JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security and Countermeasures against De-authentication Attacks

Nikhil Surve
Nagindas Khandwala College of Science,
University of Mumbai, Mumbai

Prof. Cristin Johnson
Nagindas Khandwala College of Science,
University of Mumbai, Mumbai

Abstract

Deauthentication attack is a type of denial-of-service attacks that targets communication between the user and the wireless access point and are considerable threat to Wi-Fi networks resulting in interference and potential security breaches. This research studies various countermeasures protecting against such attacks along with implementation of Wi-Fi Management Frame Protection (MFP) and the transition to Wi-Fi Protected Access 3(WPA3). After thorough research, experiments and analysis, this study evaluates the significance of countermeasures to prevent Deauthentication attacks. This paper concludes by providing a complete understanding of Deauthentication attacks and ways to secure wireless communications.

Introduction

Deauthentication attacks are a common form of Denial-of-Service (DoS) attack that targets Wi-Fi networks by exploiting the deauthentication frames used under the 802.11 protocol. These attacks enforce users by disconnecting from the network, leading to interruption of services and potential security vulnerabilities. This research aims to study and analyze the classification of deauthentication attacks, estimate existing countermeasures and initiate few enhanced security strategies to mitigate the attacks.

Literature Review

1. On the Effectiveness of 802.11 Management Frame Protection: This paper evaluates the effectiveness of Management Frame Protection to prevent deauthentication attacks and highlights the limitations.
2. Improving Wireless Network Security with 802.11w: Discusses the implementation of 802.11w(MFP) and its contribution in improving wireless network security
3. Wi-Fi Protected Access 3(WPA3): A Comprehensive Security Framework: This paper dives deep into the security features of WPA3 and its robust protection against deauthentication attacks.
4. Evaluating the Impact of Deauthentication Attacks on IoT Devices: This research analyzes the impact of deauthentication attacks on IoT devices and proposes countermeasures.
5. Denial-of-Service Attacks on Wi-Fi network: Detection & Mitigation: Reviews various DoS attacks, including deauthentication attacks, and proposes detection and mitigation techniques.
6. Implementing Robust Wi-Fi Security Solutions in Enterprise Networks: Studies about the challenges and solutions for implementing strong Wi-Fi security in enterprise environments.

7. A survey of Wi-Fi security: Protocols and Attack Mechanisms: Provides an overview of Wi-Fi security protocols and the mechanisms used by attackers to exploit vulnerabilities.
8. Security Enhancements in Wi-fi Networks using Machine Learning: Investigates the use of machine learning techniques to detect and prevent deauthentication attacks.
9. Deauthentication attacks of Public Wi-Fi Networks: Risk and Mitigation: This paper explores the risk associated with deauthentication attacks in public Wi-Fi networks and suggests mitigation strategies.
10. Advanced Security Mechanisms for Next-Gen Wi-Fi Networks: Reviews advanced security mechanisms for future Wi-Fi networks and their effectiveness against deauthentication attacks.

Existing Methodology

The current adapted methodologies to counter deauthentication attacks using the implementation of Wi-Fi Management Frame Protection (MFP) and the transition to Wi-Fi Protected Access 3 (WPA3). MFP adds cryptographic protection to management frames while WPA3 serves enhanced security features, including SAE (Simultaneous Authentication of Equals), which mitigates deauthentication attacks.

Problem Statement

In spite of the availability of MFP and WPA3, Wi-Fi networks remain vulnerable to deauthentication attacks due to incomplete adoption and implementation challenges. There is a need for more robust and comprehensive security measures to protect against these attacks effectively.

Proposed Methodology

This research presents a multi-layered approach that includes:

1. Enhanced MFP Implementation: Strengthening the cryptographic protections in MFP and ensuring widespread adoption.
2. Machine Learning-Based Detection: Utilizing machine learning algorithms to detect and respond to deauthentication attacks in real-time.
3. Transition to WPA3: Encouraging the adoption of WPA3 across all the Wi-Fi networks to leverage its advanced security features.
4. Network Segmentation and Isolation: Implementing network segmentation to limit the impact of deauthentication attacks and isolate affected devices.

Conclusion

The research study concludes that while MFP and WPA3 provides effective countermeasures against deauthentication attacks, their effectiveness can be significantly enhanced through a multi-layered security approach. With the combination of cryptographic protections, machine learning-based detection and network segmentation, Wi-Fi networks can achieve a higher level of security and resilience against deauthentication attacks.

Scope for Future Research

Future research should focus on developing and refining machine learning algorithms for real-time detection of deauthentication attacks, exploring the scalability of advanced security measures in large networks and investigation of these countermeasures into emerging Wi-Fi technologies.

References

1. On the Effectiveness of 802.11 Management Frame Protection
2. Wi-Fi Protected Access 3 (WPA3): A Comprehensive Security Framework
3. Denial of Service Attacks on Wi-Fi Networks: Detection and Mitigation
4. Improving Wireless Network Security with 802.11w
5. A Survey of Wi-Fi Security: Protocols and Attack Mechanisms
6. Implementing Robust Wi-Fi Security Solutions in Enterprise Networks

7. Deauthentication Attacks in Public Wi-Fi Networks: Risks and Mitigation
8. Security Enhancements in Wi-Fi Networks Using Machine Learning
9. Evaluating the Impact of Deauthentication Attacks on IoT Devices
10. Advanced Security Mechanisms for Next-Generation Wi-Fi Networks