Published on *Tux Machines* (http://www.tuxmachines.org)

Shrinking Linux Attack Surfaces

By *Roy Schestowitz*
Created *18/07/2019 - 12:28pm*
Submitted by Roy Schestowitz on Thursday 18th of July 2019 12:28:18 PM Filed under Linux [1] Security [2]

Often, a kernel developer will try to reduce the size of an attack surface against Linux, even if it can't be closed entirely. It's generally a toss-up whether such a patch makes it into the kernel. Linus Torvalds always prefers security patches that really close a hole, rather than just give attackers a slightly harder time of it.

Matthew Garrett recognized that userspace applications might have secret data that might be sitting in RAM at any given time, and that those applications might want to wipe that data clean so no one could look at it.

There were various ways to do this already in the kernel, as Matthew pointed out. An application could use mlock() to prevent its memory contents from being pushed into swap, where it might be read more easily by attackers. An application also could use atexit() to cause its memory to be thoroughly overwritten when the application exited, thus leaving no secret data in the general pool of available RAM.

The problem, Matthew pointed out, came if an attacker was able to reboot the system at a critical moment?say, before the user's data could be safely overwritten. If attackers then booted into a different OS, they might be able to examine the data still stored in RAM, left over from the previously running Linux system.

As Matthew also noted, the existing way to prevent even that was to tell the UEFI firmware to wipe system memory before booting to another OS, but this would dramatically increase the amount of time it took to reboot. And if the good guys had won out over the attackers, forcing them to wait a long time for a reboot could be considered a denial of service attack?or at least downright annoying.

[3]

Linux Security

Source URL: http://www.tuxmachines.org/node/126025

Links:
[1] http://www.tuxmachines.org/taxonomy/term/63
[2] http://www.tuxmachines.org/taxonomy/term/59
[3] https://www.linuxjournal.com/content/shrinking-linux-attack-surfaces