SAND2021-8325D

The Center for Cyber Defenders
Expanding computer security knowledge

Wi-Fi Attack Detection

Harrison Hill, University of Texas at San Antonio; BS ECE ‘21

James Ryan, University of Texas at San Antonio; BS ECE ‘21

Susan Gardner, Manager 5629

David Carter, Project Mentor 5629

- Problem Statement:
  - Wi-Fi networks use an authentication system such that the act of authentication is vulnerable to offline brute-forcing
  - Wi-Fi networks use unprotected packets to transmit deauthentication instructions, leaving them vulnerable to attackers using common hardware and free software
  - We want to develop a low-cost system to detect attacks in real-time, that can be deployed by anyone.
- Objectives and Approach:
  - We want to understand exactly what the characteristics of an attack are
  - We want to especially pay attention to tools included with Kali Linux
  - We want to develop a Wireless Intrusion Detection System (WIDS) that works on an ESP8266 microcontroller
  - We will base our system on an existing open-source project that detects deauthentication packets, but offers little advanced detection
- Results
  - Deauthentication attacks send floods of deauth packets, sometimes targeted to a specific device, sometimes to all devices on a network.
    - The tools we looked at in Kali Linux worked this way
  - While these attacks are noisy and fairly easy to detect, there are few widely available WIDSs
  - There is a new Wi-Fi authentication system, WPA3, which implements protections against deauthentication attacks
    - This system is still not in wide use, despite being released in 2018
  - Due to scheduling delays, we did not have enough time to develop the WIDS
  - We put together the groundwork that will allow a future team to begin development quickly
- Impact and Benefits:
  - By alerting users that a network is under attack, network intrusion could more easily be stopped

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.