Subject: Random number generators
Posted by TRNG98 on Tue, 11 Jan 2011 05:19:00 GMT
View Forum Message <> Reply to Message

I once had a customer who asked many questions on how to integrate a hardware random number generator to a computer application.

This is not uncommon; most customers use a hardware random number generator for a game application, a lottery, or possibly a statistical science application. This was a bit different, after a while it came out what he was trying to accomplish.

He ran security for a diamond mine. In such a mine a security issue is that a worker can find a diamond in the dirt, and then pocket it and take it home. So workers are searched when they leave work. But, for cost and convenience, they don't search all workers when they leave the mine. He was looking for a solution, where guards could not select who is to be searched. Co-operation between a worker and a guard should also be eliminated.

An additional complication -- this was in the south part of Africa -- that possibly a majority of the guards was white, while the workers was mostly black. But not all workers are black, some are also white. Some kind tricky situation emerge, of a political nature, that could be solved eliminating the thought that the white gourds never select a white worker for search.

The solution used a serial port random number generator such as the TRNG9803.

Subject: Re: Random number generators
Posted by David_T on Fri, 21 Jan 2011 18:56:02 GMT
View Forum Message <> Reply to Message

I was wondering if these special applications are common? Most units are used for computer security?

Subject: Re: Random number generators
Posted by TRNG98 on Sun, 23 Jan 2011 10:27:37 GMT
View Forum Message <> Reply to Message

My opinion would be that most units are sold for game applications and lotteries. The typical application would be a poker server.

Subject: Re: Random number generators
Posted by RWilliamson3 on Thu, 19 Jan 2012 05:14:04 GMT
View Forum Message <> Reply to Message

When I was working software for a Poker company, a strange thing occurred. The random

number testing failed on one of the production servers in Netherlands Antilles, in this case running test-scripts for the next update. This server had a hardware random number add-on that seeded the Linux /dev/random. Apparently the hardware had failed in some way, and this not only did stop the hardware generated contribution, the software messed up the normal operation in some way so that the statistical testing failed.
I was brought in on this issue, as the software guys thought that there was something wrong with the statistical test software!
