Brief Report: How the Simulation Aligns with CIA Principles

The secure IoT network simulation in Cisco Packet Tracer effectively demonstrates adherence to the Confidentiality, Integrity, and Availability (CIA) principles. The configurations and security measures implemented ensure the network is robust and capable of safeguarding sensitive user data while maintaining reliable functionality.

Confidentiality

The simulation ensures data confidentiality by implementing WPA2 encryption on the Cisco Wireless Router, securing communication between IoT devices and the network. MAC filtering further enhances confidentiality by restricting network access to pre-approved devices, blocking unauthorized connections. VLAN segmentation on the Cisco Catalyst 2960 Switch isolates IoT devices, the central server, and management traffic into separate logical networks, preventing unauthorized access to sensitive resources. HTTPS communication between the central server and users ensures encrypted management interactions, protecting data integrity and privacy.

Integrity

Data integrity is maintained through the use of Access Control Lists (ACLs) on network devices, restricting communication to authorized devices and blocking unauthorized traffic. Firmware updates for IoT devices are digitally signed, ensuring that only authentic and tamper-free updates are applied. The secure boot process ensures that only verified software is executed on IoT devices, protecting against malicious tampering. During the simulation, traffic monitoring verified that transmitted data remained unaltered, maintaining the integrity of communications within the network.

Availability

The simulation protects system availability through robust firewall configurations, which block unauthorized traffic and protect the network against Distributed Denial of Service (DDoS) attacks. VLANs help to reduce the attack surface by isolating traffic, ensuring disruptions in one segment do not impact the entire network. The network design incorporates redundancy and ensures failover capabilities to maintain consistent functionality. Real-time traffic monitoring and anomaly detection during testing validated the system’s ability to sustain operations even under attempted unauthorized access.

Conclusion

This simulation successfully demonstrates how the secure IoT framework aligns with the principles of confidentiality, integrity, and availability. By employing encryption, access controls, VLAN segmentation, and redundancy, the network ensures that user data is protected, communications remain authentic, and the system is consistently operational. These measures collectively create a secure and reliable IoT environment.