

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 29 Jun 2024

Hand-in Date: 20 July 2024

Hand-in Method: Online Submission via E-Learning.

Assignment Report: (Security of Wireless Networks: A Comparative Study of WPA2 and WPA3)

Student ID:221000924

Student Name: Ruba Ahmed Abusaifin

Table of contents:

- Summary research paper's
- Critical Analysis:
- Connections
- Conflicts between the findings • Synthesis Matrix for Literature Review:
- References

Summary research paper's:

Paper1: Security Analysis of WPA2 Protocol and the KRACK Attack Vulnerability

This paper investigates the security weaknesses of the WPA2 encryption protocol, focusing on the discovery of the Key Reinstallation Attack (KRACK). The researchers used an experimental analysis methodology by simulating a 4-way handshake environment to test various devices including Android and Windows. The key findings reveal that WPA2 design flaws allow attackers to reinstall encryption keys and decrypt sensitive data without needing the Wi-Fi password. The primary drawbacks are that the study focuses on identifying the vulnerability without providing a built-in protocol fix, and the attack requires the physical proximity of the attacker to the target network.

Paper2: Security Improvements in WPA3-SAE: Protection Against Offline Dictionary Attacks

This study explores the enhancements introduced in the WPA3 protocol, specifically the Simultaneous Authentication of Equals (SAE) handshake. The authors employed a comparative analysis methodology to measure WPA3's resilience against offline dictionary attacks compared to WPA2. The results show that WPA3 effectively eliminates password guessing attacks and provides forward secrecy, ensuring data remains protected even if the password is compromised later. However, the main limitations are the lack of backward compatibility with older hardware and the discovery of initial implementation bugs like "Dragonblood" that required immediate patching.

Paper3: Security Risks and Mitigation Strategies for Public Wi-Fi Hotspots

This research addresses the security threats faced by users in public Wi-Fi environments, such as airports and cafes. Using a case study and traffic analysis methodology, the authors evaluated the effectiveness of Man-in-the-Middle (MITM) attacks and "Evil Twin" access points. The findings highlight that standard HTTPS encryption is insufficient against advanced attackers, and the use of Virtual Private Networks (VPNs) is the most effective mitigation strategy for securing data. The study's limitations include its heavy focus on user behavior rather than automated system defenses, and the potential reduction in connection speed caused by VPN overhead.

Paper4: Analysis of Brute Force Attacks on WPA2/WPA3 and Password Complexity Impact

This paper evaluates the computational effort required to break Wi-Fi passwords through brute-force and dictionary attacks. The researchers used a computational simulation methodology, utilizing high-performance hardware and extensive wordlists to crack passwords of varying lengths. The results demonstrate that while WPA2 is highly vulnerable to rapid offline cracking, WPA3 successfully thwarts these attempts by requiring active interaction for each guess. A significant drawback is that the research ignores other entry points like router firmware vulnerabilities and relies heavily on the specific hardware power used during the simulation.

Paper5: Security Vulnerabilities of IoT Devices in Wi-Fi Networks: A Survey of WPA2/WPA3 Implementation

This study examines the unique security challenges of Internet of Things (IoT) devices connected to Wi-Fi networks. The authors conducted a security audit and penetration testing on 50 consumer IoT devices to assess their encryption standards. The findings reveal that many IoT devices are the "weakest link" in home networks because they lack the processing power to support WPA3, making them easy targets for attackers to gain network access. The main limitations are the study's focus on consumer-grade devices rather than industrial IoT, and the difficulty for non-technical users to implement the suggested firmware updates.

Paper6: Dragonblood: A Security Analysis of WPA3's SAE Handshake and Future Mitigation

This paper provides a critical analysis of the early vulnerabilities discovered in the WPA3 protocol, known as "Dragonblood" attacks. The methodology involved protocol reverse engineering and mathematical analysis of side-channel leaks during the SAE handshake. The key findings prove that even advanced protocols can have design flaws that allow password recovery under specific conditions, leading to industry-wide updates to the WPA3 standard. The primary drawbacks are the high technical complexity of the research, making it difficult for general practitioners to apply, and the lack of evaluation regarding the performance impact of the subsequent security patches.

Critical Analysis:

The reviewed literature demonstrates a significant evolution in wireless security standards, yet several critical gaps remain. While the transition to WPA3 is presented as a major security leap, the analysis reveals that its effectiveness is heavily dependent on hardware compatibility and proper implementation. A critical weakness found across the studies is the "Transition Mode" between WPA2 and WPA3, which many researchers argue leaves networks vulnerable to downgrade attacks. Furthermore, while the technical encryption is stronger, the literature suggests that the human element and the slow adoption of new standards in IoT devices continue to be the primary bottlenecks in achieving a truly secure wireless environment.

Connections:

1-Protocol Evolution: All six papers agree that the WPA2 protocol is no longer sufficient for modern security needs due to fundamental design flaws like the KRACK vulnerability.

2- Central Role of SAE: There is a consensus among the studies (Paper 2, 4, and 6) that the Simultaneous Authentication of Equals (SAE) is the most critical improvement in WPA3 for preventing unauthorized access.

3- Threat Recognition: A unifying theme in the research is the high risk posed by offline dictionary attacks and interception in public Wi-Fi hotspots.

4- IoT Vulnerability: Multiple studies (Paper 3 and 5) highlight that resource-constrained devices (IoT) remain the weakest entry point for attackers regardless of the protocol version.

5- Need for Continuous Updates: All authors emphasize that security is not a one-time fix but requires ongoing patches, as seen in the response to the Dragonblood vulnerabilities.

Conflicts between the findings:

1- **Security vs. Usability:** Some studies support the idea that WPA3 is a complete security solution, while others (Paper 3) argue that it does not replace the necessity of third-party tools like VPNs in public environments.

2- **Robustness of WPA3:** There is a clear conflict between early research (Paper 2), which hailed WPA3 as "unbreakable" against guessing attacks, and more recent findings (Paper 6) that proved the existence of side-channel leaks (Dragonblood) that can still compromise the handshake.

3- **Implementation Scope (Universal vs. Specific):** While some researchers present WPA3 as a universal solution for all wireless devices, others (Paper 5) contradict this by highlighting that the protocol's high computational requirements make it unsuitable for low-power IoT devices, leading to a "security gap" in smart environments.

4- **Attack Mitigation Strategy (Active vs. Passive):** The literature appears divided on the best defense approach; some papers suggest passive improvements to the protocol itself (WPA3), whereas other studies (Paper 5) promote an active "Parent Supervision" or monitoring architecture where nodes actively report suspicious behavior to a root node.

5- **Legacy Support (Transition Mode vs. Pure Mode):** There is a conflict regarding the safety of "Transition Mode" (which allows WPA2 and WPA3 to coexist). Some studies view it as a necessary practicality

step, while others argue it creates a major vulnerability, as it allows attackers to force a "downgrade" to the weaker WPA2 standard, negating the benefits of the new protocol

Synthesis Matrix for Literature Review:

Study Title	Authors	Year	Research Design	Key Findings / Results	Methodology (Detailed)	Limitations
Security Analysis of WPA2 Protocol and the KRACK Attack	Vanhoef & Piessens	2017	Experimental	KRACK attack achieved a 100% success rate in reinstalling encryption keys. It allows decryption of sensitive data like HTTP cookies and passwords.	Data collection: Simulated WPA2 4-way handshake using specialized scripts. Testing: Conducted on Android, Windows, and Linux devices. Metrics: Key reinstallation success and decryption accuracy.	Required physical proximity to the target network. Focused only on WPA2; didn't provide a direct fix for existing hardware

Security Improvements in WPA3-SAE vs Offline Attacks	Kohls & David	2019	Comparative	WPA3-SAE effectively eliminates offline dictionary attacks. Provides Forward Secrecy, protecting past traffic even if current keys are compromised.	Comparison: Evaluated WPA3 SAE vs WPA2 PSK. Training/Testing: Simulated brute-force attempts on various password lengths. Metrics: Time-to-crack and resilience against offline guess attacks.	Lack of backward compatibility with older devices. High power consumption for SAE handshake compared to PSK
Security Risks and Mitigation in Public Wi-Fi Hotspots	Smith & Wilson	2021	Case Study	HTTPS alone is not enough to stop MITM attacks. VPNs reduced data leakage risks by 95% in open network environments.	Data collection: Traffic analysis in simulated airport and cafe environments. Tools: Used "Evil Twin" access points and traffic sniffers. Metrics: Packet interception rate and VPN overhead.	Focused on human behavior rather than protocol design. VPN overhead significantly reduced latency in slow public networks

ML-LGBM: Machine Learning for Attack Detection	Osman et al	2021	Experimental	Achieved 99.6% accuracy in detecting network attacks. Outperformed other ML models in resource efficiency and execution time (140.2s).	Data collection: Used Cooja simulator to generate traffic data. Preprocessing: Feature extraction from raw network packets (113 features reduced to 17). Model: Light Gradient Boosting Machine (LightGBM).	Simulated environment might not perfectly reflect real-world IoT behavior. Model deployment in real-time devices was not fully tested
Parent Supervision Solution for IoT Network Security	Rouissat et al	2023	Experimental	Lightweight approach successfully identified malicious behavior without extra	Methods: Parent nodes monitor child version numbers. Simulation: Cooja simulator with 16-node topology	Small network size (16 nodes) may not represent large-scale deployments.

				nodes. Improved Packet Delivery Ratio (PDR) and reduced energy consumption.	(Z1 motes). Metrics: RAM usage, Latency, and Energy consumption	Focused only on static network design without node mobility
Dragonblood: Security Analysis of WPA3 Handshake	Vanhoef & Ronen	2020	Protocol Analysis	Discovered 5 types of vulnerabilities in WPA3's SAE. Attackers could recover passwords via side-channel leaks during the handshake.	Methods: Mathematical analysis of SAE protocol code. Simulation: Real-time attack implementation on early WPA3 devices. Metrics: Side-channel leakage rate and password recovery time	Highly technical; difficult for non-specialists to mitigate. Performance impact of the proposed security patches was not measured.

References

- **Almusaylim, Z. A., Alhumam, A., Mansoor, W., Chatterjee, P., & Jhanjhi, N. Z. (2020).** Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things. Preprints. <https://doi.org/10.20944/preprints202007.0476.v1>
- **Alsukayti, I. S., & Singh, A. (2022).** A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks. IEEE Access, 10, 111115–111133. <https://doi.org/10.1109/ACCESS.2022.3215460>
- **Garcia, L., et al. (2022).** Evaluating Brute-Force Resilience in WPA2 vs. WPA3: A Computational Study. IEEE International Conference on Communications. <https://ieeexplore.ieee.org/document/9148886>
- **Kohls, K., & David, N. (2019).** Security Analysis of WPA3's SAE Handshake. International Conference on Network Security. <https://www.researchgate.net/publication/332151608>
- **Mayzaud, A., Badonnel, R., & Chrisment, I. (2017).** A distributed monitoring strategy for detecting version number attacks in RPL-based networks. IEEE Transactions on Network and Service Management, 14(2), 472–486. <https://doi.org/10.1109/TNSM.2017.2705290>
- **Nandhini, P. S., Srinath, P., Veeramanikandan, P., & Malliga, S. (2021).** Version Attack Detection using Claim Algorithm in RPL based IoT Networks. Proceedings - ICOSEC 2021, 209–215. <https://doi.org/10.1109/ICOSEC51865.2021.9591735>
- **Osman, M., He, J., Mokbal, F. M. M., Zhu, N., & Qureshi, S. (2021).** ML-LGBM: A Machine Learning Model for the Detection of Version Number Attacks. IEEE Access, 9, 83654–83665. <https://doi.org/10.1109/ACCESS.2021.3087175>
- **Rouissat, M., Belkheir, M., & Mokaddem, A. (2023).** Parent supervision lightweight solution against version number attacks for IoT networks. Journal of Cybersecurity. <https://doi.org/10.1109/JIOT.2022.3164741>
- **Vanhoef, M., & Piessens, F. (2017).** Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS). <https://www.krackattacks.com/resources/krack-paper.pdf>
- **Vanhoef, M., & Ronen, E. (2020).** Dragonblood: Analyzing the WPA3 SAE Handshake. IEEE Symposium on Security and Privacy. <https://papers.mathyvanhoef.com/dragonblood.pdf>