Security of Security Tools

As computers become an inseparable part of many persons’ everyday life, plenty of critical personal information is stored in computers and many commercial activities are proceeded through computers and networks. Hence, computers become a major battlefield between attackers and computer users. In order to defense computer systems against incessant attacks from various resources, diverse security tools, such as anti-virus software, auto-patch mechanisms, firewall, and intrusion detection systems, have been developed to handle this critical work. However, as the complexity of these security tools increases and the security tools also become attack targets, the security of the security tools also become a crucial issue. Research has shown that diverse approaches have been developed to disable different anti-virus software. Hence, an immediate problem to this type of security tools is how to guarantee the normal operation of them. If attackers can disable anti-virus software, is it possible that they can also change the behavior of the anti-virus software through replacing, injecting, or hooking code? Given the fact that most, if not all, computers allow only one anti-virus application to be installed on them at one time, an attacker that can control the anti-virus application of a computer can fully command the computer without being detected. Moreover, when computers can automatically execute auto-patch code, how could a computer guarantee that the auto-patch code it executes is not malicious code? If the correctness of auto-patch code cannot be protected, instead of being a tool to seal the security breaches of a computer, auto-patch may become an efficient channel for attackers to intrude a computer or spread malicious code. The above issues disclose an important security problem that can influence the results of the wars between attackers and computer users. Hence, when security tools staying in the most frontline to protect our systems, how could we guarantee the security of the security tools?