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

Mikołaj Koszowski 274392
Hubert Nowakowski 274415

Zadanie na poziom 4

W celu oceny maksymalnej wydajności odtwarzania systemowego źródła entropii, odczytywane były przyrosty dostępnej liczby bitów entropii na przedziale 2 sekund. Liczbę bitów entropii w systemie odczytywano przy pomocy skryptu bash czytającego wartości z */proc/sys/kernel/random/entropy_avail*
Więcej informacji: https://github.com/Fisher16/KiBD

Pomiary wykonano dla różnych początkowych poziomów dostępnej entropii, dla dwóch różnych maszyn:

- maszyna 1: ubuntu 18.04(4.15.0-70), rzeczywista instalacja
- maszyna 2: ubuntu 18.04(5.3.0-40), maszyna wirtualna (VirtualBox)

Dla obu systemów zauważyliśmy spadkowe tempo wzrostu entropii w zależności od jej aktualnej wartości. W przypadku maszyny 1 po przekroczeniu wartości 3400 entropia przestaje rosnąć. Dla maszyny 2 obserwujemy oscylacje powyżej wartości 3100. Poniższe wyniki były dokonane przy wyłączonym ruchu sieciowym i z wyłączonymi aplikacjami działającymi w tle, są one również uśrednione po 10 próbach. W celu uzyskania precyzyjniejszych wartości należałoby stworzyć bardziej izolowane środowisko, ponieważ sam pomiar wypływa tutaj na wartość mierzoną.

Wyniki pomiarów przedstawione są w tabelach 1 i 2. Dla maszyny 2 obserwujemy wolniejszy przyrost entropii co może być spowodowane tym, że maszyna wirtualna ma mniejszy dostęp do urządzeń systemowych, z których może generować entropię.

Tabela 1: Zmierzony średni przyrost entropii dla maszyny 1.

Początkowa entropia [bit]	Końcowa entropia [bit]	Średni przyrost entropii na sekundę [bit/s]
183	813	15,7
603	887	14,2
2080	2345	6,6
2834	2967	3,3
3435	3435	0,0

Tabela 2: Zmierzony średni przyrost entropii dla maszyny 2.

Początkowa entropia [bit]	Końcowa entropia [bit]	Średni przyrost entropii na sekundę [bit/s]
118	144	0,65
485	510	0,63
1603	1619	0,40
2515	2525	0,25
3021	3032	0,28

Źródła:
https://linux.die.net/man/4/random
https://security.stackexchange.com/questions/126875/whats-eating-my-entropy-or-what-does-entropy-avail-really-show