Crypto Libraries Entropy

Arthur T. N. Yoshikawa

October 18, 2019

1 CryptoPP

A biblioteca criptográfica CryptoPP possui um arcabouço de geradores pseudoaleatórios (PRNG), um dos método citados na documentação original: **AutoSeededRandomPool. AutoSeeded*.** É dito a origem de entropia do gerador baseado nas piscinas de entropia do sistema operacional (OS's Entropy Pool). A entropia é coletada baseado no sistema operacional Windows ou Linux.

- Em Linux utiliza **OS_GenerateRandomBlock** usando a entropia baseada no /dev/random ou /dev/urandom.
- Em Windows utiliza o **CryptGenRandom** baseado no /dev/srandom ou /dev/urandom.

2 OpenSSL

De acordo com United States Patent Application Publication (2018), é ilustrado três fatos de funcionamento da biblioteca.

- Utilizando o Modo FIPS, o OpenSSL não possui uma fonte própria de entropia, dependendo da aplicação hospedeira à obter entropia e sem tratamento de qualidade dessa fonte.
- Sem o modo FIPS, o OpenSSL lê um intervalo de 32 a 256 Bytes de entropia fornecido pelo /dev/urandom como seed para o PRNG da biblioteca.

- O OpenSSL v.1.1 tentaram gerar fontes próprias de entropia com base em ad.hoc, mas não houveram empenhos para melhorar as qualidades e quantidades geradas. Essa fonte de entropia própria não possui manutenção desde a versão 1.0.

3 Referências

1. https://patents.google.com/patent/US20190050202A1/en
2. https://wiki.archlinux.org/index.php/Random_number_generation
3. https://www.cryptopp.com/wiki/RandomNumberGenerator