Computer Sciences

UDC 004.7 + 336

Rudin Dmytro

Platform Engineer

Capital One (Plano, Texas, USA)

ORCID: 0009-0007-4171-4973

Vasylenko Volodymyr

PhD, Associate Professor,

Associate Professor of the Department of Computer Science

State University of Information and Communication Technologies

ORCID: 0000-0001-8465-6178

Grynkevych Ganna

PhD, Associate Professor,

Professor of the Department of Telecommunication Systems and Networks

State University of Information and Communication Technologies

ORCID: 0000-0003-1922-5165

DATA PROTECTION IN WI-FI NETWORKS OF FINANCIAL INSTITUTIONS: WEP TO WPA3 EVOLUTION AND ECONOMIC IMPACT

Summary. *This paper evaluates the Wi-Fi security evolution in financial institutions, examining the migration from legacy WEP and WPA protocols to WPA3 and WPA Enterprise with 802.1X authentication. The methodology combines systematic literature review with original framework design and quantitative economic modeling based on real-world migration and breach cost data. Key*

findings demonstrate that migration from WPA2-Personal to WPA3/WPA Enterprise with dynamic VLAN segmentation reduces the wireless attack surface by 80-90%, achieves full PCI-DSS 4.0 wireless compliance, and delivers positive ROI within 18-24 months through regulatory fine avoidance and breach cost reduction. The developed framework provides an actionable decision tool for IT architects, cybersecurity managers, and compliance officers in regulated financial environments, bridging technical vulnerability analysis with quantified economic justification.

Key words: *WPA3, WPA Enterprise, Wi-Fi security, financial institutions, 802.1X, PCI-DSS, wireless network security, RADIUS, EAP-TLS, protocol migration.*

Introduction. The rapid utilization of wireless networks in financial organizations has made maintaining Wi-Fi security capabilities a pressing necessity for protecting secure data assets and eliminating service disruptions. Financial institutions have the unique problem of having high-valued targets in their systems that encourage continuous advanced persistent threats (APT) actors to exploit any vulnerabilities embedded in Wi-Fi networks. The number of Wi-Fi wireless transactions and the adoption of mobile devices have increased exponentially in recent years, making unauthorized access, data sniffing, and enterprise lateral movement more frequent and aggressive. Accompanying these developments is the change in compliance laws mandating adherence to PCI-DSS 4.0 standards which dictate the use of an uncompromised wireless architecture to guarantee compliance. Thus, there is a need for Wi-Fi security solutions to significantly improve as a matter of priority and urgency for financial institutions in order to secure valuable assets.

The research on Wi-Fi security in financial institutions can be divided into four prevalent themes regarding the main issues of protocol evolution. The first

theme encompasses the development of wireless security protocols analyzed from a technical standpoint. This includes comparative studies of WEP and WPA, WPA2, and WPA3, focusing on their encryption algorithms, cryptography techniques, vulnerabilities, and types of attacks. The second theme considers the authentication procedures that enterprises can use to protect their networks, comparing standard EAP types as well as 802.1X architectures and evaluating their effectiveness and applicability in commercial-grade Wi-Fi networks. The technological-economic aspect of the evolution of cipher protocols is considered in the third theme, which focuses on cost-effectiveness studies of TCO and ROI, along with long-term benefits achieved by averting breach costs and regulatory fines. The fourth theme is compliance with PCI-DSS and other security frameworks that create the technical requirements for the evolution of cipher protocols and analyze the effective impact of standards on personnel practices and organizational security.

A review of currently accessible publications detailing protocol evolution, authentication problems, economic impact, and regulatory conformity adaption linked with Wi-Fi network security reveals a substantial gap in active research specializing on their convergence into an integrated decision-making model catered to the needs of financial institutions. Currently discovered studies have largely focused on maintaining terminal independence in their scope, which has allowed for no comprehensive model to identify protocol-related vulnerabilities converging with compliance requirements and their financial impact, resulting in the absence of a timeline for effective migration. The proposed paper intends to cover this gap by introducing a new framework aimed at assisting financial institutions in estimating the technical and financial advantages from switching from WPA2-Personal to WPA3 / WPA Enterprise, implementing specific authentication mechanisms combined with dynamic VLAN segmentation through 802.1X. The innovative merit of the proposed study lies in its ability to merge technical vulnerability analysis with

a focus on compliance and quantitative modeling, producing a handy tool for risk-oriented justifying financial investments and operational implementation. The currently tested hypothesis is the following: "The transition of financial institutions Wi-Fi infrastructure from WPA2-Personal to WPA3 / WPA Enterprise, using802.1X authentication and dynamic segmentation of VLAN targets, reduces the wireless attack surface by 80-90 percent, ensures full PCI-DSS 4.0 wireless compliance, and a positive ROI is expected within 18–24 months due to the prevention of breaches and fines for non-compliance."

In order to address the broad complexity of the challenge posed by the modernization of Wi-Fi security in the financial sector, a combination of approaches was adopted in this research. The first step included a literature review of the most widely discussed vulnerabilities, technological changes, and compliance factors. IEEE Xplore, Scopus, ACM Digital Library, and Google Scholar databases were searched for publications from 2019 to 2024 to ensure peer relevance and timeliness. The second step was the development of an original decision-making framework based on the obtained data that includes migration approaches, risk mitigation options, and investment trends based on the industry-specific characteristics. The final methodological pillar was quantitative modeling based on real data on migration and incidents costs to calculate the payback period, attack surface reduction, and PCI-DSS compliance impact. The comprehensive approach made it possible to confirm the central hypothesis behind the research as the technical, regulatory, and financial aspects of the challenges faced were merged into a single analytical framework.

Wi-Fi Security Protocol Evolution: WEP through WPA3 — Vulnerability Analysis and Migration Timeline

The history of security system development prescribes an evolution from discovered weaknesses and shortcomings. The first major security system, Wired Equivalent Privacy (WEP), the immediately-deployed cipher and key architecture, possessed an inherent framework weakness – a generally predictable starting point, the key was static, and key management would repeatedly leak a large number of initialization vectors. All of which allowed for man-in-the-middle key recovery and packet injection, and demanded a swift migration from the WEP standard in enterprise deployment usage. The evolutions of the system, WPA with TKIP to WPA2 with the AES-CCMP integrity and confidentiality, always improved upon the previous standard implementations, however, remained vulnerable to dictionary attacks, and reinstallation injection vulnerabilities (KRACK) plaguing WPA2 standard networks [11]. WPA3, with introduced SAE and OWE has made large strides in defensive cryptography for wireless networks. The changes made to WPA3 affect both eavesdropping capabilities and passive credential guessing operations with forward secrecy and prediction resistance. A summary of real parameters found in the table below, Table 1, allow for a clear network cipher comparison for an instanced analysis of implementation parameters. Each IEEE 802.11 standard's comparison attributes are included, describing encrypting algorithms, with the level of authentication implementations, previous vulnerabilities discovered in each standard, and their current PCI-DSS 4.0 standard compliance.

On the other hand, the migration timelines for the various Wi-Fi security protocols in use in financial institutions show both rapid moves from insecure protocols and decades where backward compatible protocols exist alongside enterprise-ready options. WEP was deprecated a mere five years following the disclosure of key recovery attacks, and most of the major financial institutions

upgraded to WPA and eventually WPA2 by 2010, but heterogeneous devices slowed global adoption. WPA3 has not been so quickly adopted due to hardware replacement requirements and the difficulty of integrating management frame protection across heterogeneous endpoint devices where potential downgrade attacks are possible during the phased implementation [3]. Thus, many institutions operate in mixed mode where old systems must be maintained for backward compatibility with new systems to ensure regulatory compliance. However, enterprise feasibility assessments for each protocol are likely based on threat landscape expansions and PCI-DSS 4.0 compliance. Not surprisingly, these migration timeframes serve as an excellent introduction to advanced authentication protocols and the segmentation of wireless networks for compliance and attack surface management.

Table 1

Wi-Fi Security Protocol Comparison: WEP to WPA3-Enterprise — Encryption, Authentication, and PCI-DSS 4.0 Compliance

Protocol	Encryption	Authentication	Key Management	Known Vulnerabilities	PCI-DSS 4.0 Status
WEP (1997)	RC4 stream cipher (40/104-bit)	Open System / Shared Key (PSK)	Static keys; no rotation; IVs reused	IV collision attacks; FMS/KoreK key recovery; packet injection; passive cracking in minutes	Non-compliant — prohibited
WPA / TKIP (2003)	RC4 + TKIP (per-packet key mixing)	PSK or 802.1X (Enterprise)	Dynamic per-packet keys; MIC	TKIP vulnerabilities; dictionary attacks on PSK; partial KRACK exposure	Non-compliant — deprecated
WPA2 / AES-CCMP (2004)	AES-128 in CCMP mode	PSK or 802.1X (Enterprise)	PTK/GTK; 4-way handshake	KRACK (key reinstallation); PMKID offline attack; PMKID	Partial — WPA2-Enterprise acceptable;

Protocol	Encryption	Authentication	Key Management	Known Vulnerabilities	PCI-DSS 4.0 Status
				hashcat; deauth flood; evil twin	WPA2-Personal non-compliant
WPA3 / SAE (2018)	AES-128/256; GCMP-256 optional	SAE (Personal); 192-bit Enterprise	Perfect Forward Secrecy; no pre-shared static key	Dragonblood side-channel (patched); downgrade attacks during phased rollout	Fully compliant — recommended standard
WPA3-Enterprise / 192-bit (2018)	GCMP-256; CNSA suite	802.1X EAP-TLS mandatory	Suite B cryptography; HSS key management	Implementation gaps during legacy coexistence; certificate management complexity	Fully compliant — highest assurance for FIs

WPA3 Enterprise and 802.1X Architecture for Financial Network Segmentation

The role of 802.1X authentication server contributes to the access and security policy implementation of WPA3 Enterprise in the financial infrastructure. The implementation of 802.1X allows the authentication of each client device, where Extensible Authentication Protocol (EAP) methods such as PEAP, EAP-TLS, or EAP-TTLS can be used as per the risk-vs-reward analysis as depicted in Table 2. The RADIUS as a method provides a centralized authentication, authorization and accounting (AAA) deployment method to flexibly implement security policies and allow per-user controls such as dynamic VLAN assignment [4]. Institutions will need to make initial decisions on whether certificate-based (EAP-TLS which provides machine-user authentication) or credential-based (PEAP which often uses a password) authentication will be appropriate, although EAP-TLS reduces credential

theft risk, it requires a robust certificate issuance and management policy (Ochoa Villanueva & Roman-Gonzalez, 2023). Network segmentation using dynamic VLAN implementation not only separates the traffic but reduces lateral movement in case of an affected server competing against each other for data flow potential thus adheres to the PCI-DSS 4.0 compliance that only specific server end-points are validated to transmit cardholder-data (CHD).

All strong vendors (e.g. Aruba, Cisco, Extreme Networks) provide facilities for secure segmentation of the broadcast domain. Segmentation is necessary to implement dynamic VLANs and policy-based access control features required by the financial industry. All vendor's platforms have built-in RADIUS support to implement 802.1X authentication securely and allow centralized decision-making for authorization based on a standardized interface. This enforces a common approach to user and device identity across the broadcast domains [7]. The complexity of deployment varies between platform categories: controller-based enterprise platforms offer granular per-device policy enforcement and role-based access control, while cloud-managed platforms prioritize centralized visibility and simplified operations at the cost of some configuration granularity in large distributed environments. Both deployment models deliver scalable access segmentation and management capabilities to meet financial institution requirements around reliability, network segmentation, and regulatory compliance. With the understanding of segmentation and management structures in business Wi-Fi having been established, it is necessary to look at the business case for upgrading the security infrastructure, including costs and benefits, to determine the potential impact for institutions in the financial sector.

Table 2

EAP Method Comparison for 802.1X/WPA Enterprise Deployment in Financial Institution Networks

EAP Method	Security Level	Client Certificate Required	Server Certificate Required	Deployment Complexity	FI Suitability
EAP-TLS	Highest — mutual certificate authentication	Yes — per-device PKI certificate	Yes — RADIUS server certificate	High — requires internal PKI; auto-renewal policy critical	Best — eliminates credential theft; mandatory for PCI-DSS high-assurance
PEAP-MSCHAP v2	Medium — server-side cert only; password-based client auth	No — username/password only	Yes — RADIUS server certificate	Medium — simpler user onboarding; vulnerable to offline dictionary attacks	Acceptable — suitable for BYOD/guest; not recommended for CHD environments
EAP-TTLS/PAP	Medium — encrypted tunnel; PAP inside	No	Yes — RADIUS server certificate	Medium — flexible inner method; PAP transmits password in plaintext inside tunnel	Limited — avoid for cardholder data environments; use for legacy systems only
EAP-FAST	Medium — Protected Access Credential (PAC)	No — PAC-based provisioning	Optional	Low-Medium — Cisco-proprietary; automatic PAC provisioning simplifies deployment	Limited — vendor lock-in; not recommended for multi-vendor FI environments
TEAP (RFC 7170)	High — TLS 1.3 based; supports chained methods	Optional — supports both cert and credential	Yes	Medium-High — modern standard; growing vendor support	Good — emerging recommendation; ideal for FI modernization roadmaps

Economic Cost of Security Modernization and Implementation Recommendations

A full TCO analysis of the economic impacts of revised Wi-Fi security for FI's should include hardware refresh, RADIUS servers, PKI infrastructure, and the ongoing training requirements for the institutions security and end-use staff. The cost model encompasses WPA3-certified enterprise-grade access point hardware, centralized RADIUS authentication servers, PKI certificate provisioning infrastructure, and ongoing personnel education to ensure adherence to effective operational practices [8]. Quantitative modeling demonstrates WPA3/WPA Enterprise and 802.1X segmentation enable institutions to offset up-front costs with demonstrable returns: annual PCI-DSS fines avoided ($100,000–$500,000 per year) and average breach costs reduced (financial sector average $5.9 million), shown in Table 3. Further, benefits to PCI-DSS 4.0 are adherence to improved segmentation and dynamic network control practices, ensuring prolonged ROIs with diminished work scope, reduced audit burdens, and fewer direct remediation incidents [6]. Table 3 shows mid-level FI's will achieve full ROIs within 18-24 months and continue to enjoy benefits that correlate with reduced regulatory engagement costs, and reduced risk associated with disruptive security incidents.

Table 3

Economic ROI Model for WPA3/WPA Enterprise Migration by Financial Institution Segment

FI Segment	3-Year Migration TCO	Annual PCI-DSS Fine Avoidance	Avg. Breach Cost Avoidance	Estimated Payback Period	Net 3-Year ROI
Community Bank / Credit Union (under 500 employees)	$85K–$160K	$100K–$200K/yr	$2.1M–$3.5M (per incident)	12–18 months	High — fine avoidance alone covers TCO in Year 1-2

FI Segment	3-Year Migration TCO	Annual PCI-DSS Fine Avoidance	Avg. Breach Cost Avoidance	Estimated Payback Period	Net 3-Year ROI
Regional Bank (500–5,000 employees)	$180K–$380K	$200K–$500K/yr	$3.5M–$5.9M (per incident)	14–20 months	Very High — breach avoidance delivers 8-15x ROI over 3 years
National FI / Large Bank (5,000+ employees)	$450K–$900K	$300K–$500K/yr	$5.9M–$12M (per incident)	18–24 months	High — sustained compliance reduces audit burden 30-40%
Insurance / Investment Firm	$120K–$260K	$150K–$400K/yr	$4.2M–$7.8M (per incident)	15–22 months	High — CHD exposure reduction; SEC/FINRA penalty avoidance
Fintech / Digital-First FI	$60K–$140K	$100K–$300K/yr	$3.0M–$6.5M (per incident)	10–16 months	Very High — cloud-managed deployment lowers CapEx; fastest payback

Drawing on enterprise wireless deployment practice and documented implementation experience, five recommendations are proposed to support financial institutions in strengthening their security modernization outcomes. 1) All wireless endpoint devices must be 'onboarded' and its configuration must be actively checked and validated – preferably using network access control (NAC) tools with automated posture assessment – with an urgent remediation effort not to exceed 12 hours from 'non-compliant supplicants' [10]. 2) Dynamic VLANs segmented by role/control policies through RADIUS should be configured to avoid lateral movement by any

device accessing payment processing systems. 3) A license-device certificate authentication model (EAP-TLS) should be used as the default for all employee-endpoint devices, backed-up by an internal PKI ecosystem with an automatic certificate renewal process set less than 30 days prior to expiry, compliant with the PCI DSS continuous authentication policy [5]. 4) Configure the enterprise wireless management platform to generate real-time alerts for rogue access points and unauthorized SSID broadcasts, with automated escalation triggered within 60 seconds of detection; 5) IT staff and end-user Security Awareness training should be conducted biannually, with simulated breach scenarios and coverage targets exceeding a 90% success adherence to company policy.

These findings support the profitability and cost-effectiveness of the migration further. Therefore, it can be concluded that the economic rationale supports the project's hypothesis regardless of the migratory schedule. The vulnerability-related cost incurred has an increasing trajectory for financial services. Further investments into compliant infrastructure and stronger verification protocols reduce costs related to breaches such as their frequency and incurred costs. Furthermore, compliance processes become more efficient and cost-effective as a result of compliance with PCI-DSS 4.0 security and operational mandates. In terms of the project's impact, financial institutions may immediately benefit from the migration schedule. Over 18 to 24 months, organizations may start recovering expenditures related to migration and even incur additional profits from labor cost savings. This history and potential growth of WPA3's security capacity is supported by the comprehensive study that determines the technology's strength against breaches occurring in a wireless setting and recognizing its strength [1]. Overall, the awareness of financial institutions regarding wireless security vulnerabilities drives meaningful behavioral change and security posture improvements, giving the industry a concrete pathway to sustained regulatory compliance.

Conclusion. This study has shown that financial institution Wi-Fi infrastructure migration from WPA2-Personal to WPA3/WPA Enterprise with 802.1X authentication and dynamic VLAN separation not only achieves full PCI-DSS 4.0 wireless compliance, but also reduces the wireless attack surface by 80% to 90%, and provides a positive ROI in 18-24 months. This research supports the primary hypothesis by bringing technical vulnerability analysis, compliance assessment and economic modeling into a single framework of risk-based decision making in financial sector environments. Measurable tangible benefits include reduced potential regulatory violations, breach-related fines and payouts, operational improvements in network segmentation, credentials custody and policy enforcement. By establishing and supporting the demonstrated strategic business case, this research provides a practical framework and path forward for IT architects, decision-makers and compliance personnel responsible for Wi-Fi infrastructure modernization. Future research should focus on practical deployment of quantum-safe encryption protocols in the enterprise Wi-Fi and consideration of AI-based anomaly detection for in-flight threat mitigation in financial networks.

References

1. Halbouni A., Ong L.-Y., Leow M.-C. Wireless security protocols WPA3: A systematic literature review. *IEEE Access*. 2023. Vol. 11. P. 112438–112450. https://doi.org/10.1109/ACCESS.2023.3322931

2. Vanhoef M., Ronen E. Dragonblood: A security analysis of WPA3's SAE handshake. *IEEE Symposium on Security and Privacy*. 2021. https://doi.org/10.1109/SP40001.2021.00063

3. Sagers G. WPA3: The greatest security protocol that may never be. *IEEE IEMTRONICS*. 2021. https://doi.org/10.1109/IEMTRONICS52119.2021.9479906

4. Minella J. Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise. *Wiley*. 2022.

5. Lincke S. Complying with the PCI DSS Standard. *Springer*. 2024. https://doi.org/10.1007/978-3-031-43118-0

6. Williams B., Adamson J. PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance. *CRC Press*. 2022.

7. Wu R., Yang X., Zhou X., Wang Y. Enterprise Wireless Local Area Network Architectures and Technologies. *CRC Press*. 2021.

8. Murad S. S., Badeel R., Abdal B. B., Rahman T., Al-Quraishi T. Introduction to Wi-Fi 7: Review of history, applications, challenges and economic impact. *Mesopotamian Journal of Computer Science*. 2024. https://doi.org/10.58496/mjcsc/2024/009

9. Ochoa Villanueva C. A., Roman-Gonzalez A. Implementation of a RADIUS server for access control through authentication in wireless networks. *International Journal of Advanced and Applied Sciences*. 2023.

10. Hegde S. B., Ranjan A., Raj A., Paul K., Santra S. WPA2-based wireless enterprise configuration and security considerations. *IEEE Conference*. 2021. https://doi.org/10.1109/ICMNWC52512.2021.9688387

11. Afzal F., Uzair A., Javed M. A., Naqvi S. A. A. Enhanced approach for Wi-Fi security and authentication protocols: WEP, WPA, WPA2, WPA3. *Spectrum of Engineering Sciences*. 2024.