

Review and Outlook of the Detection of Viruses using Intrusion Detection Systems

Morton Swimmer
IBM T. J. Watson Research Center
Antivirus Sciences and Technologies
Hawthorne, USA-NY 10532

Extended Abstract

A few years ago, I demonstrated that MS-DOS viruses could not only be reliably detected by an IDS (we called the prototype VIDES), but also classified into particular families using detailed audit data and appropriate rules (see [?] and [?]). I was able to detect 95% of the known viruses time with only a small set of rules, in contrast to the thousands of pattern required at the time to detect the same viruses in a string-based scanner. So, why are antivirus vendors not using intrusion detection to catch viruses? In this paper I will explore the reasons for this as well as the possibilities opening up for IDS use in virus detection in the future.

First of all, I will show how some current antivirus technology is similar to IDS technology. In particular, the so-called online scanners are similar to host-based IDS. However, in contrast to IDS, such components must cooperate with removal and administrative tools to be effective. The most effective model is manifest in the Digital Immune System, which may offer an interesting model for maintenance of an effective IDS.

Next, I will elaborate on the use of IDS technology in finding and defending against viruses. A few years ago, together with Dr. Le Charlier and Dr. Mounji, we showed that MS-DOS viruses could be found using fairly simple IDS patterns reliably ([?] and [?]). The implementation or the sensors was impractical for commercial use, because of the way the sensor was implemented, but found a home in the analysis center of the Digital Immune System. I will discuss the implications when trying to catch newer classes of viruses. The key is creating sensors. I will discuss the difficulties in creating sensors capable of detecting the activity of macro viruses and 32-bit MS-Windows viruses.

Once we have detected a virus, what do we do? In a Digital Immune System environment (see [?] or [?]), the sample will be sent to the analysis center for analysis and deployment of antigen. Currently, heuristics based on string n-gram heuristics (or similar methods), are used to find suspicious objects, and the quality of the heuristics determines the number of false positives and false

negatives. A virus IDS is a very powerful heuristic, probably the best as it is possible to observe the virus property directly. Still, an IDS is badly positioned to find an antigen and use it, so cooperating with a Digital Immune System and a virus scanner is the best approach.

I will also describe some work by Dr. Fischer-Hübner and myself [?] into intrusion detection and avoidance of viruses (IDA). However, this work was better formalized in a Rule Based Access Control (RBAC) antivirus policy as described in [?]. Both approaches require a secure system, and therefore not applicable to MS-Windows-based machines.

Finally, I will conclude with an informal discussion on why I believe using an IDS to find viruses is a powerful approach to virus intrusion detection. The replication of viruses is sufficiently unique to be able to create rules that have both low false positives and false negatives. The challenges are in creating sensors that are robust enough and collect the required data.