Software Assurance Tips

A product of the Software Assurance Tips Team[3]

Jon Hood

Monday 31st January, 2022

1 So you put an Unclassified CD in a Classified Machine

Updated Tuesday 1st February, 2022

NOTE: When in doubt, it's always appropriate to ask your security office for guidance. Hiding a potential mistake carries a greater penalty than admitting a mistake that turns out to be insignificant. The scenario in this article is contrived. If you got here from a search engine because you're wondering if you should report a security incident, you should probably go ahead and call your security officer that you are investigating a possible incident. They have the authority to establish enhanced rules and should have the expertise to help you.

1.1 A Nervous Newbie

It had already been a long, stressful day at work when the panicked, young professional sheepishly knocked on my door to report that they "did a dumb." The terror in his voice made me think that he had either given classified information to a hostile government or that he was a spy admitting that he wanted to defect.

But the truth was much more benign. This young employee had taken a finalized, unclassified, properly-marked CD-R with some unclassified software on it and loaded the software onto his shiny new classified analysis machine. After he finished the installation, he placed the CD beside the machine and continued working, only to notice his coworker installing the software on her new unclassified machine a little while later.

These two young employees had been trained that a CD-R placed onto a classified computer makes the CD go to the classification of the information system it's placed on. They then did the right thing–unplug the lower-classified machine and report a possible security violation.

Certainly, each information system can have its own requirements for how to handle such a scenario, but in general, the DoD and Army have published guidance and minimum security requirements for how to handle such things. There are two things that can go classified in the above scenario: the storage media and the data on it.

1.2 The Data

Security violations always receive priority handling of everyone involved. It's an immediate "stop work and fix it" scenario. But the data involved was inconsequential: an installer for a common word processor that had nice text markup for the programming languages these employees were analyzing. The data was unimportant from a security and OPSEC standpoint; it was data that was already publicly released and freely available on the internet.

Had the employees loaded data of a higher classification onto a lower-classified machine, we'd have what's known as a spillage event, and the data owners of the higher classified data would have the authority to dictate cleanup procedures that we would follow.

1.3 The Media

I recognized the media immediately. It was a CD I had burned with analysis tools the previous month. My practice is to burn a single-session UDF CD that can be written only once to help mitigate the risk of security violations for this specific scenario. I breathed a sigh of relief when they brought the finalized CD to me.

The metric for increasing the classification of removable media is "if the level of classification of the information on the medium changes."[1, § 4.b] The information system that the CD was being used on permits the use of data diodes (one-way data connections from low to high). I could verify that the classified machine could not and did not write data to the CD. You can see this metric for classified media documented in the examples of DA PAM 25-2-13. Section 4-7.a–b gives the requirements for when inserting a SIPR token into a NIPR computer is and is not a security violation. Section 4-7.c gives the scenarios for declaring a security incident when a NIPR token is inserted into a SIPR machine, pointing out that the metric for an incident is “if classified data were written to the token, or if malicious code was introduced.”[2] Merely inserting a NIPR token into a properly-configured SIPR machine is not a security incident, just like inserting any other unclassified media into a classified machine may not be a security incident.

1.4 Conclusion

Each information system’s security department is different and defines its own rules for when removable media can go classified. There is always the possible scenario where an important tactical mission is using a Sega Dreamcast that reads discs from the outside inward, making it possible to write classified data to the end of a finalized CD or DVD. That’s why security offices exist, and reporting a possible security violation is asking those officers to perform a role they’re already being paid to do.

In the situation documented above, the optical drive was incapable of burning data to a properly finalized, non-rewritable disc. All of the possible filesystem records were checked for modification, and the security office was called to verify that there were no additional security policies documented governing the insertion of unclassified, write-protected media into a classified environment.

Nevertheless, you can help by using data diodes, properly marking media, finalizing non-rewritable CDs and DVDs, and verifying the state of finalized/write-protected media when it is inserted into higher-classification environments. Remember that optical media often has multiple filesystem tables that must be verified (often Joilet and UDF).

References

[1] Department of Defense. Department of Defense Manual 5200.01 Volume 2. Tech. rep. Incorporating Change 4, Effective July 28, 2020. Washington, D.C.: Department of Defense, 2020. URL: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520001m_vol2.pdf.

[2] Department of the Army. Department of the Army Pamphlet 25–2–13. Army Identity, Credential, and Access Ma Tech. rep. Washington, D.C.: Department of the Army, 2019. URL: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN17425_P25_2_13_Admin_FINAL.pdf.

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