Assignment 1:

Communication Over the Internet and Software Applications’ Vulnerabilities

Corbin Osman

INTL440 – Cyber Warfare

Beth Subero

January 21, 2024

Introduction

We live in a world that has become increasingly reliant on technology and its many rapid advancements. Many individuals utilize the internet and technology to communicate with one another through means such as phone calls, text messages, and email communications. At times the communications we send and our interactions across the internet are targeted by cyber criminals who search for data and information that they can capture and misuse. To help protect themselves from such attacks, users would benefit from learning how communications take place over networks and the internet.

This paper aims to educate readers on the basics of networking and the internet, along with how data and messages are communicated through device and network components. Readers will gain an understanding of components such as addresses, routers, servers, domains, and end-user devices. Common targets of malicious actors will be explored, such as data and personal information, and knowledge about how this information is compromised through network and internet communications will be shared. Additionally, software application vulnerabilities will be discussed such as those found in software applications and web browsers.

Communication on the Internet

Technology allows individuals to connect to local networks and the internet for a variety of purposes. One of these is to communicate with others, and there are many ways this is accomplished. Mobile devices such as cell and smart phones allow users to send text messages and make phone calls to other individuals. Emails can be sent from a variety of devices including mobile devices, laptops, and desktops, and websites such as social media sites allow users to connect with others across the same devices.

To understand how these types of communications are possible, it is important to know what technological components work to connect users and their devices for communication purposes. These same components may be the target of cyber-attacks, so understanding them and their purposes can help users know how to secure them to protect themselves and their personal information and data.

**Device and Network Components**

In order for an individual to connect to a network or the internet to communicate with others, they must have a device. Many of the devices we use such as phones, tablets, laptops, and desktop computers have MAC addresses, which are unique twelve-digit hexadecimal values that are assigned to devices. When these devices are connected to a network, they can be identified through their MAC address.

Devices may also be identified through Internet Protocol, commonly referred to as IP. IP addresses are similar to MAC addresses in that they are unique values which identify a device that is connected to a network or the internet. Two forms of IP addresses are IPv4 addresses and IPv6 addresses. The former are the addresses more commonly used today and are 32-bit numeric values, and the latter are the next generation of addresses which are 128 bits in length and utilize hexadecimal values. These addresses can be static and manually assigned, or they can be dynamic addresses which are assigned by a network when connected. IP addresses on Windows Operating Systems that are dynamically assigned are often done so through Dynamic Host Configuration Protocol (DHCP), which automatically assigns host devices an IP address when connecting to a network.

Other components that aid in connecting users and their devices to networks and the internet are routers, servers, and the Domain Name System. These will be explored shortly to better understand how communications across the internet are performed.

**Connection to the Internet**

Imagine trying to connect to all of your favorite websites using just their 32-bit numeric values? It could get confusing trying to remember all of their individual numbers when trying to connect to them. To help make this process simpler, the Domain Name System (DNS) is used to connect a domain name to an IP address. When a user attempts to connect to a website on the internet they are able to enter the domain name, such as google.com, to connect to the website. The DNS will then attempt to locate the IP address associated with the domain name, and if found they will be able to connect to the site (Lutkevich and Burke 2021).

A router is a device that connects devices to a local network or the internet. This device acts as a gateway that transfers data and information between one or more devices or networks, which is a primary way we communicate with others over the internet. When a user’s device is connected to a router that has internet access, that user is able to communicate with others who are also connected to the internet by sending messages, emails, files, and other forms of communication. This is done through the use of routing tables that direct how and where data is to travel.

Servers are systems that store and provide information, data, and resources to other networks and computers connected to it. The type of information or resources found on a server will greatly depend upon the design and intent of the server. Some servers may store and manage files and allow users to share files and resources across a network, while others may act as hosts for web pages that users can connect to on a network or over the internet (Progressive Digital Media Technology News). Additional types of servers that can be implemented are application servers, mail servers, and database servers which offer users access to specific applications and data they may need.

Each of these components play a part in communication between users over the internet. Routers allow users to connect their devices to the internet to begin communicating with others through their personal devices. They can use built-in device functions such as text messaging and phone applications on mobile devices, or they can access websites to send emails, host video calls, and interact over social media. Users are able to connect to these websites thanks to the functions of Dynamic Host Configuration Protocol and the Domain Name System helping to assign domain names and IP addresses to networks and devices. These components are essential networking building blocks that form the basis of connectivity to the internet.

Targeted Information and Data

Routers and servers are often targeted by malicious actors because of the valuable information they transmit and have stored. Because routing tables help to direct data traffic, attackers may try to manipulate the routing tables to direct the traffic to a location other than its intended destination. They may also attempt to gain access to a router or a server to search for and capture valuable information that is either stored or being transmitted. In order to make their efforts easier, attackers will often search for vulnerabilities in hardware and software that they can take advantage of and exploit.

Malicious actors will often search for personally identifiable information that can be used for their gain. Examples of this personal information include full legal names, date of birth, social security numbers, home address, bank account information, and medical information. When this information is obtained, attackers may attempt to sell it to others or use it themselves for purposes such as opening bank accounts or accessing preexisting bank and credit accounts. Implementing strong best practices while on the internet can help protect users from the attacks of others, but there are times when it may be difficult to avoid such potential attacks.

Software Vulnerabilities

One area in which malicious actors will plan and launch attacks is software applications. There are many types of applications that can be targeted by attackers, such as word processors, image and video editing software, streaming applications, and web browsers. These software applications are often installed on devices such as phones and desktop computers, and while they are often designed with security in mind there are times when vulnerabilities appear in the applications. Because they are unintended, vulnerabilities are often oversights or flaws in the code or functions of software, which in turn make it easier for attackers to take advantage of and exploit the software (Dowd et al. 2006).

One vulnerability software applications face are injection attacks. This vulnerability, often encountered with web browser applications and web pages, involves sending commands or queries to a web application that tricks the software into running unintended commands or operations. These injections may allow attackers to change settings of software applications or retrieve sensitive data and information that they would otherwise not be able to access. Some examples of injection attacks are SQL injection, LDAP injection, and cross-site scripting.

Another threat that software applications face are attacks which exploit flaws in the security design of software applications. Improper design and coding can cause flaws to appear in the security of an application, such as scripting or authentication vulnerabilities (Palmer 2011). Malicious actors may be able to exploit these flaws and bypass security features of software applications, such as the authentication of users through credentials or other forms of identification. This vulnerability could lead to sensitive information and data being accessed by unauthorized individuals and parties.

Because humans are considered the weakest link when it comes to security, most software applications are vulnerable to phishing attempts. These attacks involve social engineering methods to convince someone to do something that they would not otherwise do, such as sharing confidential information or data with another party that is not authorized to have access to it. Due to their manipulative nature, it can be hard to develop software applications that are resistant to phishing and social engineering attacks (Khurana et al. 2016, 3). One of the best methods of combatting this vulnerability is through educating users about the potential phishing attacks they may encounter and how to react when they occur.

There are many more types of vulnerabilities that could be encountered in software applications, and it is important for designers to consider what potential vulnerabilities they might experience. Because users interact with others over the internet and share confidential and personal information, it is important that the software applications they use are developed with protection of user information in mind. There are many different ways for users to communicate online, and understanding how methods of communication work and what potential vulnerabilities may appear will allow users to better protect themselves and their information over the internet.

Bibliography

Dowd, M., McDonald, J., & Schuh, J. (2006). *The Art of Software Security Assessment: Identifying and Preventing software Vulnerabilities*. https://dl.acm.org/citation.cfm?id=1196394

Khurana, P., Sharma, A., & Singh, P. (2016). A Systematic Analysis on Mobile application software vulnerabilities: Issues and challenges. *Indian Journal of Science and Technology*, *9*(32). https://doi.org/10.17485/ijst/2016/v9i32/100190

Lutkevich, Ben, and John Burke. “Domain Name System (DNS).” TechTarget, August 26, 2021. https://www.techtarget.com/searchnetworking/definition/domain-name-system.

Palmer, S. (2011). *Web application vulnerabilities: Detect, Exploit, Prevent*. Elsevier. https://learning-oreilly-com.ezproxy2.apus.edu/library/view/web-application-vulnerabilities/9781597492096/ch05.html#ch05lev1sec8

"What is a Server?" 2016. Progressive Digital Media Technology News, May 24, 2016. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fwire-feeds%2Fwhat-is-server%2Fdocview%2F1790881567%2Fse-2%3Faccountid%3D8289.