Internet As a Source of Randomness

Markus Brandt Haya Shulman Michael Waidner
Fraunhofer SIT / Technische Universität Darmstadt

March 14, 2019

Significant efforts in the theoretical and practical research communities are invested to improve the security of PRGs, to identify faults in entropy sources, and to detect vulnerabilities allowing attacks against the PRGs.

Despite the critical role that secure generation of unpredictable pseudorandom bits plays, there is a long history of attacks exploiting bugs and vulnerabilities in PRGs, e.g., [BM84, CG88, DGP07, Gut98, GPR06, GW96, SW17]. The causes for vulnerabilities in generation of pseudorandom strings range from faulty implementations, to generation of pseudorandomness on virtualised environments, and to reuse of randomness.

In this work we take an alternative approach at the pseudorandomness generation problem. We design and implement Network Pseudorandomness Collector (NPC) which collects pseudorandom strings from servers in the Internet. NPC does not require cooperation nor synchronisation of those servers. NPC is easy to use and to integrate into the existing systems. We analyse the security of NPC and show how it addresses the main factors behind the vulnerabilities in current PRGs. Further, we perform extensive simulations on empirically derived datasets that validate the security of NPC against attacks by realistic Man-in-the-Middle (MitM) attackers.

References

[BM84] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM journal on Computing*, 13(4):850–864, 1984.

[CG88] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[DGP07] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the windows random number generator. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 476–485. ACM, 2007.

[GPR06] Zvi Gutterman, Benny Pinkas, and Tzachy Reinman. Analysis of the linux random number generator. In *Security and Privacy, 2006 IEEE Symposium on*, pages 15–pp. IEEE, 2006.

crypto day matters 30 (2019)
Beiträge vom 30. Kryptotag, 28.-29.03.2019, Mozilla, Berlin.
doi:10.18420/cdm-2019-30-24

[Gut98] P Gutmann. Software generation of random numbers for cryptographic purposes. In *Proceedings of the 1998 Usenix Security Symposium*, pages 243–257, 1998.

[GW96] Ian Goldberg and David Wagner. Randomness and the netscape browser. *Dr Dobb's Journal-Software Tools for the Professional Programmer*, 21(1):66–71, 1996.

[SW17] Haya Shulman and Michael Waidner. One Key to Sign Them All Considered Vulnerable: Evaluation of DNSSEC in Signed Domains. In *The 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*. USENIX, 2017.