Politechnika Warszawska
Wydział Fizyki
Kryptografia i bezpieczeństwo informacji dla fizyków

Sprawozdanie z zadania nr. 7 na temat:

Pakiety sieciowe Ethernet jako źródło sygnału losowego

Wykonali:
Maciej Czarnecki
Denys Morokov
Fizyka techniczna II stopień, 2 rok

1. Wstęp

1.1. Cel: celem zadania jest napisanie programu śledzącego ruch z wybranego hosta i rejestrujący kolejne wartości losowych bitów z pól nagłówków sieciowych.

1.2. Wykorzystana technologia: skrypt został zaimplementowany w Python.

2. Opracowanie wyników

Do śledzenia ruchu sieciowego wykorzystano bibliotekę Scapy (dla Python). Najpierw w celu wyznaczenia jakie wartości losowe będą rejestrowane przez pisany program, wykorzystano analizator danych sieciowych (Wireshark). W trybie interaktywnym wyznaczono jakie wartości w pakietach mają losowe zachowanie, w których bitach występują owe wartości w offsecie. Zastosowano następne kryteria:

1. Najpierw sprawdzano typ protokołu internetowego (IPv4 lub IPv6).
    a. Dla **IPv4** dla dwóch typów protokołów TCP i UDP wyznaczono następne wartości losowe:
        i. **TCP**: source port (34-35 bajt), header checksum (24-25 bajt), sequence number (38-41 bajt), total length (16-17 bajt).
        ii. **UDP**: source port (34-35 bajt), header checksum (24-25 bajt), total length (16-17 bajt).
    b. Dla **IPv6** wyznaczono następujące wartości losowe: source port, checksum, transaction ID, payload length (w skrypcie z powodu skomplikowanego określenia konkretnego typu protokołu IPv6 wyznaczano tylko payload length).

3. Podsumowanie

Napisano program w Pythonie, który dla wybranego hostu rejestruje kolejne wartości losowe bitów z pół nagłówkowych sieciowych.