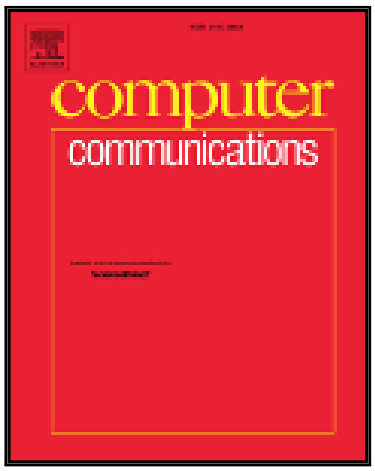

The Nexmon Firmware Analysis and Modification Framework: Empowering Researchers to Enhance Wi-Fi Devices

Matthias Schulz, Daniel Wegemer, Matthias Hollick

PII: S0140-3664(17)31294-X
DOI: 10.1016/j.comcom.2018.05.015
Reference: COMCOM 5708

To appear in: *Computer Communications*

Received date: 18 January 2018
Accepted date: 23 May 2018

Please cite this article as: Matthias Schulz, Daniel Wegemer, Matthias Hollick, The Nexmon Firmware Analysis and Modification Framework: Empowering Researchers to Enhance Wi-Fi Devices, *Computer Communications* (2018), doi: 10.1016/j.comcom.2018.05.015

The Nexmon Firmware Analysis and Modification Framework: Empowering Researchers to Enhance Wi-Fi Devices

Matthias Schulz[a,*], Daniel Wegemer[a], Matthias Hollick[a]

[a]*Secure Mobile Networking (SEEMOO), Technische Universität Darmstadt, Mornewegstr. 32, 64293 Darmstadt, Germany*

Abstract

The most widespread Wi-Fi enabled devices are smartphones. They are mobile, close to people and available in large quantities, which makes them perfect candidates for real-world wireless testbeds. Unfortunately, most smartphones contain closed-source FullMAC Wi-Fi chips that hinder the modification of lower-layer Wi-Fi mechanisms and the implementation of new algorithms. To enable researchers' access to lower-layer frame processing and advanced physical-layer functionalities on Broadcom Wi-Fi chips, we developed the Nexmon firmware patching framework. It allows users to create firmware modifications for embedded ARM processors using C code and to change the behavior of Broadcom's real-time processor using Assembly. Currently, our framework supports nine Broadcom chips available in smartphones and Raspberry Pis. Our example patches enable monitor mode, frame injection, handling of ioctls, ucode compression, flashpatches, software-defined radio capabilities, channel state information extraction and access to debugging features. To enhance firmware analysis, we present a debugger application that directly accesses the debugging core of the ARM microcontroller executing the Wi-Fi firmware. Additionally, we discuss how Wi-Fi chips can be protected from malicious firmware while still allowing researchers to run custom code. Using Nexmon, researchers can unleash the full capabilities of off-the-shelf Wi-Fi devices.

Keywords: Wi-Fi Chips, Reverse Engineering, Firmware, Smartphones, Debugging, Channel State Information Extraction, Software-Defined Radio, Nexmon, Broadcom

*Corresponding author

Email addresses: mschulz@seemoo.tu-darmstadt.de (Matthias Schulz), dwegemer@seemoo.tu-darmstadt.de (Daniel Wegemer), mhollick@seemoo.tu-darmstadt.de (Matthias Hollick)