Using Embedded Platforms to Monitor Network Security

Cristian PASCARIU, Ionuţ-Daniel BARBU, Ioan C. BACIVAROV
EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania
proteus_web5@yahoo.com, barbu.ionutdaniel@gmail.com,
bacivaro@euroqual.pub.ro

Abstract

Although in these moments wireless routers are accessible for consumer use in public places as well as in households, from a security perspective, wireless networks pose an increased risk, not only for unauthorized access to the network, but more important for manipulating the information flow of other users on the network. Man-in-the-middle attacks enable attackers to impersonate legitimate services and intercept communications from the users in an attempt to steal sensitive information. In this paper the authors propose a solution based on embedded devices to detect attackers that manipulate the network with the scope of stealing sensitive information. This solution is based on low cost and energy efficient computers that can be connected to regular network equipment to detect and alert on malicious activity.

Index terms: Security, Embedded devices, ARP Spoofing, Man-in-the-middle, Packet Analysis, Intrusion Detection

References:

[1]. https://en.wikipedia.org/wiki/ARP_spoofing
[2]. https://en.wikipedia.org/wiki/Man-in-the-middle_attack
[3]. https://scapy.net/
[4]. https://pentest.blog/what-is-llmnr-wpad-and-how-to-abuse-them-during-pentest/
[5]. https://www.trustedsec.com/2013/07/wpad-man-in-the-middle-clear-text-passwords/
[6]. https://www.bro.org/
[7]. https://suricata-ids.org/
[8]. https://thepacketgeek.com/scapy-sniffing-with-custom-actions-part-1/
[9]. https://fossbytes.com/arp-spoofing-attacks-detection-prevention/
[10]. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html