DRAFT -- Please do not redistribute.

How to Keep Evil Children out of Your Pool and Other Random Facts

Henry Corrigan-Gibbs and Suman Jana
Stanford University

Abstract

A number of common misconceptions about randomness underlie the design and implementation of randomness sources in popular operating systems. We debunk these fallacies with a survey of the "realities of randomness" and, in doing so, we derive a number of new architectural principles for OS randomness subsystems.

1 Introduction

Randomness is at the heart of the security of a modern operating system (OS): cryptographic keys, TLS nonces, ASLR offsets, password salts, TCP sequence numbers, and DNS source port numbers all rely on a source of hard-to-predict random bits. Unfortunately, misuse or abuse of random numbers and random number generators has led to a jaw-dropping number of bugs and security holes of late [9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 44, 55].

We argue that the blame for many of these failures does not lie with the application developers. Instead, we posit that the design of and interface to the randomness subsystems in many OSes are the source of many application-level randomness failures. Misconceptions about the nature of cryptographic randomness underlie the design of the random number generators used in Linux and other popular OSes. The documentation of randomness interfaces is often misleading or incorrect and serves to spread myths about randomness, rather than dispel them. In addition, APIs for OS randomness are dangerous by default, and they make it difficult, if not impossible, for applications to safely use randomness under adversarial conditions. Given the state of randomness subsystems in popular OSes, it is no surprise that developers often misunderstand and misuse randomness.

This paper has two parts. First, we identify and debunk a number of common misconceptions about randomness in OSes. Along the way, we point out a number of weaknesses in and attacks against randomness subsystems of existing OSes. Second, we outline a new design for the OS randomness subsystem that solves many of the issues raised in the first portion of the paper. In sum, we attempt to "set the record straight" on randomness for designers of future OSes with the hope that new systems will take a more principled view towards this important but counter-intuitive piece of the OS.

2 Preliminaries

We first define a few key terms and concepts.

Entropy. For our purposes, entropy is a measure of an adversary's uncertainty about the state of a particular value. To make this notion precise, let S be a discrete random variable representing, for example, the state of a cryptographic random number generator. Let $G(S \mid \mathcal{A}\text{'s knowledge})$ be a random variable representing the number of guesses required to recover the value of S given an adversary $\mathcal{A}$'s knowledge of the distribution of S, following an optimal strategy [48]. We say that the distribution of the state S has k bits of *guessing entropy* ("entropy") with respect to an adversary $\mathcal{A}$ if the expected number of guesses $E[\,G(S \mid \mathcal{A}\text{'s knowledge})\,]$ is greater than or equal to 2^k [7, Section 3.2.4]. A value S sampled uniformly at random from a set of 2^k values has just over $k-1$ bits of guessing entropy, since $E[G(S)]$ is equal to $(2^k+1)/2$.[1] When we say that a particular value "has k bits of entropy," we mean that the value is sampled from a distribution with k bits of entropy from the perspective of some adversary.

Pseudo-random Bit Generator. A *pseudo-random bit generator* (PRG) is a family of deterministic algorithms mapping short bitstrings ("seeds") to long bitstrings ("outputs") [6, 49]. To be useful in a cryptographic setting, the output of a PRG must be indistinguishable from random, as long as the seed is sampled from a distribution over the seed space with "enough" entropy.[2]

One suitable PRG is the AES block cipher instantiated in counter mode [3]. The seed for the PRG is the AES key k and the output of the PRG is the concatenation of the AES encryptions of the bitstrings representing "0," "1," "2," and so on. As long as the seed for this PRG is sampled from a distribution with many bits of entropy (e.g.,

[1] The guessing entropy of this distribution is *not* equal to its Shannon entropy or min entropy [7, Section 3.4].

[2] To be precise, the seed must be sampled from a distribution with k bits of entropy such that k has size polynomial in the security parameter.

128 bits) it appears infeasible to distinguish the output of this PRG from random.

OS Randomness Subsystem. All modern operating systems implement some sort of *randomness pool*. The pool contains a bitstring derived from other values in the system that are ostensibly difficult for user-level processes to guess. These values typically include the CPU's cycle counter, disk seek times, outputs from a hardware randomness source (e.g., Intel's `RdRand` instruction), network packet arrival times, and other fast-changing values known to the operating system. The operating system periodically updates this pool with fresh values as they become available.

In Unix-like operating systems, user processes interact with the randomness subsystem through a special file named `/dev/random`.[3] The `CryptGenRandom` function serves a similar purpose in recent versions of Windows. When we say that a process reads random bytes from the OS, we mean that it requests bytes from `/dev/random` or `CryptGenRandom`.

User-space processes read random bytes from the OS to obtain random values for cryptographic purposes (e.g., secret keys or session nonces). Kernel threads may also read random bytes from the OS when they need unpredictable values (e.g., for DNS source port numbers). All common flavors of Unix also allow user-space processes to *write* random bytes to the OS (by writing to `/dev/random`), which has the effect of mixing user-provided bits into the randomness pool.

3 Realities of Randomness

In this section, we review a number of realities of randomness, which inform the randomness architecture we introduce in Section 4.

3.1 Your Randomness Won't Run Out

There is a common misconception that randomness in the entropy pool can somehow be "used up"—that the OS must constantly add new hard-to-predict bits to the pool to ensure that its outputs remain unpredictable. For example, a post on the CloudFlare Security Blog about the Linux randomness pool states:

> When random numbers are generated from the pool the entropy of the pool is diminished (because the person receiving the random number has some information about the pool itself). [53]

[3] In Linux and Solaris, `/dev/random` can block so there is a second non-blocking file called `/dev/urandom` for accessing the randomness pool.

This statement is *false* as long as widespread cryptographic assumptions hold.

In particular, once there is enough randomness in the pool to derive a seed for a pseudo-random generator, then the OS can produce an endless string of random-looking bits.[4] The procedure for deriving an endless stream of bits from a random-enough randomness pool is straightforward: extract the entropy from the pool by using SHA-256 to hash the pool's contents into the space of PRG seeds (e.g., AES keys). Then, use the PRG (e.g., AES in counter mode) to expand the short seed into a long bitstring. Application of the random-oracle model [4] allows a rigorous analysis of the security of this extract-then-expand technique [45]. This procedure leads to the following finding:

Reality 1. *Once the randomness pool has accumulated enough entropy to seed a PRG, the pool can never "run out" of random bits (if the pool implementation is sane).*

As we note, Reality 1 is only true as long as the randomness pool uses a "sane" implementation. The extract-than-expand technique outlined above is an example of a "sane" implementation [45]. An example of an "insane" implementation is any one that returns bits of the randomness pool state to a user-space processes without running it through a hash function and cryptographic PRG. Implementations like these may reveal the entire state of the randomness pool to an adversarial user-space process, and can thus "run out" of entropy.

Corollary. *The only time that the randomness pool is vulnerable to compromise is in the period* before *it has accumulated enough entropy to seed a PRG.*

Before the randomness pool has enough entropy to seed a PRG, an adversary who can read random bytes from OS can learn the internal state of the OS's randomness pool. To mount this attack, the adversary first reads a random bitstring b from the OS, and guesses the state of the randomness pool that would have produced the string b. The number of guesses required is bounded by 2^k, where k is the number of bits of entropy in the randomness pool.

Figure 1 graphically depicts a hypothetical example of this process: the pool starts out with zero bits of entropy (e.g., after the machine's first boot) and in every time unit, the OS harvests 32 bits of entropy from hardware sources. If a malicious process can read several bytes from `/dev/random` at every time unit and brute-force through the 2^{32} choices, the malicious process can always recover the state of the randomness pool and the system will *never* accumulate enough entropy to seed a PRG.

[4] Well, "endless" at least from the perspective of all polynomial-time adversaries.

DRAFT -- Please do not redistribute.

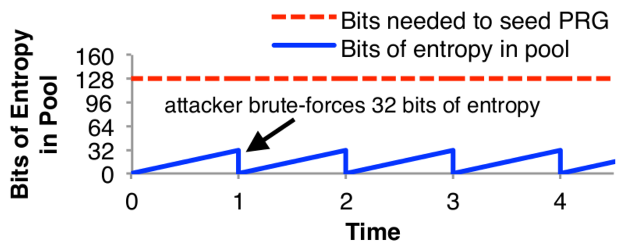


Figure 1: Under unfavorable conditions, the system will never accumulate enough entropy to generate strong cryptographic keys (using the 128-bit security level).

3.2 Entropy Estimation is Hopeless

A tempting way to address the problem depicted in Figure 1 is to just disallow reads from the OS randomness source until the pool accumulates enough entropy to seed a PRG (e.g., 128 bits). Indeed, several operating systems—including Linux, NetBSD, and Solaris—try to *estimate* how many bits of entropy are in the randomness pool and will block `/dev/random` until there is enough entropy to prevent the attack of Figure 1. Unfortunately, this strategy is misguided.

Reality 2. *Building an accurate entropy estimator is infeasible.*

To see why entropy estimation is infeasible, recall the definition of entropy: it is a measure of the *adversary*'s uncertainty about the value of a certain variable. The OS generally has no way of knowing what the adversary knows about the system and thus has no hope of estimating how many bits of entropy are in the randomness pool [1]. Since the OS cannot *ever* accurately estimate how many bits are in the pool, and since the OS should only block reads to the randomness source when there are "too few" bits of entropy in the randomness pool, we conclude:

Corollary. *Reads to the OS randomness source should never block.*

Although Linux, NetBSD, and Solaris still offer a blocking `/dev/random`, FreeBSD, MacOS, and recent versions of Windows (correctly) only support a non-blocking interface to the randomness pool.

3.3 All Bits Should Be Treated Equally

The widespread use of entropy estimation techniques has given rise to the misconception that the OS should differentiate between "trusted" and "untrusted" inputs to the randomness pool. In Linux, for example, only kernel threads or users with the `CAP_SYS_ADMIN` capability can write to the randomness pools in a way that increases the entropy estimate.

The intuition behind this design decision is clear: internal entropy sources, like the cycle counter and disk seek times, are considered "more random" than user-provided bitstrings, which might be adversarially crafted. However, there is no need to make such a distinction, since adding data to the randomness pool should *never* decrease the amount of entropy in the pool:

Reality 3. *Adding bits to the randomness pool will* never *decrease the amount of entropy in the pool, as long as the implementation is sane.*

For an example of a "sane" implementation: let the state of the randomness pool be an ℓ-bit string and let $E_k(m)$ be an ideal cipher that encrypts a message m with a key k, such that m and k are both ℓ-bit strings [5, 52]. We can calculate the new state s_{i+1} of the pool by hashing the input string into a cipher key k and computing $s_{i+1} \leftarrow E_k(s_i)$ [45]. Since E defines a family of permutations (indexed by k), the adversary's uncertainty about the value of s_{i+1} is at least as large as the adversary's uncertainty about the value of s_i, no matter whether the input string is adversarially chosen. In practice, the OS could implement E with the AES cipher.

Corollary. *The OS should allow any user and any process to contribute to the randomness pool.*

Since adding bits to the randomness pool can only increase the adversary's uncertainty about the pool contents, it can never hurt to allow writes into the pool.

3.4 User-Space is a Danger Zone

Cryptographic folklore, as well as the OpenBSD and Linux randomness manpages, suggest that it is good practice to maintain a user-space randomness pool when an application needs many random bytes. This thinking suggests that processes requiring random bits should read only small number of bytes from `/dev/random` and use these bytes as the seed for the process' own PRG. Many popular cryptography libraries (including OpenSSL) follow this advice and implement their own user-space randomness pools and PRGs.

Reality 4. *User-space randomness pools are often unsafe.*

Maintaining a randomness pool in user-space entails a number of risks:

Fork (un)safety. The implementation must be sure to reseed the child of a `fork()` call with fresh randomness to make sure that the child's pool differs from its parent's. Neglecting to reseed after forking is easy to do and can lead to dangerous security vulnerabilities [26, 30, 31].

Pool leakage. Maintaining the privacy of the state of randomness pool is often much harder in user-space than kernel-space. Chow et al. [8] showed that secret content of user-space applications may leak through swap and other unexpected sources.

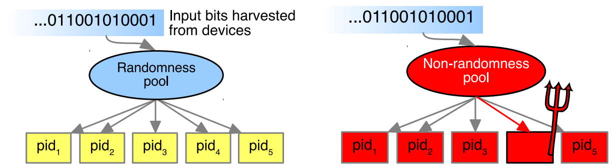
Reseeding required. If the user-space randomness pool seeds itself from `/dev/random` soon after boot, the OS's pool may not yet have enough entropy to provide a strong seed. Even if the amount of entropy in the kernel pool eventually increases, the amount of entropy in the user-space pool will not increase unless the user-space implementation periodically reseeds itself from `/dev/random`. OpenSSL does not reseed itself automatically from the OS and some applications wrapping OpenSSL (e.g., PHP) do not provide a way to request a reseeding.

There are legitimate reasons for maintaining a user-space randomness pool: it avoids the system-call overhead of reading a special file and it allows an application to use a different PRG than the one the kernel supports. Even so, the risks of maintaining a user-space pool are much greater than the benefits in many cases and the OS design should not encourage the application developers to implement their own randomness pools unless it is absolutely necessary.

3.5 Use a System Call, Not a Special File

We argue that a system call is a much safer interface to an OS randomness pool than is a special file (like `/dev/random`). The most dangerous aspect of accessing the randomness pool through a file is that most OSes limit the number of file descriptors that can be open at any one time. If either the per-user or global file descriptor limit is reached, then no process can open the special file to access system randomness. In this case, applications have to choose between two bad alternatives: (a) fail and halt, or (b) proceed without randomness from the OS.

An Attack. Most applications we have inspected choose option (b) above, which opens them up to a file descriptor denial-of-service attack: a coalition of malicious users opens so many files that the system's global file descriptor limit is reached. When an honest user tries to generate a cryptographic secret key (for example), the cryptography library will produce a key derived without access to OS randomness (and thus easy to predict by guessing) [27, 28]. Many components of OpenSSL (including SSL/TLS pre-master secret generation and RSA key generation) are vulnerable to this attack, as is the `arc4random` function used for cryptographic randomness in FreeBSD, OpenBSD, Mac OS, and LibreSSL.



(a) Today's OSes use a single entropy pool shared amongst all processes.

(b) A single malicious process can prevent entropy accumulation indefinitely.

Figure 2: Today's OS randomness subsystems.

Reality 5. *Special-file interfaces for randomness are often unsafe.*

The latest versions of Windows, Linux, and OpenBSD offer a system-call interface, but FreeBSD, Mac OS X, and Solaris do not.

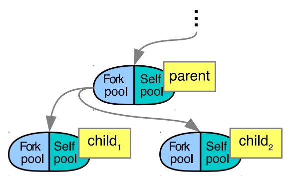
4 Improving OS Randomness to Keep Evil Children Out of Your Randomness Pools

In this section, we propose a new architecture for OS randomness that uses *per-process* randomness pools to ensure entropy accumulation even in adversarial conditions. Our design does not require any form of entropy estimation and eliminates the distinction between "trusted" and "untrusted" inputs to the pools. Also, unlike existing OS randomness implementations, it is secure against the attack described in Section 3.2.

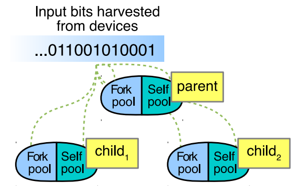
The corollary to Reality 1 indicates that the system's randomness pool is vulnerable *only* in the time before the pool has accumulated enough entropy to seed a PRG (e.g., before it has accumulated 128 bits of entropy). The focus of the randomness subsystem, then, should be to ensure that eventually there is enough entropy in the pool to seed a PRG, even in the presence of many adversarial processes.

To our knowledge, *no current OS* provides this property. Existing OSes use a single common entropy pool shared amongst all processes, as shown in Figure 2. If the system starts out in a known state (e.g., after first boot), the hardware supplies only a few bits of entropy per time unit, and an adversarial process can read a few bits of OS-supplied randomness in every time unit, then the adversary will *always* know the contents of the entropy pool via a brute-force guessing attack (Figure 1) [32, 33, 34]. In these conditions, benign processes will not be able to generate strong cryptographic secrets.

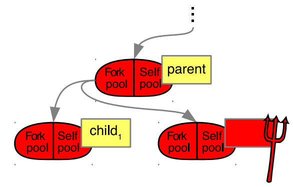
To prevent this failure case, we propose allocating different entropy pools to each process in the system. By limiting the number of pools from which an adversarial process can read, we minimize the number of pools that



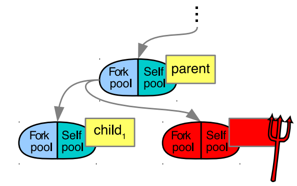
(a) Children of `fork()`s have pools seeded from the parent's fork pool.



(b) The OS replenishes *all* pools in the system in a round-robin fashion.



(c) An evil child might initially be able to learn the state of other pools.



(d) However, the parent's other child processes can eventually accumulate entropy (recover).

Figure 3: Unlike current designs, our pool-per-process design allows the system to accumulate entropy in the presence of a malicious process.

an adversary can attack. This ensures that benign processes eventually accumulate enough entropy to generate strong cryptographic keys (of course, by Reality 2 we will never know precisely *when* this has happened).

In our architecture (Figure 3), the OS maintains two randomness pools for each process in the system: one for generating random values for the process itself and another for initializing the pools of forked child processes. When a process asks the OS for random bits, the OS derives these bits from the first pool, the "self" pool. When a process forks a child process, the OS seeds the child's two randomness pools from the parent's "fork" pool. The OS feeds new input bits into all active pools in the system on a round-robin schedule. Under the minimal assumption that the random input bits are not perfectly correlated with each other, all non-adversarial pools in the system will eventually accumulate enough entropy to seed a PRG.

The use of two separate pools per process provides protection in scenarios where the pool of a parent process contains few bits of entropy and an adversary can repeatedly read from the randomness pools of the parent's recently forked children processes. For example, if the parent is an (honest) forking TLS server, an adversarial client can learn the state of the parent's randomness pool by connecting to a forked child server process and inspecting the nonces in the child process' TLS messages. If the parent's pool started out with few bits of entropy, the adversary will be able to learn the state of the parent's pool and will be able to keep the parent's pool from ever accumulating entropy (using the guessing attack described after the corollary to Reality 1).

By having a separate forking pool, we ensure that the child processes cannot read from the parent's "self" pool and thus the child cannot recover the state of the parent's "self" pool. This allow the parent's "self" pool to eventually accumulate entropy with respect to the adversarial client, even though the "fork" pool never will.

Instead of having a separate "fork" pool, we could just initialize the child's randomness pools to all zeros and let the child's pool accumulate entropy over time from input sources. This addresses the forking attack above, but introduces a more serious problem: a child will not have *any* access to randomness immediately after forking, even if the parent's pool has many bits of entropy. In the case of a forking TLS server, in which a child needs to generate cryptographic secrets immediately after forking, zero-initializing the child's pool is unsatisfactory.

The downside of having separate randomness pools is that the system as a whole will accumulate entropy more slowly than today's systems do—P times more slowly, where P is the number of active pools. Although the reduced entropy accumulation is a drawback, in deployment scenarios where environmental sources of randomness are particularly scarce (e.g., [42, 47]), it is even more important to separate out randomness pools to ensure that eventually honest processes in the system will gain access to unpredictable bits. To increase the rate of accumulation, a process not needing randomness could instruct the OS to stop adding input bits to its "self pool." Since not all processes need access to cryptographic randomness, this could reduce the number of active pools in the system and increase the rate of accumulation.

5 Related Work

There is a long and fruitful line of work investigating randomness failures in operating systems and cryptographic tools. Prior work has found weaknesses in the random number generators used in Debian [19, 55], Java [40], Linux [39, 41], Netscape [38], Windows [35]. Weak hardware entropy sources [42, 47] and use of virtual machine snapshotting [36, 37, 51] also give rise to randomness failures. Lazar et al. investigate the source of bugs in cryptographic software, including cases involving misuse of randomness [46].

Another line of work has proposed techniques to protect against weak randomness. Barak and Halevi [1] and Dodis et al. rigorously analyze random number generators as used in operating systems and offer improved constructions [33, 34]. Mowery et al. conjecture that even embedded devices have potentially rich sources of entropy at boot time [50]. Hedged public-key cryptographic techniques, developed by Bellare et al. [2, 51], allow for a graceful degradation of security in the face of bad randomness. Many of the arguments of Section 3 are in the folklore and some have been discussed in prior work [1, 43, 54]. To our knowledge, no one has proposed using per-process randomness pools as we do in Section 4.

6 Conclusion

We have debunked a number of common misconceptions about randomness in OSes. From the counter-intuitive realities of randomness, we derive a number of straightforward design principles for the OS's randomness subsystem. We also make the unorthodox recommendation that OSes maintain two separate randomness pools for every process. We hope that our paper will encourage OS designers to question common myths about randomness and to rethink how they provide randomness to users.

References

[1] Boaz Barak and Shai Halevi. A model and architecture for pseudo-random generation with applications to `/dev/random`. In *CCS*, pages 203–212. ACM, 2005.

[2] Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. Hedged public-key encryption: How to protect against bad randomness. In *ASIACRYPT*, pages 232–249. Springer, 2009.

[3] Mihir Bellare, Anand Desai, Eron Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *Foundations of Computer Science*, pages 394–403. IEEE, 1997.

[4] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *CCS*, pages 62–73. ACM, 1993.

[5] John Black. The ideal-cipher model, revisited: An uninstantiable blockcipher-based hash function. In *Fast Software Encryption*, pages 328–340, 2006.

[6] Lenore Blum, Manuel Blum, and Mike Shub. A simple pnpredictable pseudo-random number generator. *SIAM Journal on computing*, 15(2):364–383, 1986.

[7] Christian Cachin. *Entropy Measures and Unconditional Security in Cryptography*. PhD thesis, ETH Zürich, 1997.

[8] Jim Chow, Ben Pfaff, Tal Garfinkel, and Mendel Rosenblum. Shredding your garbage: Reducing data lifetime through secure deallocation. In *USENIX Security*, pages 22–22, 2005.

[9] CVE-2000-0357: ORBit and esound in Red Hat Linux do not use sufficiently random numbers, December 1999.

[10] CVE-2001-0950: ValiCert Enterprise Validation Authority uses insufficiently random data, January 2001.

[11] CVE-2001-1141: PRNG in SSLeay and OpenSSL could be used by attackers to predict future pseudo-random numbers, July 2001.

[12] CVE-2001-1467: mkpasswd, as used by Red Hat Linux, seeds its random number generator with its process ID, April 2001.

[13] CVE-2003-1376: WinZip uses weak random number generation for password protected ZIP files, December 2003.

[14] CVE-2005-3087: SecureW2 TLS implementation uses weak random number generators during generation of the pre-master secret, September 2005.

[15] CVE-2006-1378: PasswordSafe uses a weak random number generator, March 2006.

[16] CVE-2006-1833: Intel RNG Driver in NetBSD may always generate the same random number, April 2006.

[17] CVE-2007-2453: Random number feature in Linux kernel does not properly seed pools when there is no entropy, June 2007.

[18] CVE-2008-0141: WebPortal CMS generates predictable passwords containing only the time of day, January 2008.

[19] CVE-2008-0166: OpenSSL on Debian-based operating systems uses a random number generator that generates predictable numbers, January 2008.

[20] CVE-2008-2108: GENERATE_SEED macro in php produces 24 bits of entropy and simplifies brute force attacks against the rand and mt_rand functions, May 2008.

[21] CVE-2008-5162: The arc4random function in FreeBSD does not have a proper entropy source for a short time period immediately after boot, November 2008.

[22] CVE-2009-0255: TYPO3 creates the encryption key with an insufficiently random seed, January 2009.

[23] CVE-2009-3238: Linux kernel produces insufficiently random numbers, September 2009.

[24] CVE-2009-3278: QNAP uses rand library function to generate a certain recovery key, September 2009.

[25] CVE-2011-3599: Crypt::DSA for Perl, when `/dev/random` is absent, uses the Data::Random module, October 2011.

[26] CVE-2013-1445: The `crypto.random.atfork` function in pycrypto before 2.6.1 does not properly reseed the pseudo-random number generator (prng) before allowing a child process to access it, October 2013.

[27] CVE-2013-4442: Password generator (aka Pwgen) before 2.07 uses weak pseudo generated numbers when `/dev/urandom` is unavailable, December 2013.

[28] CVE-2013-5180: The `srandomdev` function in Libc in Apple Mac OS X before 10.9, when the kernel random-number generator is unavailable, produces predictable values instead of the intended random values, October 2013.

[29] CVE-2013-7373: Android before 4.4 does not properly arrange for seeding of the OpenSSL PRNG, April 2013.

[30] CVE-2014-0016: tunnel before 5.00, when using fork threading, does not properly update the state of the OpenSSL pseudo-random number generator, March 2014.

[31] CVE-2014-0017: The `rand_bytes` function in `libssh` before 0.6.3, when forking is enabled, does not properly reset the state of the openssl pseudo-random number generator, March 2014.

[32] CVE-2014-4422: The kernel in Apple iOS before 8 and Apple TV before 7 uses a predictable random number generator during the early portion of the boot process, October 2014.

[33] Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergniaud, and Daniel Wichs. Security analysis of pseudo-random number generators with input: `/dev/random` is not robust. In *CCS*, pages 647–658. ACM, 2013.

[34] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too-optimal recovery strategies for compromised rngs. In *CRYPTO*, volume 2014.

[35] 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*, CCS, pages 476–485, 2007.

[36] Adam Everspaugh, Yan Zhai, Robert Jellinek, Thomas Ristenpart, and Michael Swift. Not-so-random numbers in virtualized linux and the whirlwind rng. In *IEEE Security and Privacy*, 2014.

[37] Tal Garfinkel and Mendel Rosenblum. When virtual is harder than real: Security challenges in virtual machine based computing environments. In *HotOS*, 2005.

[38] 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.

[39] Peter Gutmann. Random number generation. *Cryptographic Security Architecture: Design and Verification*, pages 215–273, 2004.

[40] Zvi Gutterman and Dahlia Malkhi. Hold your sessions: An attack on Java session-id generation. In *CT-RSA*, pages 44–57, 2005.

[41] Zvi Gutterman, Benny Pinkas, and Tzachy Reinman. Analysis of the Linux random number generator. In *IEEE Security and Privacy*, pages 371–385, 2006.

[42] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *USENIX Security Symposium*, pages 205–220, 2012.

[43] Thomas Hühn. Myths about `/dev/urandom`. `http://www.2uo.de/myths-about-urandom/`, November 2014.

[44] Alex Klyubin. Some SecureRandom thoughts. `http://android-developers.blogspot.com/2013/08/some-securerandom-thoughts.html`, August 2013.

[45] Hugo Krawczyk. Cryptographic extraction and key derivation: The HKDF scheme. In *CRYPTO*, pages 631–648. Springer, 2010.

[46] David Lazar, Haogang Chen, Xi Wang, and Nickolai Zeldovich. Why does cryptographic software fail?: A case study and open problems. In *Proceedings of 5th Asia-Pacific Workshop on Systems*, page 7. ACM, 2014.

[47] Arjen K Lenstra, James P Hughes, Maxime Augier, Joppe W Bos, Thorsten Kleinjung, and Christophe Wachter. Ron was wrong, Whit is right. *IACR ePrint archive*, 64, 2012.

[48] James L. Massey. Guessing and entropy. In *International Symposium on Information Theory*, page 204. IEEE, 1994.

[49] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 2010.

[50] Keaton Mowery, Michael Wei, David Kohlbrenner, Hovav Shacham, and Steven Swanson. Welcome to the Entropics: Boot-time entropy in embedded devices. In *IEEE Security and Privacy*, 2013.

[51] Thomas Ristenpart and Scott Yilek. When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. In *NDSS*, 2010.

[52] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[53] Nick Sullivan. Ensuring randomness with Linux's random number generator. `http://blog.cloudflare.com/ensuring-randomness-with-linuxs-random-number-generator/`, October 2014.

[54] John Viega. Practical random number generation in software. In *ACSAC*. IEEE, 2003.

[55] Scott Yilek, Eric Rescorla, Hovav Shacham, Brandon Enright, and Stefan Savage. When private keys are public: Results from the 2008 Debian OpenSSL vulnerability. In *IMC*, pages 15–27, November 2009.