

Re: How to develop a random number generation device

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2007-09/msg02875.html>

- *From:* JosephKK <joseph_barrett@xxxxxxxxxxxxxx>
 - *Date:* Sat, 15 Sep 2007 19:48:55 GMT
-

MooseFET kensmith@xxxxxxxx posted to sci.electronics.design:

On Sep 12, 9:26 pm, JosephKK <joseph_barr...@xxxxxxxxxxxxxx> wrote:

John Larkin jjlar...@xx posted to sci.electronics.design:

On Tue, 11 Sep 2007 17:28:32 +0100, Nobody <nob...@xxxxxxxxxxxxxx> wrote:

On Tue, 11 Sep 2007 07:44:01 -0700, John Larkin wrote:

Cool. When can we expect buffer overrun exploits to be impossible under Windows?

When it stops letting you run arbitrary machine code.

Nothing the OS does can prevent machine code from overrunning a buffer.

Re: How to develop a random number generation device

Ancient computers, PDP-11 and VAX certainly, had memory management hardware that separated I and D space, where I space was read-only, and D space could not be executed. And the OS's enforced those rules. It was common to have many users running the exact same code, but mapped into different data spaces.

Problem is, neither Intel nor Microsoft was in the mainstream of computing when they kluged up x86 and Windows.

John

The hardware only became capable of the basics of worthwhile implementation in early Pentiums, and became capable of really worthwhile implementations with Opteron (AMD) and EMT64 (Intel).

I disagree with what you may not have meant to say above. In the microprocessor area, you are largely correct but in other machines, there were many hardware systems that could protect against buffer overflows getting evil code to run. Some of them used a different stack for call and return than for the data. Some such as the IBM-360 didn't have a stack and required each routine to handle its "save area".

Some of the more DSPish machines would also be hard to make a buffers overflow do anything evil. They are far from general purpose machines so although they may show that it could have been done, we can say that they could have made a general purpose PC that was well defended.

OK. Thanks for the addition to my knowledge.