

# Re: How to develop a random number generation device

---

*Source:* <http://sci.tech-archive.net/Archive/sci.electronics.design/2007-09/msg03303.html>

---

- *From:* Rich Grise <[rich@xxxxxxxxxxxx](mailto:rich@xxxxxxxxxxxx)>
  - *Date:* Mon, 17 Sep 2007 23:15:52 GMT
- 

On Mon, 17 Sep 2007 23:37:49 +0100, Nobody wrote:

On Sat, 15 Sep 2007 17:06:31 +0000, Rich Grise wrote:

That doesn't address the issue, which was whether the OS can prevent buffer overruns.

With a hardware MMU, and software that can catch the exception, yes.

That still doesn't address the question of how you decide that a write operation has overrun its buffer; the details of where one buffer starts and another ends are unknown to the OS.

But it knows what chunks of memory it has allocated to a particular process. As long as it's in your own memory space, who cares if you overwrite/overrun your own buffers?

Doing so is the essence of a "buffer overrun exploit", one of the most common types of security vulnerability for code written in C/C++.

It allows a malicious user to make a program do something that it isn't supposed to do.

E.g. consider a program being run on a web server to process form input from a web page. If the program suffers from a buffer overrun flaw, simply sending the right data in a POST request can allow the attacker to execute arbitrary code on the web server.

Re: How to develop a random number generation device

My God! You've got to quit using MICRO\$~1 web servers!

Good Luck!

Rich

.