Contribution ID: **147** Type: **Poster**

Router Firmware Security: Bridging the Gap Between Network Infrastructure and Digital Forensics

Router firmware has emerged as India's most critical yet overlooked cybersecurity vulnerability, creating a dangerous blind spot that threatens millions of connected devices across homes and businesses. This embedded software, which controls the fundamental operations of networking equipment, remains largely ignored despite being the primary gateway through which all digital traffic flows. The situation is particularly alarming in India due to widespread deployment of legacy hardware, inconsistent firmware update practices, poorly configured default settings, and limited cybersecurity awareness among everyday users. Common vulnerabilities plaguing Indian networks include hardcoded or default passwords, weak encryption protocols, insecure update mechanisms, and the dangerous practice of storing sensitive credentials in plain text. Recent security advisories have exposed these theoretical risks as real-world threats: Digisol's DG-GR6821AC XPON ONU routers, widely deployed by Indian ISPs, contain multiple critical flaws including hardcoded root access credentials and unencrypted password storage. Similarly, TP-Link's popular Archer C50 router uses a static, hardcoded DES encryption key to "protect" configuration files, making it trivial for attackers to decrypt administrative and Wi-Fi credentials offline. CERT-In has responded by assigning CVE identifiers to these vulnerabilities and issuing urgent patching recommendations, though many affected devices have reached end-of-life status, forcing users toward expensive hardware replacement rather than simple software updates. Once cybercriminals exploit these firmware vulnerabilities, they can install persistent malware that survives reboots, factory resets, and power cycles, effectively transforming compromised routers into permanent surveillance outposts for long-term data theft, botnet recruitment, and staging attacks against other network-connected devices. India faces significant structural challenges in addressing this threat landscape, as proprietary firmware complicates security analysis, specialized reverse-engineering tools remain uncommon, and many organizations delay updates due to operational concerns or lack of awareness. The solution requires fundamental changes across multiple levels: users must abandon default credentials, enable automatic updates, and implement network segmentation; manufacturers need secure coding practices including cryptographic firmware signing and transparent vulnerability disclosure; and India's incident response capabilities must evolve to include firmware acquisition and analysis as standard procedures. With India's rapid IoT adoption and smart device proliferation, router firmware vulnerabilities create cascading risks that can compromise entire digital ecosystems, making coordinated improvements across policy, engineering, and operational domains essential for reducing attacker persistence and strengthening public confidence in digital services.

Keywords: Persistent malware routers, firmware anti-forensics, digital forensics India, IoT security India, firmware update best practices, firmware reverse engineering, network security India, secure firmware update, vulnerability management India

Author: NAIDU, KEERTHANA (JAIN (Deemed-to-be) University)

Co-author: Mr NATARAJAN, VISHNU VENKATESH (JAIN (Deemed-to-be) University)

Presenter: NAIDU, KEERTHANA (JAIN (Deemed-to-be) University)

Track Classification: Forensic Sciences