IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 9, March 2025

Impact Factor: 7.67

Leveraging Device Management Protocols for Network Security: A Comprehensive Approach to Handling Device Infections

Arun Sugumar
Anna University, India

Abstract: *The proliferation of Internet of Things devices within critical infrastructure has created significant security challenges for organizations worldwide. This technical article explores how Device Management protocols can be leveraged to establish comprehensive security frameworks addressing the complete threat management lifecycle. By implementing protocols such as TR-069, OMA-DM, and LWM2M, organizations can create standardized approaches to identifying compromised devices, isolating them to prevent lateral movement, recovering affected systems to secure states, and implementing preventive measures to reduce future incidents. The article examines how these protocols enable integrated threat detection through communication pattern analysis, diagnostic data collection, and reputation-based monitoring. It further discusses isolation mechanisms including network segmentation, interface management, and service restriction capabilities that contain infections. Recovery procedures through remote software updates, configuration restoration, and device reset options are detailed, along with preventive measures such as security policy enforcement, continuous monitoring, and threat intelligence integration. This holistic approach to device security management provides organizations with the tools needed to address the expanding attack surface created by interconnected devices while maintaining operational resilience.*

Keywords: Device Management Protocols, Network Security, IoT Security, Threat Isolation, Vulnerability Management

DOI: 10.48175/IJARSCT-24607