Wired And Wireless Communications Are Vulnerable To Security Threats

Posted on September 19, 2019

Introduction

Wired and wireless communications are both vulnerable to security threats, although the nature of exposure differs. Wired networks require physical or logical access to cables, switches, ports, or connected devices, while wireless networks transmit signals through the air and may be observed from outside the organization's premises. Neither medium is automatically secure. Effective protection depends on encryption, authentication, network design, device configuration, monitoring, software maintenance, and user behavior. This issue is especially important in healthcare facilities because compromised communications may expose protected health information, interrupt clinical services, damage connected medical devices, and delay treatment. The most appropriate approach is therefore layered security: modern wireless protocols, secure wired infrastructure, identity-based access controls, segmented networks, updated systems, staff training, and a tested incident-response plan. (Ayala, 2016; National Institute of Standards and Technology, 2024)

How Wired and Wireless Risks Differ

Wired networks are sometimes considered inherently safer because an attacker may need access to a cable, wall port, network closet, endpoint, or internal system. However, physical access is not the only route. Malware, stolen credentials, vulnerable remote services, compromised vendors, misconfigured switches, and malicious insiders can all expose traffic on a wired network. An unused wall port that remains active can provide an unauthorized device with direct access. Poorly protected network closets and unmanaged switches can also create opportunities for interception or disruption.

Wireless networks extend the potential attack surface because radio signals do not stop at walls. An attacker within range may attempt to capture traffic, impersonate an access point, guess credentials, exploit weak encryption, or disrupt availability. Yet a well-designed wireless network using modern encryption and strong authentication can be safer than a poorly managed wired network. Security must therefore be assessed by controls and architecture rather than by assuming that one transmission medium is always secure. (National Institute of Standards and Technology, 2012)

Why WEP Is Insecure

Wired Equivalent Privacy, or WEP, was intended to give early wireless local-area networks privacy comparable to a wired connection. It encrypts frames at the data-link layer, but serious weaknesses in its use of the RC4 stream cipher and short initialization values allow attackers to collect traffic and recover keys. Automated tools can exploit these design flaws quickly, even when passwords appear complex. WEP also lacks the robust integrity and authentication protections expected in modern networks. (Stallings, 2017)

Organizations should not use WEP for any production network. Replacing the password is not enough because the weakness is built into the protocol. Legacy devices that support only WEP should be replaced, isolated from sensitive systems, or removed from service. In healthcare environments, unsupported equipment may require a documented risk assessment and compensating controls while replacement is arranged, but it should not remain connected to the primary clinical network.

WPA and the Transition Away from WEP

Wi-Fi Protected Access was introduced as an interim improvement for hardware originally designed for WEP. WPA used the Temporal Key Integrity Protocol to change encryption keys more dynamically and added message-integrity protections. It also supported stronger authentication through enterprise mechanisms. These changes made WPA substantially safer than WEP at the time, but its dependence on older cryptographic designs means it is now obsolete for modern deployments.

Organizations sometimes retain old WPA settings because a single legacy device cannot support newer protocols. This creates risk for the entire network. A safer strategy is to isolate the device in a tightly restricted segment, limit its permitted communications, monitor it, and establish a replacement date rather than weakening the security configuration for all users.

WPA2, WPA3, and Modern Wireless Protection

WPA2 replaced TKIP with the Advanced Encryption Standard through CCMP and became the dominant wireless security standard. WPA2-Enterprise can authenticate individual users or devices through an 802.1X and EAP infrastructure rather than relying on one shared password. This is important because individual credentials can be revoked without changing the password for every employee, and authentication events can be logged.

WPA3 provides additional improvements, including stronger protection against offline password guessing in personal mode and more robust cryptographic options for enterprise environments. Organizations should prefer WPA3 where devices and infrastructure support it, while using securely configured WPA2-Enterprise during transition. WPA2-Personal with a shared passphrase may be

acceptable for a small, low-risk network, but it is difficult to manage in a large organization because passwords are easily shared and cannot be attributed to a single user. (Wi-Fi Alliance, n.d.)

Secure Wireless Configuration

Modern encryption alone does not eliminate risk. Default administrator passwords should be changed, access-point firmware should be maintained, remote administration should be restricted, and unnecessary features such as Wi-Fi Protected Setup should be disabled. Certificates should be validated in enterprise authentication to reduce the risk of users connecting to a fraudulent access point. Guest networks must be separated from clinical and administrative systems. Wireless coverage should be planned to meet operational needs without unnecessarily extending signals, although reducing signal strength should never replace encryption and authentication. (National Institute of Standards and Technology, 2012)

Common Wireless Attacks

An evil-twin attack uses a fraudulent access point that imitates a trusted network name. Users may connect to it and expose credentials or traffic. Rogue access points may also be installed by employees seeking convenience, bypassing security controls. Deauthentication and jamming attacks target availability by forcing devices offline or interfering with radio communication. Attackers may also exploit weak passwords, outdated access-point software, or improperly configured authentication.

Wireless intrusion-detection or prevention tools can help identify unusual access points, repeated failed authentication, impossible device movement, and interference. However, alerts require trained staff and response procedures. A system that generates warnings without investigation provides little protection.

Threats to Wired Infrastructure

Wired security begins with physical control. Network rooms, patch panels, switches, and servers should be locked and monitored. Unused switch ports should be disabled, and network access control can require devices to authenticate before receiving access. Port security, dynamic address inspection, protections against address-resolution spoofing, and secure switch management can reduce local attacks.

Traffic on internal networks should not be treated as automatically trustworthy. Sensitive applications should use end-to-end encryption such as TLS so that information remains protected even if the local network is compromised. Administrative interfaces should use secure protocols and separate management networks. Logs from switches, routers, firewalls, identity systems, endpoints, and

applications should be centralized to support detection and investigation.

Network Segmentation in Healthcare

Segmentation limits how far an attacker can move after compromising one device. Clinical workstations, medical devices, guest Wi-Fi, administrative systems, building controls, vendor connections, and public-facing services should not share unrestricted access. Firewall rules should permit only communications required for approved workflows. A guest device should not be able to contact an infusion pump, imaging system, or patient-record database. (Ayala, 2016)

Medical devices create special challenges because some run old software, cannot support endpoint security tools, or require vendor approval before updates. Segmentation, device inventory, passive monitoring, strict access rules, and vendor coordination are therefore essential. The organization should know which devices are connected, who owns them, what they communicate with, and when they will reach end of support.

Firewalls and Zero-Trust Principles

Firewalls inspect and control communications according to defined rules. Perimeter firewalls remain useful, but organizations also need internal controls because attackers may enter through phishing, stolen credentials, vulnerable remote access, or third-party systems. Host-based firewalls and segmentation firewalls can restrict lateral movement.

Zero-trust principles strengthen this approach by requiring explicit verification rather than assuming that a user or device is safe because it is inside the network. Access decisions should consider identity, device health, location, sensitivity of the requested resource, and current risk. Users should receive only the privileges necessary for their roles, and privileged accounts should be separated from ordinary work accounts.

Software Updates and Vulnerability Management

Updating software closes known vulnerabilities, but effective vulnerability management is broader than installing patches. Organizations need an inventory of operating systems, applications, firmware, network equipment, cloud services, and connected devices. Vulnerabilities should be prioritized according to exploitability, exposure, business importance, and available controls. Internet-facing and actively exploited weaknesses usually require urgent action. (Cybersecurity and Infrastructure Security Agency, n.d.)

Healthcare facilities must balance patching with patient safety and operational continuity. Updates should be tested where necessary, scheduled carefully, and supported by recovery plans. When an

immediate patch is impossible, temporary controls may include disabling a service, restricting network access, increasing monitoring, or isolating the asset. Delayed patches should remain visible on a risk register rather than being forgotten.

Cybersecurity Training and Human Factors

Employees influence security through password use, phishing decisions, handling of sensitive data, reporting behavior, and response to unusual device activity. Training should be continuous, relevant to each role, and connected to real risks. General awareness may cover phishing, multifactor authentication, secure remote work, safe handling of removable media, and rapid reporting. Clinical staff may need guidance on maintaining patient care when systems are unavailable, while administrators and technical teams require deeper instruction.

Training should not create a culture of blame. Employees are more likely to report mistakes quickly when they believe the organization will focus on containment and learning. Simulated phishing can be useful, but humiliating individuals may discourage reporting. Security teams should make the correct behavior practical by providing easy reporting buttons, clear support channels, password managers, and reliable authentication systems.

Backups, Incident Response, and Resilience

Prevention cannot stop every attack. Healthcare organizations need offline or otherwise protected backups, tested restoration procedures, and plans for maintaining essential services during outages. Ransomware can encrypt systems and disrupt scheduling, diagnostics, medication workflows, communications, and records. Backups are valuable only when they are complete, protected from the attacker, and regularly tested.

An incident-response plan should define authority, technical containment, legal and regulatory notification, clinical continuity, communication, evidence preservation, and recovery. Tabletop exercises help leadership and staff practice decisions before a crisis. Lessons from incidents and exercises should lead to revised controls, not merely a written report. (National Institute of Standards and Technology, 2024)

Conclusion

Wired and wireless communications face different but overlapping security threats. WEP and older WPA configurations are no longer suitable, while WPA2-Enterprise and WPA3 provide stronger wireless protection when combined with secure configuration and certificate-based authentication. Wired networks require physical safeguards, controlled ports, encrypted applications, and internal monitoring. Across both media, the most effective defense is layered: segmentation, least privilege,

firewalls, multifactor authentication, software maintenance, device inventory, trained employees, protected backups, and tested incident response. For healthcare facilities, cybersecurity is part of patient safety and operational resilience, not merely an information-technology concern. (National Institute of Standards and Technology, 2024)

References

Ayala, L. (2016). *Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention*. Apress.

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity performance goals*. https://www.cisa.gov/cpg

National Institute of Standards and Technology. (2024). *Cybersecurity framework 2.0*. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2012). *Guidelines for securing wireless local area networks (SP 800-153)*. https://csrc.nist.gov/publications/detail/sp/800-153/final

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Wi-Fi Alliance. (n.d.). *Wi-Fi security*. https://www.wi-fi.org/discover-wi-fi/security