Software Assurance Tips

A product of the Software Assurance Tips Team[1]

Generated Monday 24th May, 2021

Jon Hood

Monday 24th May, 2021

1 Side-Channel Attacks

The insider threat is one of the most difficult to find. I thought I'd lay out some ways in which we've found side-channel attacks (CWE-514) in actual systems that we have evaluated. They include:

- Inadvertent data through a backdoor
- Purposeful use of hard drive architectures to hide files
- Using seemingly benign documents to deliver an evil payload

1.1 Development Backdoors

Developers often leave backdoors into a system. This is sometimes left-over debug access meant to speed up development (CWE-489). When these backdoors are deployed in the wild, they become attack vectors wielded to access and sneak data out of a system without any visibility in logs and access control mechanisms. But this article primarily deals with the intentional side channels:

1.2 Malicious Hardware

Hard drive architectures and other removable media can be exploited to provide a side channel. Suppose that you want to send a sensitive file to a malicious entity, but you don't want that file to show up in any filesystem scans or perfunctory data scans of the media. The data may be hidden outside of filesystem control. In *nix systems, the dd command can be used to hide data outside of the filesystem. Assuming the removable device is /dev/sdb (it doesn't even have to be partitioned) and it has 1465149168 sectors, an attacker can run "`dd of=/dev/sdb bs=512 skip=1465140001 < 'I am a sneaky little string!'`" to sneak their message onto the hard drive. To retrieve the string, the recipient can simply "`dd if=/dev/sdb bs=512 skip=1465140001 count=30`" and retrieve the text.

This becomes especially hidden when:

1. The filesystem does not have anything else stored at the sectors starting at 1465140001
2. There is no filesystem provisioned that includes the sectors starting at 1465140001
3. A Host Protected Area (HPA) is set so that the operating system can't see anything past sector 1465140000 ("`hdparm -N p1465140000 /dev/sdb && reboot`")

1.3 Malicious Software

Seemingly benign files can hide an attacker's payload. Don't believe me? Then take the PDF or HTML version of this tip and run the commands in Listing 1 against it in cygwin!

```
$ cat -v 20210524.pdf | grep "^%PAY:" | tail -c +6 | base64 -d > sneaky.exe
$ chmod +x sneaky.exe
$ ./sneaky.exe
```

Listing 1: Hidden Binary in This File

References

[1] Jon Hood, ed. *SwATips*. https://www.SwATips.com/.