

## Re: Toaster to Generate Random Numbers

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-01/0369.html>

---

**From:** Nicol So ([nobody@no.spam.please](mailto:nobody@no.spam.please))

**Date:** 01/17/03

From: Nicol So <nobody@no.spam.please>

Date: Fri, 17 Jan 2003 17:28:44 -0500

Bill Unruh wrote:

>

> *Paul Crowley <[paul@JUNKCATCHER.ciphergoth.org](mailto:paul@JUNKCATCHER.ciphergoth.org)> writes:*

>

> *JA secure PRG is one for which if the input is fairly drawn, the output*

> *jis indistinguishable from a fairly drawn output, and so in effect is*

> *jas good as a fairly drawn output for any purpose.*

>

> *No, it is NOT "as good as". That is why people worry about a PRNG being*

> *broken. It spews out a completely deterministic string given a small*

> *input. The entropy of the output cannot be higher than the entropy of*

> *that small input.*

It think Paul's "as good as" comment could use some clarification. The output of a *secure* PRNG is as good as maximally random bit sequence in *some* (realistic) threat models. But the same is not true in other threat models.

> *Now it may be difficult to break, but the amount of time needed to break*

> *it is strictly bounded by the effort to run an exhaustive search on the*

> *inputs. That effort is small (in the context of the output) and the*

> *entropy is small.*

In contexts in which PRNGs are used, that the adversary is resource-bounded is implicitly assumed. The defining property of a secure PRNG is that its output is distinguishable, *to the resource-bounded adversary*, from a true random sequence with at most a negligible probability, regardless of what algorithm the adversary executes.

For any realistic adversary, it is easy to scale up the security parameter to a point where exhaustive search becomes infeasible for the adversary. Once something is infeasible, it doesn't matter whether it is infeasible for information-theoretic reasons, or for computational complexity reasons.

> *Now, it is certainly true that for many situations, that output of the*

comp.security.misc: Re: Toaster to Generate Random Numbers

- > *PRNG may be good enough, even though it contains very little entropy and*
- > *is not random. Ie , it may contain those properties which a real random*
- > *number stream has which you need. Fine. For those instances use a PRNG.*

--

Nicol So

Disclaimer: Views expressed here are casual comments and should not be relied upon as the basis for decisions of consequence.