THE MWALIMU NYERERE MEMORIAL ACADEMY

DIRECTORATE OF RESEARCH, CONSULTANCY AND PUBLICATION

Proceedings of the Ist Academic Conference in Commemoration of the Late Mwalimu Julius Kambarage Nyerere, the First President of United Republic of Tanzania and Father of the Nation on

The Legacy of Mwalimu Nyerere in Improving Human Welfare and Socio-economic Development

held at MNMA Kivukoni Campus, Dar es Salaam from 11th to 12th October, 2022

Edited by:
Dr. Philip Daninga
Dr. Bertha Losioki
Dr. Luzabeth Kitali
Dr. Adili Zella
Dr. Gideon Bulengela

ISBN 978-9912-41-308-5

9 789912 413085

Investigate Trojans, Wireless Concepts and Their Attacks

Kenneth Longo Mlelwa
Department of Information and Communication Technology,
The Mwalimu Nyerere Memorial Academy

Corresponding author email: kenneth.mlelwa@mnma.ac.tz

Abstract

The World is becoming increasingly more mobile over the past few years. The conventional methods of networking, which rely on physical cables, have proved insufficient to address the challenges posed by our current collective lifestyle. As individuals and businesses require constant connectivity and the ability to move freely, wireless networking has emerged as a crucial solution. Wireless networks use technologies such as 802.11 (Wi-Fi) to provide internet access without the constraints of physical cables. Devices can remain connected to the network while roaming, allowing for greater mobility. Access points are used to enhance Wi-Fi signals, ensuring that devices can connect to the network even when they are far from the router. This has made wireless networks immensely popular in various settings, including public places like restaurants and cafes. However, wireless networks are not without their security challenges. They are vulnerable to both passive and active attacks. A passive attack involves an attacker capturing the wireless signal without sending any signals themselves. These attacks can be easily carried out using wireless antennas and are often undetectable. It is important to assume that attackers can see everything on a wireless network as part of a comprehensive security procedure. To secure a wireless network, administrators need to be aware of the vulnerabilities that exist and the types of attacks that can exploit them. Malicious software, or malware, poses a significant threat to wireless LANs as they have become more common. These programs can disguise themselves as legitimate code or programs and once inside the network, attackers can perform a range of unauthorized actions such as transferring files, modifying data, or deleting files. Another security concern is the presence of backdoors, which refer to methods that allow authorized and unauthorized users to bypass normal security measures and gain high-level access to a computer system, network, or software application. These backdoors can be exploited by attackers to gain unauthorized access to sensitive information or control over the network. A denial-of-service (DoS) attack is a common threat to wireless networks as well. It involves disrupting the efficient use of network resources and essential services, rendering the network unavailable to legitimate users. This can disrupt

operations and cause significant inconvenience or financial loss. Session hijacking attacks occur when an attacker takes over a user's wireless session. This can happen while the user is performing activities such as checking their credit card balance, paying bills, or shopping online. The hijacker typically targets the user's browser or web application programs, allowing them to gain unauthorized access to sensitive information or perform fraudulent actions. Thereof, while wireless networks provide immense convenience and mobility, they also present security risks. It is crucial for network administrators to be aware of these vulnerabilities and implement appropriate security measures to protect against passive and active attacks, malware, backdoors, DoS attacks, and session hijacking. This will help ensure the integrity and privacy of the network and its users.

Key words: *Networking, Network attacks, Network administrations, Internet security*

1. Introduction

Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications take place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality.

Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to assist managers in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking.

Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN troubleshooting. Most network analysis vendors, such as Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.

2. Trojans, Backdoors, Viruses, and Worm Attacks

A Trojan horse. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans also open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

A backdoor is a typically covert method of bypassing normal authentication or encryption in a computer, product, embedded device example a home router, or its embodiment like a part of a cryptosystem, algorithm, chipset, or even a "homunculus computer."

Backdoors are most often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems. From there it may be used to gain access to privileged information like passwords, corrupt or delete data on hard drives, or transfer information within Autoschediastic networks.

A computer virus attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels. Much like human viruses, computer viruses can range in severity: Some viruses cause only mildly annoying effects while others can damage your hardware, software or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. People continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.

A worm is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book.

Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line. Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In more recent worm attacks such as the much-talked-about. Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

3. Denial of Service (Dos) Attacks

Denial of service (DoS) attacks have become a major threat to current computer networks. This paper provides an overview on existing DoS attacks and major defense technologies in the Internet and wireless networks.

Known DoS attacks in the Internet generally conquer the target by exhausting its resources that can be anything related to network computing and service

performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc.

Many attack techniques can be used for DoS purpose as long as they can disable service, or downgrade service performance by exhausting resources for providing services (Handley, et al., 2006)

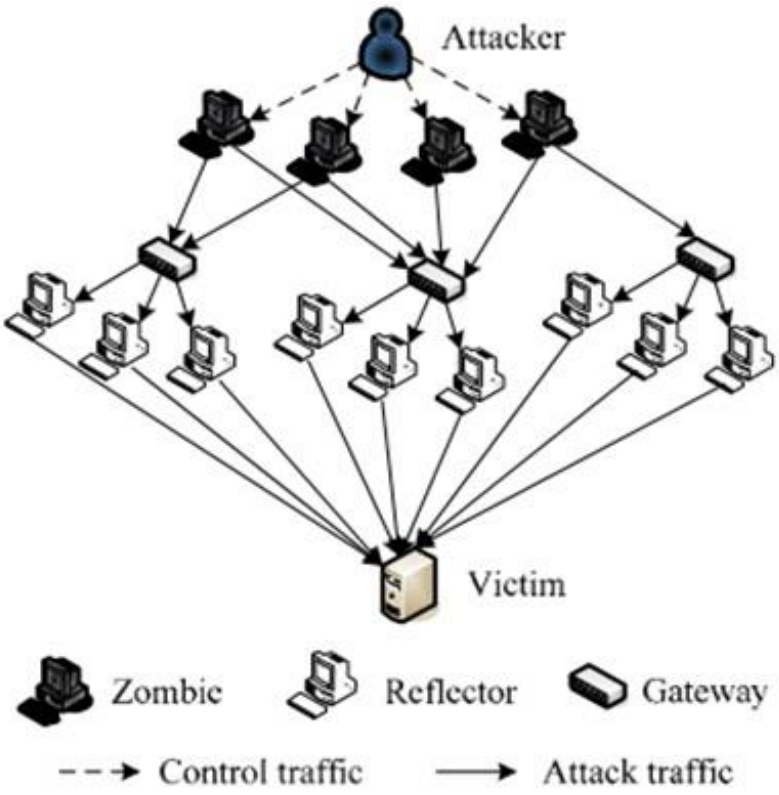

Fig: 1 ICMP Smurf Attack (GU, Q. et la., 2007)

Different from the Internet, wireless networks have their own unique DoS attacks due to the fact that wireless is an open communication approach and mobile devices can function as routers in wireless networks. DoS attacks in wireless networks extend to the scope not viable in the Internet.

4. Session Hijacking

Session hijacking is an exploitation of a valid computer session where an attacker takes over a session through acquiring the session identifier of victim and acting as the authorized user.

Gill, R et al (2005) Explain the most popular types criminals for carrying out a session hijacking are session sniffing, predictable session token ID, man in the browser, cross-site scripting, session side jacking, session fixation.

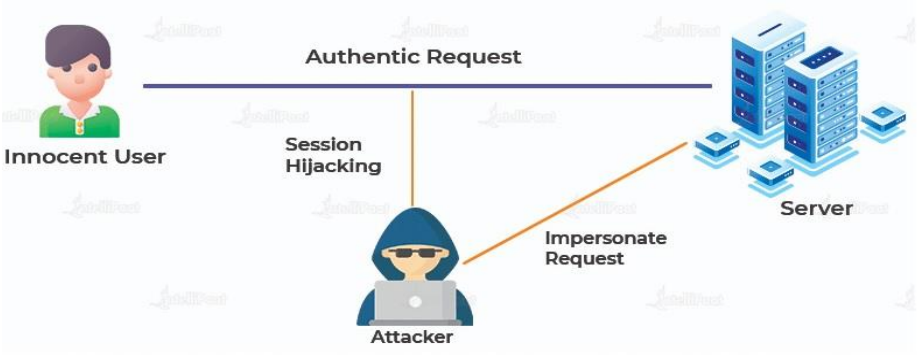

Fig: 2 Session Hijacking

Session sniffing. This is one of the most basic techniques used with application-layer session hijacking. The attacker uses a sniffer, such as Wireshark, or a proxy, such as OWASP Zed, to capture network traffic containing the session ID between a website and a client. Once the attacker captures this value, he can use this valid token to gain unauthorized access.

Predictable sessions token ID. Many web servers use a custom algorithm or predefined pattern to generate session IDs. The greater the predictability of a session token, the weaker it is and the easier it is to predict. If the attacker can capture several IDs and analyze the pattern, he may be able to predict a valid session ID.

Man-in-the-browser attack. This is similar to a man-in-the-middle attack, but the attacker must first infect the victim's computer with a Trojan through some form of trickery or deceit. Once the victim is tricked into installing malware onto the system, the malware waits for the victim to visit a targeted site. The man-in-the-browser malware can invisibly modify transaction information and it can also create additional transactions without the user knowing. Because the requests are initiated from the victim's computer, it is very difficult for the web service to detect that the requests are fake.

Cross-site scripting. Cybercriminals exploit server or application vulnerabilities to inject client-side scripts into web pages. This causes the browser to execute arbitrary code when it loads a compromised page. If Http only isn't set in session cookies, cybercriminals can gain access to the session key through injected scripts, giving them the information, they need for session hijacking.

Session side jacking. Cybercriminals can use packet sniffing to monitor a victim's network traffic and intercept session cookies after the user has authenticated on

the server. If TLS encryption is only used for login pages and not for the entire session, cybercriminals can hijack the session, act as the user within the targeted web application.
Session fixation attacks. This technique steals a valid session ID that has yet to be authenticated. Then, the attacker tries to trick the user into authenticating with this ID. Once authenticated, the attacker now has access to the victim's computer. Session fixation explores a limitation in the way the web application manages a session ID.

5. Wireless Concepts

A wireless network is nothing but a wireless media connecting via Radio waves. A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to business network and its applications. When one connects a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, a wired network connects devices to the Internet or other network using cables.

Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The bases of wireless systems are radio waves, an implementation that takes place at the physical level of network structure.
Main Types of Wireless Network

Wireless Local Area Network (LAN): LAN links two or more devices using a wireless medium, providing a connection through access points to the wider Internet. Wireless personal area networks (WPANs) interconnect devices within a relatively small area, which is generally within a person's reach. For example, both Bluetooth radio and invisible infrared light provides a WPAN for interconnecting a headset to a laptop
Wireless Metropolitan Area Networks (MAN):

It connects several wireless LANs that make a larger wireless network called MAN. WiMAX is a type of Wireless MAN and is described by the IEEE 802.16 standard
Wireless Wide Area Network (WAN):
Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system. The wireless connections between access points are usually point to point

microwave links using parabolic dishes on the 2.4 GHz band, rather than omni-directional antennas used with smaller networks

Wireless Personal Area Network (PAN): PAN interconnects devices in a short span, generally within a person's reach.

6. Wireless Hacking

The security requirements for wireless devices are the same as for wired devices. The minimal requirements for communication security is confidentiality, integrity, and accessibility. Confidentiality is to keep your secrets. Attackers trying to break the privacy are trying to find out something you do not want them to know.

Integrity is about making sure your data is what it is should be. Someone who changes or corrupts data compromises integrity. Availability is a feature that allows people to get the data they need when they need it. Denial of service (DoS) that attempts to bring down a network or server down is an attacks on availability. Wireless local area network (LAN) security has vulnerabilities that make it easy for hackers to create automated tools to exploit those vulnerabilities.

Attacks against wireless networks are organized around three types of wireless networks. The first is the presentation of the types of attacks that can be implemented against 802.11 wireless networks, followed by the types of attacks that can be carried out against personal area networks using the Bluetooth protocol. Also, there is a presentation of the types of attacks that can be carried out against hand-held devices smart phones. However, we cover only two types of attacks in this paper as against wireless and Bluetooth networks.

6.1 Hacking Against Wireless (802.11) Networks

WLAN technology has experienced tremendous growth, there are passive attacks as an easy matter to intercept and monitor network traffic that is using a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b). And, traffic analysis is a technique by which the attacker can determine the load on the wireless network by the number and size of packets being transmitted, to obtain three forms of information as whether there is activity on the network, identification and physical location of Access Points (APs) in the surrounding area from the analysis and lastly is the know the type of protocol being used in the transmissions.

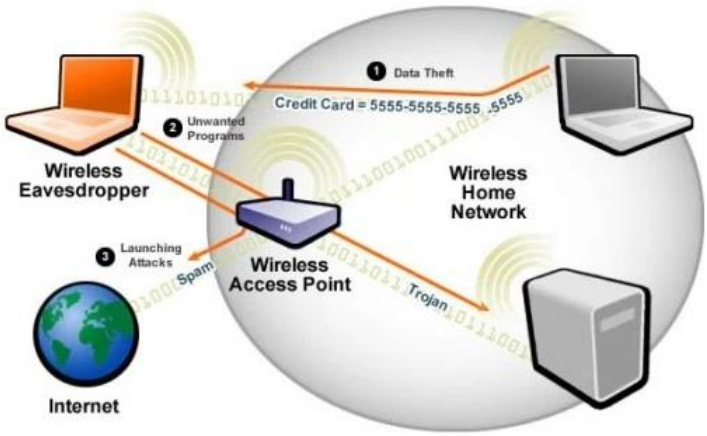

Fig 3: Wireless hacking

Active attacks, attackers can either force stations to connect to an undesired 802.11 network or alter the configuration of a station to force it to operate in an ad hoc networking mode. Ad hoc networks are self-organizing mobile wireless communication networks. The attacker's AP may provide an IP address to the victim's workstation, once the AP and station are associated, the attacker can exploit all vulnerabilities on the victim's station. Other attacks are MAC spoofing and identity theft, Insertion attacks, Brute Force attacks, Man-in-the-Middle attacks, Denial-of-Service attack.

6.2 Hacking Against Bluetooth Networks

Bluetooth is an open standard for short-range digital radio, a wireless protocol used for PANs (personal area networks). Passive attacks, the best scenario is the Eavesdropping, and where by the authorized remote users pose a threat to Bluetooth networks.

These users may employ no secure links. When they transmit their user IDs and passwords, a malicious user can easily capture them using a network sniffer, because this will be a RF transmission, it is an easy matter to intercept the transmission, hence, a device or link can be compromised for a malicious user to monitor data traffic to request and receive data. The active attacks has the same feature as for the against Wireless (802.11) Networks active attacks above.

7.0 Conclusion and Recommendations

7.1 Conclusion

Investigation into trojans, wireless concepts, and their attacks highlights the significant security risks associated with wireless networks. Trojans, as malicious software, pose a serious threat as they can infiltrate a network and perform

unauthorized activities. Passive and active attacks, such as signal interception and disruption, can compromise network integrity and compromise sensitive information. Wireless networks, while offering convenience and mobility, are vulnerable to various forms of attacks. Understanding the vulnerabilities and risks is crucial in developing effective security strategies. Implementing robust security measures, such as strong encryption protocols, secure authentication mechanisms, and regular monitoring, is imperative in safeguarding wireless networks against trojans and other attacks.

Additionally, user awareness and education play a vital role in mitigating risks. Educating users about the importance of secure practices, such as avoiding unsecured networks, regularly updating software, and being vigilant against social engineering attempts, can significantly enhance network security.

7.2 Recommendations

The study recommends the following:

i. Implement strong security measures including encryption protocols, authentication mechanisms, firewalls, and intrusion detection systems, to protect against trojans and other wireless attacks.
ii. Regularly update software and firmware to ensure that security patches and bug fixes are applied promptly.
iii. Conduct regular security audits and monitoring to identify and address any vulnerabilities in the network.
iv. Promote user education and awareness, providing training on safe browsing habits, password hygiene, and recognizing social engineering tactics.
v. Use secure and trusted Wi-Fi networks, avoiding unknown or unsecured networks that may pose security risks.
vi. Consider implementing network segmentation to limit the potential impact of a breach and protect sensitive information.
vii. Employ strong passwords and multi-factor authentication to enhance access control and prevent unauthorized access.
viii. Regularly backup critical data to protect against data loss in the event of a security breach.
ix. Stay informed about the latest security threats, vulnerabilities, and best practices through reliable sources and security forums.

By implementing these recommendations, individuals and organizations can significantly enhance the security of their wireless networks and mitigate the risks associated with trojans and other wireless attacks.

References

Aad, I., Hubaux, J.P., and Knightly, E. (2004). Denial of service resilience in ad hoc networks. Proceedings of ACM Mobicom. ACM Press, New York.

Clark, C. and Cobb, M. (2022). Trojan Horse. Techtarget, USA

Juma, M. (2021). Introduction to Wireless Networking. EngEd, Newyork

Udemy (2022). Hacking Wireless Networks: Theory and Practice. Hacking School, IT Security Academy, Newyork

Crowdstrike (2022). Trojan Malware. Crowdstrike, Newyork

Malwarebytes (2022). Backdoor Computing Attacks. Mawlwarebytes, Washngton Dc

R. S. Singh, A. Prasad, R. M. Moven and H. K. Deva Sarma, "Denial of service attack in wireless data network: A survey," *2017 Devices for Integrated Circuit (DevIC)*, Kalyani, India, 2017, pp. 354-359, doi: 10.1109/DEVIC.2017.8073968.

Johnson, A. (2021). Session Hijacking. Norton.com

Gill, R., Smith, J., Looi, M. and Clark, A., 2005. Passive techniques for detecting session hijacking attacks in IEEE 802.11 wireless networks. In AusCERT Asia Pacific Information Technology Security Conference: Refereed R&D Stream: Proceedings (pp. 26-38). University of Queensland.

Gu, Q. and Liu, P., 2007. Denial of service attacks. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 3, pp.454-468.

Handley, M. and Rescorla, E., 2006. Internet denial-of-service considerations (No. rfc4732).

Malware in IEEE 802.11 Wireless Networks: Department of Computer Science.

Mateti, P., 2006. Hacking techniques in wireless networks hacking techniques in wireless networks. Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management, 3(83)