

Real-World Scenario 14-2: PRNGs

Scenario: Once again, you are a security administrator working alongside your organization's development team. You come across some code as shown in the figure below. Examine the figure. According to one of the developers, the code is being used to collect noise in an attempt to increase entropy.

What type of algorithm are we developing here?

```
int randomData = open("/dev/random", O_RDONLY);
char myRandomData[50];
size_t randomDataLen = 0;
while (randomDataLen < sizeof myRandomData)
```

Real-World Scenario 14-2 Solution

Based on the code in the figure we are most likely developing a pseudorandom number generator (PRNG). These are used in cryptography systems and games to generate a sequence of “random” numbers. `/dev/random` and `/dev/urandom` are common files used to collect noise in order to increase entropy. They could be used with `java.util.rand`, for example. Depending on the system and environment you might also use `getrandom` (Linux) and `arc4random` (OpenBSD). The video solution below introduces PRNGs.

Video Solution: Watch the video solution “14-2: PRNGs.”