Politechnika Warszawska

Wydział Fizyki

Kryptografia i bezpieczeństwo informacji dla fizyków

Sprawozdanie z zadania nr. 1 na temat:

**„Generator liczb losowych Linux jako przykład generatora liczb pseudolosowych, entropia generatora, generator blokujący i nieblokujący”**

Data wykonania zadania w laboratorium: 15.10.2019r.

**Wykonali:**

Maciej Czarnecki

Denys Morokov

Fizyka techniczna II stopień, 2 rok

1. **Wstęp**
   1. **Cel:** celem zadania jest zbadania zmienności dostępnej entropii programowej poprzez napisanie skryptu.
   2. **Wykorzystany język programowania:** Python.
   3. **Specyfikacja komputera:** pomiary wykonano na dwóch komputerach, gdzie na jednym system operacyjny Linux jest zainstalowany natywnie, natomiast na drugim – przez użycie wirtualnej maszyny.
      1. **Natywny Linux:**

- Wersja systemu: Ubuntu 18.04 LTS

- Powłoka: GNOME 3.28.2

- Procesor: Intel Core i5

- Dysk: SSD

- Pamięć: 8 GiB

- Dostęp do internetu: poprzez Wi-Fi

- Brak hwrng

- Do komputera były podłączone klawiatura i mysz

* + 1. **Wirtualna maszyna:**

- Wersja maszyny wirtualnej: VirtualBox 6.0.12

- Wersja systemu: Ubuntu 18.04 LTS

- Powłoka: GNOME 3.28.2

- Procesor: Intel Core i5

- Dysk: SSD

- Pamięć: 3 GiB

- Dostęp do internetu: brak

- Brak hwrng

- Do komputera były podłączone klawiatura i mysz

1. **Opracowanie wyników**

Pomiar odbywał się co 3 sekundy. Dla natywnego Linuxa zebrano mniej punktów pomiarowych, ponieważ została umieszczona zła wartość czasu pomiaru w pliku XML sterującym programem. Wykres 1 przedstawia otrzymane wyniki.

Wyk. 1. Pomiar entropii programowej w ciągu do 12h

1. **Podsumowanie**

Korzystanie z komputera powoduje przyrost entropii. Dla obu systemu zaobserwowano spadek entropii spowodowany odczytem pliku entropy\_avail, gdyż istnieje mechanizm pompowania entropii z input\_pool do puli wyjściowej, która obsługuje random i urandom (entropy\_avail ocenia entropię input\_pool).