# Additional / useful / interesting links

* [‘How I Hacked my Car’, 2022-05-22 :: greenluigi1](https://programmingwithstyle.com/posts/howihackedmycar/)
* Related: [Securing Build Infrastructure: Code Signing Key Protection, Bhat, TimeSys, Oct 2022](https://www.timesys.com/security/securing-build-infrastructure-code-signing-key-protection/)
* [‘10 Years of Linux Security: A Report Card’, Bradley Spengler](https://grsecurity.net/10_years_of_linux_security.pdf)
* Linux kernel addr\_limit bug / exploitation :

<https://www.youtube.com/watch?v=UFakJa3t8Ls>

"Using syscalls in the kernel (or simply forgetting to reset the addr\_limit

value before returning to user space) may lead to this type of bugs. We're

using a stack info leak with the buggy get\_fs/set\_fs code to overwrite the

(e)uid and (e)gid of the current process to elevate privileges."

thread\_info.addr\_limit : highest userspace addr.

* MITRE [D3FEND™ : A knowledge graph of cybersecurity countermeasures](https://d3fend.mitre.org/)

Books

* ‘Hacking: the Art of Exploitation’, Jon Erickson, 2nd Ed, No Starch Press, 2008 : though old, it’s simply superb; a must-read.