Web Attacks

MODULE 14

Contents

Web Attacks

14.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Define cyber-attacks and cyber warfare.
- Categorize specific cyber-attacks.
- Explain Spoofing
- Define Repudiation
- Differentiate between Personally Identifying Information (PII) or non-PII information
- Explain Denial-of-Service attack
- Define SQL injection attack

14.2 INTRODUCTION

The web application plays a very important in today's people's lives. The first generation of web application were limited by static HTML applications. Later on, the internet and web access became quite ubiquitous and the user's expectations from web application also increased many folds. Common gateway Interface (CGI) provided a big leap in the direction of modern web applications. The users were facilitated with more features like, searching, hosting uploading etc. The CGI provided more interactive forms over internet for the users to interact. Newer more advanced frameworks came into foray like, PHP, ASP.NET, J2EE, AJAX, Ruby on Rails, and others. These aspects resulted into more user involvement and hence securing these web applications became incredibly important. This was also due to the fact that the information processed by web applications became very critical to customers, corporations and organizations including countries. There can be very critical information managed through web applications nowadays like financial data, medical records, social security numbers, intellectual property and national security data. Web applications needs to handle this information with utmost care and security.

14.2.1 Cyber-attack

Cyber-attack is any type of offensive manoeuvre employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated and dangerous.

14.2.2 Cyber Warfare and cyber terrorism

Cyber warfare utilizes techniques of defending and attacking information and computer networks that inhabit cyberspace, often through a prolonged Cyber campaign or series of related campaigns. It denies an opponent's ability to do the same, while employing technological instruments of war to attack an opponent's critical computer systems. Cyber terrorism, on the other hand, is "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population." That means the end result of both cyber warfare and cyber terrorism is the same, to damage critical infrastructures and computer systems linked together within the confines of cyberspace.

There were two such instances between India and Pakistan that involved cyberspace conflicts, started in 1990s. Earlier cyber-attacks came to known as early as in 1999.Since then, India and Pakistan were engaged in a long-term dispute over Kashmir which moved into cyberspace. Historical accounts indicated that each country's hackers have been repeatedly involved in attacking each other's computing database system. The number of attacks has grown yearly.

14.3 TYPES OF WEB ATTACKS

Firstly, let us have a look into various types of attacks that happen in web arena. Categorizing all web attacks is quite difficult as more and more different ways of attacking gets introduced and evolved. While the security is tightened the attacker also evolve to find more new ways to attack into web. Major types of web attacks are:

i. Spoofing.
ii. Repudiation.
iii. Privacy attacks.
iv. Denial of Service.
v. Privilege escalation.
vi. SQL injection attacks.

14.3.1 Spoofing

14.3.1.1 Email spoofing

Email spoofing (also discussed in next chapter) is the creation of email messages with a forged sender address. It is easy to do because the core protocols do not have any mechanism for authentication. It can be accomplished from within a LAN or from an external environment using Trojan horses. Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message.

When an SMTP email is sent, the initial connection provides two pieces of address information:

a. MAIL FROM: - generally presented to the recipient as the Return-path: header but not normally visible to the end user, and by default no checks are done that the sending system is authorized to send on behalf of that address.
b. RCPT TO: - specifies which email address the email is delivered to, is not normally visible to the end user but may be present in the headers as part of the "Received:" header.

Together these are sometimes referred to as the "envelope" addressing, by analogy with a traditional paper envelope.

Once the receiving mail server signals that it accepted these two items, the sending system sends the "DATA" command, and typically sends several header items, including:

> **From**: Joe Q Doe <joeqdoe@example.com> - the address visible to the recipient; but again, by default no checks are done that the sending system is authorized to send on behalf of that address.
>
> **Reply-to**: Jane Roe <Jane.Roe@example.mil> - similarly not checked

The result is that the email recipient sees the email as having come from the address in the From: header; they may sometimes be able to find the MAIL FROM address; and if they reply to the email it will go to either the address presented in the MAIL FROM: or Reply-to: header - but none of these addresses are typically reliable,so automatedbounce messages may generate backscatter.

Although email spoofing is effective in forging the email address, the IP address of the computer sending the mail can generally be identified from the "Received:" lines in the email header.

14.3.1.2 Website spoofing

Website spoofing is the act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization. Normally, the spoof website will adopt the design of the target website and sometimes has a similar URL. A more sophisticated attack results in an attacker creating a "shadow copy" of the World Wide Web by having all of the victim's traffic go through the attacker's machine, causing the attacker to obtain the victim's sensitive information.

Another technique is to use a 'cloaked' URL. By using domain forwarding, or inserting control characters, the URL can appear to be genuine while concealing the address of the actual website.

The objective may be fraudulent, often associated with phishing or e-mail spoofing, or to criticize or make fun of the person or body whose website the spoofed site purports to represent. Because the purpose is often malicious, "spoof" (an expression whose base meaning is innocent parody) is a poor term for this activity so that more accountable organisations such as

government departments and banks tend to avoid it, preferring more explicit descriptors such as "fraudulent" or "phishing".

As an example of the use of this technique to parody an organisation, in November 2006 two spoof websites, www.msfirefox.com and www.msfirefox.net, were produced claiming that Microsoft had bought Firefox and released Microsoft Firefox 2007.

14.3.2 Repudiation

Repudiation makes data or information to appear to be invalid or misleading (Which can even be worse). For example, someone might access your email server and inflammatory information to others under the guise of one of your top managers. This information might prove embarrassing to your company and possibly do irreparable harm. This type of attack is fairly easy to accomplish because most email systems don't check outbound email for validity. Repudiation attacks like modification attacks usually begin as access attacks.

Non-repudiation refers to a state of affairs where the author of a statement will not be able to successfully challenge the authorship of the statement or validity of an associated contract. The term is often seen in a legal setting wherein the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated".

In a general sense non-repudiation involves associating actions or changes to a unique individual. For a secure area, for example, it may be desirable to implement a key card access system. Non-repudiation would be violated if it were not also a strictly enforced policy to prohibit sharing of the key cards and to immediately report lost or stolen cards. Otherwise determining who performed the action of opening the door cannot be trivially determined. Similarly, for computer accounts, the individual owner of the account must not allow others to use that account, especially, for instance, by giving away their account's password, and a policy should be implemented to enforce this. This prevents the owner of the account from denying actions performed by the account.

14.3.3 Privacy attack

Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Internet privacy is a subset of data privacy. Privacy concerns have been articulated from the beginnings of large-scale computer sharing.

Privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behaviour on a website. PII refers to any information that can be used to identify an individual. For example, age and physical address alone could identify who an individual is without explicitly disclosing their name, as these two factors are unique enough to typically identify a specific person.

Privacy concerns exist wherever personally identifiable information or other sensitive information is collected and stored – in digital form or otherwise. Improper or non-existent

disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as:

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Ethnicity
- Privacy breach
- Location-based service and geo-location

The challenge in data privacy is to share data while protecting personally identifiable information. The fields of data security and information security design and utilize software, hardware and human resources to address this issue. As the laws and regulations related to Data Protection are constantly changing, it is important to keep abreast of any changes in the law and continually reassess your compliance with data privacy and security regulations.

Social networking sites try to get users to use their real names, interests, and locations. They believe this makes the social networking experience more realistic, and therefore more engaging for all their users. On the other hand, uploaded photographs or unguarded statements can be identified to an individual, who may regret this exposure. Employers, schools, parents, and other relatives may be influenced by aspects of social networking profiles that the posting individual did not intend for these audiences. On-line bullies may make use of personal information to harass or stalk users. Modern social networking websites allow fine grained control of the privacy settings for each individual posting, but these can be complex and not easy to find or use, especially for beginners.

Photographs and videos posted onto websites have caused particular problems, as they can add a person's face to an on-line profile. With modern and potential facial recognition technology, it may then be possible to relate that face with other, previously anonymous, images, events and scenarios that have been imaged elsewhere. Because of image caching, mirroring and copying, it is difficult to remove an image from the World Wide Web.

14.3.4 Denial of Service

In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service(DDoS) is where the attack source is more than one–and often thousands–of unique IP addresses. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks, credit card payment gateways; but motives of revenge, blackmail or activism can be behind other attacks .A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge. When a server is overloaded with connections, new connections can no longer be accepted.

14.3.5 Privilege escalation

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Most computer systems are designed for use with multiple users. Privileges mean what a user is permitted to do. Common privileges include viewing and editing files, or modifying system files.

Privilege escalation means a user receives privileges they are not entitled to. These privileges can be used to delete files, view private information, or install unwanted programs such as viruses. It usually occurs when a system has a bug that allows security to be bypassed or, alternatively, has flawed design assumptions about how it will be used. Privilege escalation occurs in two forms:

Vertical privilege escalation, also known as privilege elevation, where a lower privilege user or application accesses functions or content reserved for higher privilege users or applications (e.g. Internet Banking users can access site administrative functions or the password for a smartphone can be bypassed).

Horizontal privilege escalation, where a normal user accesses functions or content reserved for other normal users (e.g. Internet Banking User A accesses the Internet bank account of User B).

14.3.6 SQL Injection Attacks

Looking at its wide-spread use in every form of above discussed web attacks SQL injection attack is kept in an altogether separate category of web attacks. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

VIDEO LECTURE

14.4 SUMMARY

1. There can be very critical information managed through web applications nowadays which needs to handle this information with utmost care and security.
2. Cyber-attacks have become increasingly sophisticated and dangerous. Cyber-attacks have evolved into Cyber Warfare and cyber terrorism.
3. Various forms of cyber-attacks are, Spoofing, Repudiation, Privacy attacks, Denial of Service, Privilege escalation, SQL injection attacks.

14.5 CHECK YOUR PROGRESS

1. Fill in the blanks.

a) _____ is the creation of email messages with a forged sender address.
b) _____and_____ emails are typical means of spoofing.
c) IP address of the computer sending the mail can generally be identified from the _____ in the email header.

2. State True or False

a) Repudiation does not make data or information to appear to be invalid or misleading.
b) User agent is a synonym for a web browser.
c) Open Web Analytics (OWA) is open-source web analytics software created by Peter Adams

14.6 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks.

a) Email spoofing.
b) Spam and phishing.
c) Received sub-head.

2. State True or False

a) False.
b) True.
c) True.

14.7 FURTHER READINGS

1. Computer Forensics: Investigating Network Intrusions and Cyber Crime, EC-Council, Cengage learning 2010.
2. KeyunRuan, Cybercrime and Cloud Forensics: Applications for Investigation Processes, IGI Global, 2013.
3. Gutiérrez, Carlos A., Web Services Security Development and Architecture: Theoretical and Practical issues, IGI Global, 2010.
4. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
5. Amor Lazzez, ThabetSlimani Forensics Investigation of Web Application Security Attacks I. J. Computer Network and Information Security, 2015, 3, 10-17

14.8 MODEL QUESTIONS

1. What do you mean by "shadow copy" of the World Wide Web and 'cloaked' URL? Where does it take place? Describe in detail.
2. Describe the Major tasks an investigator needs to do while performing web application forensics?
3. Describe the major types of web attacks in brief.

.

References, Article Source & Contributors

[1] Cyber-attack - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Cyber-attack

[2] Denial-of-service attack - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Denial-of-service_attack

[3] Email spoofing - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Email_spoofing

[4] Event monitoring - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Event_monitoring

[5] Forensics Web Services - NIST Computer Security, csrc.nist.gov/publications/nistir/.../nistir-7559_forensics-web-services.pdf

[6] Open Web Analytics - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Open_Web_Analytics
[7] Privacy issues of social networking sites - Wikipedia, https://en.wikipedia.org/wiki/Privacy_issues_of_social_networking_sites
[8] Privilege escalation - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Privilege_escalation
[9] SQL injection - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/SQL_injection
[10] Types of Attacks, "Ethical hacking Tips", Go4Expert, www.go4expert.com
[11] Web log analysis software - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Web_log_analysis_software
[12] Web service - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Web_service
[13] Webalizer - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Webalizer

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

This MOOC has been prepared with the support of