Defeating Zero-Day Malware: A New Approach
The Software Inspection and Certification System (SI6)

The Problem
Malicious software on the Internet continues to be a severe, pervasive problem. New threats are announced on a weekly basis. Novel malware, known as zero-days, is the most severe form; the threat presented has been growing steadily for many years.

Because standard antivirus software has a very difficult time detecting zero-days, they often persist for months, if not years, on the machines they have infected.

Most estimates put the value of the cyber-crime market at $17B, making it almost twice as large as the cybersecurity marketplace ($10B). Criminals have a very strong economic motivation to continue to develop zero-days. Kits for creating such malware can be bought for as little at $1500.

State of the Art
Commercial antivirus software predominately uses two techniques: pattern matching and anomaly detection. Pattern matching uses a database of “signatures”. Suspect software is scanned to search for a match against previously identified malware. AV products that use this technique require frequent updates to the signature database in order to stay current.

Anomaly detectors use machine learning algorithms (classifiers). A variety of different event types are processed by the classifier, which attempts to assign events to one of two types: benign or malignant. Anomaly detectors may also be combined with signature detection.

The Solution
The Software Inspection and Certification System (SI6) takes a completely new approach. A security specification is created based on the underlying properties that benign binary software must obey. These rules are combined with specific information derived from the software under test to create a model. That model is then checked in the cloud. Rule violations indicate malware. Software that passes all tests is digitally signed to show that it is secure.

This approach has no false positives – any rule violation can be directly traced to a flaw in the software under test. It also has a false negative rate that can be as small as desired. Increasing the search depth decreases the likelihood of undetected malware.

This software has been demonstrated to detect zero-days in Java and Flash before they were officially announced. A complete prototype of SI6 already exists for Java. Flash has a partial implementation and other languages are in work.

Commercial AV products are very effective (99%) against known malware, but are very ineffective against zero-days (5% - 50%). Commercial AVs often have high false positive rates (up to 20%).

Mark C. Reynolds  markreyn@bu.edu