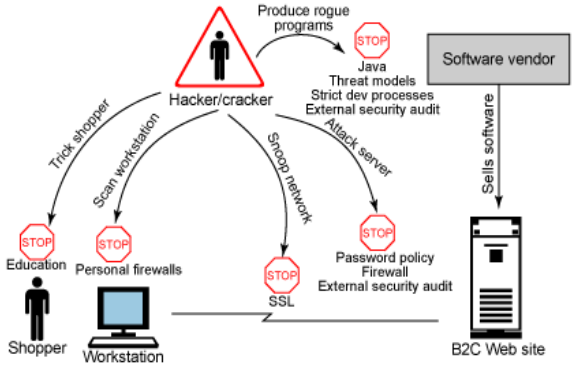

Fig 4: Defense fig

4.1 Education:

Your system is only as secure as the people who use it. If a shopper chooses a weak password, or does not keep their password confidential, then an attacker can act as that user. Users need to use good judgment when giving out information, and be knowledgeable about possible phishing schemes and other social engineering attacks.

4.2 Personal firewalls:

When connecting your computer to a network, it becomes vulnerable to attack. A personal firewall helps protect your computer by limiting the types of traffic initiated by and directed to your computer. The third party can also scan the hard drive to detect any stored passwords.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

4.3 Secure Socket Layer (SSL):

Secure Socket Layer (SSL) is a protocol that encrypts data between the shopper's computer and the site's server. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents.

The SSL certificate is issued to the server by a certificate authority authorized and authenticated by the government. When a request is raised through the shopper's browser to the site's server using https://..., the shopper's browser checks if this site has a certificate it can recognize. If the site is not recognized by trusted certificate authority, then the browser issues a warning as shown in Figure

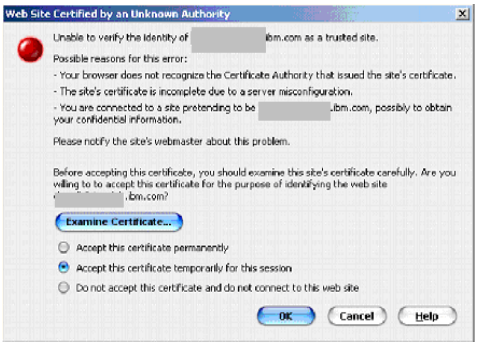

Fig 5: who cookies work

- For example in Mozilla:
-

Fig 6: secure icon in Mozilla Firefox

4.4 Server firewalls:

A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines. A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. This allows the client browser to communicate with the server. A second firewall sits behind the e-Commerce servers. This firewall is heavily fortified, and only requests from trusted servers on specific ports are allowed through. Both firewalls use intrusion detection software to detect any unauthorized access attempts.

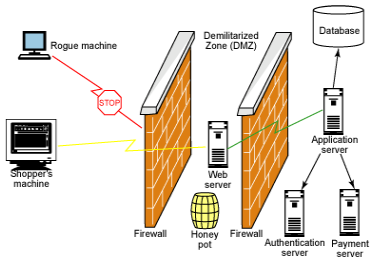

Fig 7: Figure shows the firewalls and honey pots.

4.5 Password Policies:

Ensure that password policies are enforced for shoppers and internal users. We may choose to have different policies provided by federal information standard, shoppers versus your internal users. Say, one may choose to lockout an administrator after three failed login attempts instead of six. These password policies protect against attacks that attempt to guess the user's password. They ensure that passwords are sufficiently strong enough so that they cannot be easily guessed.

Site development best practices

There are many fabricated policies and standards for avoiding security issues. However, they are not required by rules and norms.

Some of the basic rules include:

- Never store a user's password in plain text or encrypted text in the system. Instead, use a one-way Hashing Algorithm to prevent password extraction.
- Deploy external security consultants (ethical hackers) to analyze your system.
- Standards, such as the Federal Information Processing Standard (FIPS), describe guidelines for implementing features. For example, FIPS makes recommendations on password policies, etc.

Security best practices remain largely an art rather than a science, but there are some good guidelines and standards that all developers of e-Commerce software should follow.

5. USING COOKIES

One of the issues faced by Web site designers is maintaining a secure session with a client over subsequent requests. Because HTTP is stateless, unless some kind of session token is passed back and forth on every request, the server has no way to link together requests made by the same person. Cookies are a popular mechanism for this. An identifier for the user or session is stored in a cookie and read on every request. You can use cookies to store user preference information, such as language and currency. The primary use of cookies is to store authentication and session information. A secondary and controversial usage of cookies is to track the activities of users.

Using an online security checklist

This security checklist is to protect buyers as a shopper-

Whenever you logon, register, or enter private information, such as credit card data, ensure your browser is communicating with the server using SSL.

- Use a password of at least 6 characters, and ensure that it contains some numeric and special characters (for example, c0113g3).
- Avoid reusing the same user ID and password at multiple Web sites.
- If user is authenticated (logged on) to a site, always logoff after work done.
- Use a credit card for online purchases. Most credit card companies will help you with non-existent or damaged products.

6. USING THREAT MODELS TO PREVENT EXPLOITS

When architecting and developing a system, it is important to use threat models to identify all possible security threats on the server. Think of the server like your house. It has doors and windows to allow for entry and exit. These are the points that a burglar will attack. A threat model seeks to identify these points in the server and to develop possible attacks.

Threat models are particularly important when relying on A third party vendor for all or part of the site's infrastructure. This ensures that the suite of threat models Is complete and up-to-date.

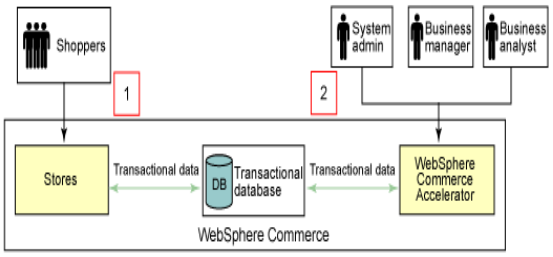

Fig 8: Threat mod

7. CONCLUSION

This paper outlined the key players and security attacks and defenses in an e-Commerce system. Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the shopper to be vigilant when shopping online.

Resources

- Learn about social factors in computer security.
- A good introduction to computer security.
- Low level tips for writing secure code.
- An example of a denial of service attack.

REFERENCES

[1] Sanctum Inc, “Ethical Hacking techniques to audit and secure web enabled applications”, 2002.
[2] B. Reto, “Ethical Hacking”, in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002.
[3] B. Kevin, “Hacking for dummies”, 2nd edition, 408 pages, Oct 2006.
[4] Smith B., Yurcik W., Doss D., “Ethical Hacking: the security justification redux”, IEEE Transactions, pp. 375-379, 2002.
[6] J. Danish and A. N. Muhammad, “Is Ethical Hacking Ethical? “ , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.
[7] Ajinkya A. Farsole, Amurta G. Kashikar and ApurvaZunzunwala , “Ethical Hacking, International journal of Computer Applications (0975-887), Vol. 1 No. 10, pp. 14-20, 2010.
[8] edia.techtarget.com/search Networking-Introduction to ethical hacking-Tech Target.
[9] H.M David, “Three Different Shades of Ethical Hacking: Black, White and ray,” in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.
[10] D. Manthan “Hacking for beginners”, 254 pages, 2010. Ajinkya A., FarsoleAmruta G., KashikarApurvaZunzunwala" Ethical Hacking", in 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 –No. 10.
[12] David Melnichuk," The Hacker’s Underground Handbook ", at http://www.learn-how-to-hack.net.
[13] Marilyn Leathers " A Closer Look at Ethical Hacking and Hackers" in East Carolina University ICTN 6865.
[14] Ethical hacking by C. C. Palme
[15] D. Irani, S. Webb, K. Li, and C. Pu, “Large online social footprints - an emerging threat,” in Proceedings of the 2009 International Conference on Computational Science and Engineering , August 2009.
[16] A. Narayanan. (2008, November) Lendingclub.com: A de-anonymization walkthrough. [Online]. Available: http://33bits.org/2008/11/12/57/
[17] L.-S. Huang and C. Jackson, “Clickjacking attacks unre-solved,” July 2011.
[18] A. Narayanan and V. Shmatikov, “Robust de-anonymization of large datasets,” in Proceedings of the 2008 IEEE Sympo- sium on Security and Privacy, May 2008.
[19] “De-anonymizing social networks,” in Proceedings of the 2009 IEEE Symposium on Security and Privacy, May 2009.
[20] A. Acquisti, R. Gross, and F. Stutzman, “Faces of Face-book,” in Black Hat 2011, August 2011.