ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 6, Issue 12, December 2018

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

An Effective Counter Measure of Attacks for Secured Online Transactions

Dr. Deepu Saini
Department of Computer Science
Guest Lecturer in Adarsh Mahila Mahavidyalaya,
Bhiwani (Haryana) – India.

***Abstract:** In the current scenario of online era, it requires to have a complete countermeasure to defuse the attacks by the attacker to provide the safeguard to online transactions. Therefore, a model during testing to check each and every step in providing security through this proposed model of e-commerce network security i.e. a complete countermeasure. This combination of Action and Underlying Countermeasures, united and decentralized during performance is special characterized in this security model. A security guard of building regularly checking the ID cards etc. and an action taken by Rapid Action Force during any attack are the best similar to the both of above countermeasures.*

***Keywords:** countermeasure, action, underlying, security, enablers, integrity.*

I. Introduction

In the current scenario of online era, it requires to have a complete countermeasure to defuse the attacks by the attacker to provide the safeguard to online transactions. Therefore, a model during testing to check each and every step in providing security through this proposed model of e-commerce network security i.e. a complete countermeasure. All the countermeasures are collaborated and integrated together to perform the action fulfilling the purpose of study. The potential errors will come out during the testing period. While experiment will also make us familiar with the limitation inherited in the model. As the name suggests, testing will present all the possible lacking in the entire system in actual. If found, will be removed.

It is important in testing of security, the testing of addition developed parts along with the entire resulted system. For newly introduced or we can say an additional part is tested by acquiring the Security Certification, which will prove whether the system will meet the requirements and inherit with all the specifications. Generally, certification is done by others than the designers.

Another security test is Accreditation, which covers the whole system inspite of only new developed or adopted parts of system in the form of review of its operations and controls.

An action by team of football is the same as our security model defuse all the attacks. A companion ready to receive the ball kick by a sportsperson to him will always be followed by the rival person to fail his prospective attack. In the security model also, on the identification of any Security Principle, there are high chances of Security Attack by Enablers. In this situation, this security model proposed Counter Measure which will follow every prospective Security Attack. An integration of countermeasures to follow the enablers and decentralization of countermeasures, as per their characteristics, to defuse the attack is the summary of the study. The countermeasures for before attack and after attack are required separation in working for fast and quick healing. An Action Countermeasure is the defender which works just after attack by attacker such as closes the account which is currently opened and an Underlying Countermeasure is of having the characteristics i.e. defendable nature which does not literally perform any action but perform its task of defending at regular basis which itself avoid the particular attack. For example the security of Captcha or user name password allows to proceeds in execution. The comparison of e-commerce network system is quite must to find out the counter measures to stop the attack after reviewing the fields where lack of security is lying in the whole system.

II. 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.

III. Denial Service of 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.

IV. 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).

V. 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.

VI. 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.

VII. Integrity, Authentication & Non-Repudiation

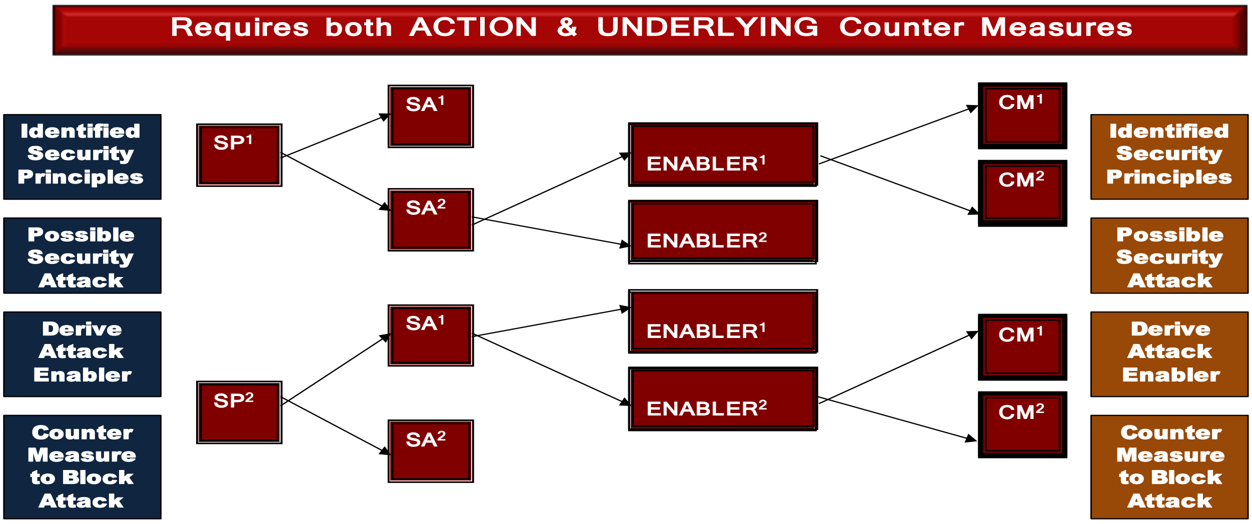
In any e-commerce system the factors of data integrity, customer & client authentication and non-repudiation are critical to the success of any online business. Data integrity is the assurance that data transmitted is consistent and correct, that is, it has not been tampered or altered in any way during 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.

VIII. Action Counter Measure


Requires both ACTION & UNDERLYING Counter Measures
Identified Security Principles
Possible Security Attack
Derive Attack Enabler
Counter Measure to Block Attack
SP¹
SP²
SA¹
SA²
SA¹
SA²
ENABLER¹
ENABLER²
ENABLER¹
ENABLER²
CM¹
CM²
CM¹
CM²
Identified Security Principles
Possible Security Attack
Derive Attack Enabler
Counter Measure to Block Attack

An action by team of football is the same as our security model defuse all the attacks. A companion ready to receive the ball kick by a sportsperson to him will always be followed by the rival person to fail his prospective attack. In the security model also, on the identification of any Security Principle, there are high chances of Security Attack by Enablers. In this situation, this security model proposed Counter Measure which will follow every prospective Security Attack. An integration of countermeasures to follow the enablers and decentralization of countermeasures, as per their characteristics, to defuse the attack is the summary of the study. The countermeasures for before attack and after attack are required separation in working for fast and quick healing. An Action Countermeasure is the defender which works just after attack by attacker such as closes the account which is currently opened.

IX. Underlying Counter Measure

An Underlying Countermeasure is of having the characteristics i.e. defendable nature which does not literally perform any action but perform its task of defending at regular basis which itself avoid the particular attack. For example the security of Captcha or user name password allows to proceeds in execution. The comparison of e-commerce network system is quite must to find out the counter measures to stop the attack after reviewing the fields where lack of security is lying in the whole system.

X. Conclusion

The identification of Security Principles and possible security attacks by finding the Enablers, the requisite countermeasures are adopted to perform security action is the prime working of this methodology.

During various phases, the existing status of security principles/measures are required to be studied by going through of pros & cons which are inherit in current available security measures and compared. After NIST study, we have to identify & to select the three security principles. i.e. Privacy, Integrity & Authentication. For every principle a design of countermeasure model will be derived.

The main objective of our proposed study is to avail the appropriate countermeasure security model for existing e-commerce network system and also to the upcoming network system.

The complete architecture of design documents took place in actual form. Testing will present all the possible lacking in the entire system in actual. If found, will be removed.

The application of countermeasures leads to achieve the objective for which the complete model is launched and hence, are used to get the best possible results of achieving the objective for which it is formed.

References

1. Rolf Oppliger, Ralf Hauser b, 1, David Basin c, 'SSL/TLS session- aware user authentication or how to effectively thwart the man - in -the- middle'. 23 March 2006
2. Baja and Nag, 'E – Commerce', TMH Publications.
3. Z. Djuric, Securing money transactions on the Internet, 2005.
4. Z. Djuric, Secure internet payment System"ITCC-2005.
5. Kaliski Jr, B.S. and Yin, Y. L., September 1998, 'On the security of the RC5 Encryption Algorithm', 2006.
6. Z. Djuric, Ognjen Maric 'Internet payment System', Journal of University Computer Science -2007.
7. A R Dani1, P Radha Krishna and V Subramanian 'An Electronic Payment System Architecture for Composite Payment Transactions', 2007.

AUTHOR(S) PROFILE

Deepu Saini, received the Ph.D. degree in Computer Science from Singhania University Pacheri Bari Jhunjhunu Rajasthan –India in the year of 2018 and Full Time M.Sc. Computer Science from Rajiv Gandhi Govt. College for women Bhiwani Haryana-127021 this college is affiliated to M.D.University (State University of Haryana) Rohtak Haryana. From 2008 (after Complete my M.Sc. Computer Science Degree) teaching in Adarsh Mahila Mahavidyalaya, Bhiwani (Haryana) in B.Sc. Computer Science Department.