SCHOOL OF CONTINUING AND DISTANCE EDUCATION

JAWAHARLAL NEHRU TECHNOLOGICALUNIVERSITY - HYDERABAD

Kukatpally, Hyderabad – 500 085, Telangana, India.

SIX MONTH ONLINE CERTIFICATE COURSES – 2023

CYBER SECURITY - ASSIGNMENT - 04

1) Web Browser Extensions: How risky are extensions & how can you choose safe ones?

Ans:

Popup blocking, form filling, and many other features of modern web browsers were first introduced as thirdparty extensions. New extensions continue to enrich browsers in unanticipated ways. However, powerful extensions require capabilities, such as cross-domain network access and local storage, which, if used improperly, pose a security risk. Several browsers try to limit extension capabilities.

Modern Web browsers make it easy to access websites, search the Web, and do just about everything online. But by default, browsers might not have all the functionality you want. In these cases, many people will customize by installing a browser extension.

At essence, Web browsers process information. Uploads from your computer, downloads from the Web, visiting websites…all this happens in your browser, with information constantly sent back and forth. Browser extensions modify this basic flow of information in some way.

Extensions can do almost anything. They might enable email encryption, ad blocking, one-click password storage, spell-checking, and more. Extensions are like specialized agents working with the flow of information through your browser. They might organize your notes, protect you from hackers, or just transform how that information appears in the browser window.

Security and privacy risks with browser extensions

Many browser extensions are safe, but there’s always some degree of inherent risk. Installing an extension introduces new software to your browser—software which could potentially have security weaknesses

Third-party extensions might secretly include malware, or have security flaws that hackers can exploit. And it’s very common for attackers to “spoof” legitimate browser extensions, creating fraudulent versions to trick and defraud users.

A guide to safely using browser extensions:

- Check the source of an extension before you install.
- Stick with extensions from official sources.
- Don’t overload your browser with extensions.
- Know what extensions you have installed.
- Delete unused extensions.

Browser extensions are often not written by security experts, and many extensions contain security vulnerabilities. Every cross-site scripting vulnerability in a web browser extension is an avenue for malicious web site operators to install malware onto the user’s machine because web browser extensions run with the user’s full privileges.

2) Securing Your Browser: Best methods & their trade-offs for a safer browsing experience.

Ans:

Secure Your Browser:

Today, web browsers such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari are installed on almost all computers. Because web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead quickly to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer.

There is an increasing threat from software attacks that take advantage of vulnerable web browsers. We have observed new software vulnerabilities being exploited and directed at web browsers through use of compromised or malicious websites. This problem is made worse by a number of factors, including the following:

- Many users have a tendency to click on links without considering the risks of their actions. Web page addresses can be disguised or take you to an unexpected site.
- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities are often discovered after the software is configured and packaged by the manufacturer.
- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.
- Third-party software may not have a mechanism for receiving security updates.

Web Browser Features and Risks:

It is important to understand the functionality and features of the web browser you use. Enabling some web browser features may lower security. Vendors often enable features by default to improve the computing experience, but these features may end up increasing the risk to the computer. Attackers focus on exploiting client-side systems (your computer) through various vulnerabilities. They use these vulnerabilities to take control of your computer, steal your information, destroy your files, and use your computer to attack other computers. A low-cost method attackers use is to exploit vulnerabilities in web browsers. An attacker can create a malicious web page that will install Trojan software or spyware that will steal your information.

Keeping Your Computer Secure:

ENABLE AUTOMATIC UPDATES

Research shows that 88% of publicly disclosed vulnerabilities are exploited within a day of release1 . Administrator-driven manual patching often incurs significant lag time before patches are deployed. Adversaries take advantage of this lag time to exploit known vulnerabilities. Automatic updating limits the time available for attackers to exploit publicly disclosed vulnerabilities.

ENABLE REPUTATION SERVICES

Reputation-based blocking services (such as Microsoft SmartScreen®3F5 or Google®6 Safe Browsing) block browsers from accessing sites known to deliver malware. Most browsers offer reputation-based blocking as a core component, but blocking can also be achieved through the use of a trusted browser extension available through each browser’s official extension repository. Reputation services continuously update from a variety of sources enabling adaptive protection against emerging threats. Reputation-based blocking prevents an average of 87.7% of socially engineered malware and phishing attempts.

DISABLE UNSAFE PLUGINS AND EXTENSIONS

Web browser plugins and extensions enrich web browsers by embedding extra features. Based on data calculated from the 2017 CVE database, browser plugins accounted for 34.5% of browser-related vulnerabilities8 . Plugins and extensions expand the browser’s attack surface and provide plugin vendors with access to sensitive browser information. Administrators should carefully consider the risks associated with each plugin and extension installed in their environment.

ADVANCED MITIGATIONS

Well-resourced adversaries have the advantage of time and skill, enabling them to target weaknesses in even properly configured systems. Zero-day vulnerabilities can often defeat most web browser defenses, so administrators must add additional defensive layers in order to slow down exploitation and increase chances of detection. Additional mitigations for web browsers include browser isolation, disabling unnecessary features, and enabling operating system level mitigations.

ENABLE BROWSER ISOLATION

Browser isolation is a strategy that creates a logical barrier between the web browser and the operating system. This barrier decreases the impact of exploits by limiting malicious code to an ephemeral environment. Several browser isolation products exist, and administrators should consider how they can be implemented in their environments.

DISABLE UNNECESSARY FEATURES

Some web browser features are not intended for wide spread use in a production environment, resulting in an unnecessarily large attack surface. Features which provide no benefit to the end user can sometimes be disabled to reduce overall risk. Determining necessary features is dependent upon each specific environment.

3) Two-Step Authentication: Compare methods, strengths, weaknesses & choose the right one.

Ans: **Authentication forms an important step in any security system to allow access to resources that are to be restricted.**

As the number of web applications is increasing day by day, a greater number of private data is being generated, and hence comes the need to access these resources in a protected and secure manner. Authentication and authorization form the basis in most web services in today's era for accessing protected data. Many methods of authentication exist today, each applicable to a certain type of application. There are five main authentication methods:

1. Password-based Authentication.
2. Multi-Factor Authentication
3. Certificate-Based Authentication
4. Biometric Authentication
5. Token-based Authentication.

The simplest form of authentication involves the use of a simple username and a password. With simplicity comes the problem of easily getting your account compromised. Attackers may use different techniques like brute-forcing, keyloggers, etc. to access your private resources. This may be easily protected with the help of the second method that is multi-factor authentication. In this method, the user needs to enter additional information other than the password to access their resource. This is by far the safest and most used authentication method for good security. The third method of authentication is using a certificate file generated by a certifying authority. Any access to the resource needs the user to first share the certificate with the server and get the request authenticated. If the certificate is incorrect or has expired, then the access is rejected. This type of authentication is used everywhere from your browser which uses it for SSL certificate to the server access through the terminal. The main issue with this is the user needs to have the key file always with them to authenticate. Which makes it a little inconvenient. Hence this method is restricted to advanced users and programmers. The fourth method is to use a type of biometric device to scan your fingerprint, iris, etc. To authenticate. This is a very secure method but requires additional hardware cost hence it's not feasible to be used at every website. The last method is by using token-based access. This method is mostly used by mobile applications for accessing the protected resources. But the issue with this method is that it is dependent on the first two methods to get the initial token. Hence indirectly the security of this method depends on the method that is used to get the token.

Advantages of 2FA

It is highly secure as the access to the second factor is usually with the user only.

Disadvantages of 2FA

It adds complexity to the implementation.

It adds an additional step for authentication which some users may not like.

Huge Cost is involved if SMS & email is used for delivery of the access code.

Time is wasted waiting for the access code.

The user will have to carry the registered device to get the token in the case of SMS & Google Authenticator.

4) Strong Passwords: What makes them weak, how attackers exploit them & how to create secure, memorable ones.

Ans; A password is typically a string of characters that a user must provide in order to confirm their identity and gain access to a system or service. Passwords are a common method of authentication, which are used to verify the identity of a user.

Uses of passwords:

Authentication

Access

Security

Possible vulnerabilities:

It can be easily forgotten

Brute force attack or dictionary attacks.

Sharing and misusing

Noting down in books

Phishing scams

Weak and easy guessable.

Best practices:

Use unique, complex and long passwords

Use a password manager

Enable 2FA

Regular update of password

Beware of public wi-fi

Monitoring accounts

creating strong passwords

- **Never use personal information** such as your name, birthday, user name, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.
- **Use a longer password**. Your password should be **at least six characters long**, although for extra security it should be even longer.
- **Don't use the same password for each account**. If someone discovers your password for one account, all of your other accounts will be vulnerable.
- Try to include **numbers, symbols**, and both **uppercase** and **lowercase letters**.
- Avoid using words that can be **found in the dictionary**. For example, **swimming1** would be a weak password.
- **Random passwords are the strongest**. If you're having trouble creating one, you can use a **password generator** instead.

5) POS Security threats: Identify vulnerabilities & suggest solutions for mlaware, breaches & theft.

Ans: The term Point of Sale (POS) is used to describe the technology used by a consumer to provide their payment information in exchange for a good or service. POS technology has actually been around for many years with the first cash register dating back to 1879. However, it wasn't until the mid-70s that this technology was converted from a mechanical to an electrical form. In the 1980s, the technology was advanced again to leverage modern day personal computing (PC) technology. Over the next several years, support for barcode scanning and payment card reading was added. Today, the most familiar example of a POS system would be the check-out counter at a retail or grocery store.

Today’s POS systems consist of many of the same components that are found in traditional information systems. One of the key differences between POS systems and other information systems is its stakeholders. The primary stakeholders for today’s POS systems are as follows: consumers, merchants, acquirer, issuer, card brand companies, payment processors, payment gateways, software vendors, and hardware vendors. A consumer is those people that use payment cards for the purchase of goods (most humans). Merchants are businesses who accept payment cards as a form payment for goods and services.

Data Vulnerabilities

With respect to POS data vulnerabilities, there are three specific areas that should be given attention including data in memory; data in transit; data at rest. Data in memory in this context is when the card track data is brought into the system at the POS system via a POI (or some other input device). Data in memory is nearly impossible to defend if an attacker has access to the POS system. Traditionally, data input into the POS system was in memory in the clear, which is what allowed attackers’ memory scrapers to be very successful. The way to minimize this risk is by encrypting the card data ASAP and keeping it encrypted as much as possible through its life within the system. Point to Point Encryption (P2PE) is a technical feature that can be taken to address the issue of encrypting data in memory, Data in Memory). Data in transit in this context would be the data that’s passed via the network connections between the systems that process the payment card data. By not encrypting the data that is transmitted, it offers an attacker another point where they could capture easily usable payment card data. The technologies that are normally used for addressing the data in transit vulnerability include the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and IPsec. Data at rest in this context would be anytime the card data is stored somewhere within the entire system other than a form of primary storage (i.e. system memory, cache, etc.). The best option for defending against data at rest attacks is to not store the data. P2PE would be the next option with direct symmetric encryption of the data as a last resort.

Attack Methods:

Understanding the areas where card data is vulnerable provides the context to look at some of the attack methods that have been used by bad actors for intercepting payment card data within the POS system. The methods covered include skimming, supply chain integrity, memory scraping (including specific malware), forcing offline authorization, attacking the application, sniffing, 3rd party usage, and crimeware kit usage.

Skimming has been an attack method that has been around for a while. It's a scenario where the POI components of POS system are replaced by a bad actor. When the unsuspecting consumer uses these devices, their data is captured. There are some risks from the bad actor's perspective (i.e. physical presence at the POS location) but with the growth in P2PE, this may become a more viable option. There have been several cases where POS systems have been purchased with vulnerable or misconfigured software. In these cases, the attackers find the software and leverage it for access to the POS system. If you consider a small business or franchise that doesn't have the resources of a large retailer, they may not consider what's "inside" the system, thus the system shows up to their store and they install it without an awareness of the potential information security concerns. Memory scraping has become a popular choice among bad actors. Scrapers are very opportunistic in that they can be can be tailored to target specific patterns of data (i.e. track data) or they can simply grab all data. Further, they don't require information on the environment where they will be emplaced, they're system agnostic. The bottom line is that they are a simple yet extremely effective attack choice. Just like standard viruses, POS malware doesn't have a single, well-defined, taxonomy. However, there are several specific POS malware families to include but not limited to Alina, Dexter, vSkimmer, FYSNA, Decebel, and BlackPOS. It's important to be familiar with the family behaviors to understand how best to defend against them. In general, all of these families inject themselves into memory, collect the desired information (i.e. track data), exfiltrate the data to another system, and use a C&C system. The POS malware families are extremely opportunistic and in many cases aren't detectable with traditional antivirus detection. In most cases, the captured data is exfiltrated from the POS system to another system within the targeted environment for aggregation and uploaded to a remote system, thus reducing the chances of detection. These families continue to evolve as evasion techniques improve with several versions of each family in existence.

POS Breach Phases:

With an understanding of the POS system architectures and various attack methods, the basis has been provided to look at the general POS breach phases. As with most basic pentesting methodologies, POS breach phases don't necessarily have to happen in any particular order but generally there is some consistency in the methodology. The phases include infiltration, propagation, aggregation, and exfiltration. The infiltration phase is where the attacker collects information on the target environment (i.e. reconnaissance) in an effort to find access. Once access is found, it’s exploited and the attacker then creates a more permanent foothold in the environment (i.e. a beachhead) normally using a stealthy trojan. After the infiltration phase, the bad actor moves to spread malware to the target systems (i.e. POS systems). Propagation of malware is often done leveraging existing resources in the target environment.

After the malware is propagated to the targeted systems, it will often send the desired information to a single point (i.e. pivot machine) within the environment for aggregation and exfiltration. However, the data could also be sent directly from the target machine to a single point outside the environment -- exfiltrating the information before aggregating it.