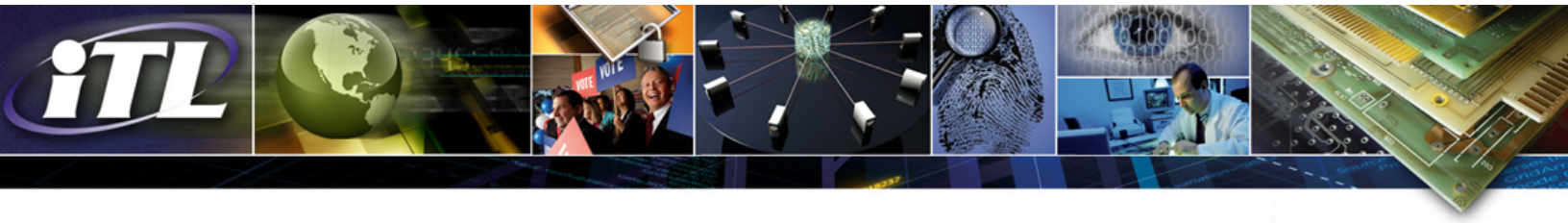


ITL BULLETIN FOR DECEMBER 2015

STOPPING MALWARE AND UNAUTHORIZED SOFTWARE THROUGH APPLICATION WHITELISTING

Adam Sedgewick, Murugiah Souppaya, Karen Scarfone,[1] and Larry Feldman,[2] Editors
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

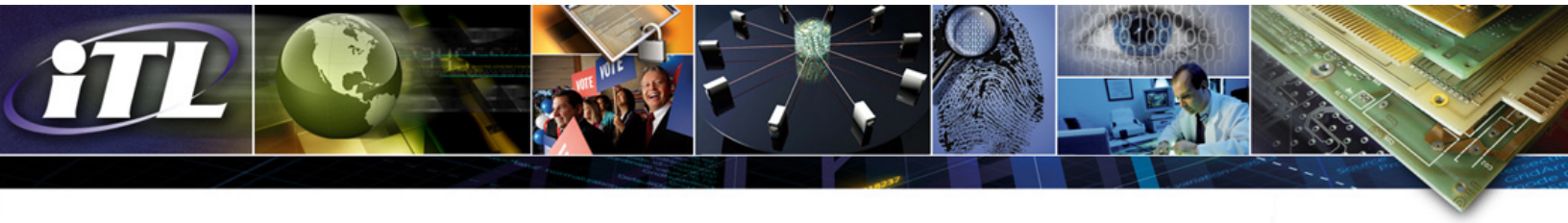
NIST's Information Technology Laboratory has released a significant new guidance document, Special Publication (SP) 800-167, *Guide to Application Whitelisting*. Application whitelisting technologies control which applications may be installed or executed on a computer. These technologies are most often used to detect and stop the execution of malware and other unauthorized software. Malware infections are frequently used to steal sensitive information from a user or an organization, and to tamper with the integrity and availability of computing systems. Unauthorized software can pose multiple problems. For example, it can introduce unmanaged, vulnerable software into the environment, which can then be used by attackers to exploit hosts and further compromise them. NIST Special Publication (SP) 800-167, *Guide to Application Whitelisting,* explains the basics of application whitelisting technologies and shows organizations how they can plan for, implement, and use these technologies successfully.

The Need for Application Whitelisting Technologies

An application whitelist is a list of applications and application components, such as software libraries, browser plug-ins and add-ons, and configuration files that are approved for use on an organization's computers. The application whitelisting technology is the mechanism for specifying and enforcing the whitelist. Application whitelisting works on the opposite principle from antivirus software, which is based on defining malicious behavior and blocking anything that is clearly malicious. Application whitelisting permits only that which is known to be acceptable to the organization and blocks everything else, malicious or benign. As antivirus software becomes less effective, many organizations are turning to whitelisting approaches to complement antivirus software.

In addition to stopping malware, application whitelisting technologies have other purposes and functions. They can be used to stop the execution of unlicensed software and other software that is not appropriate to install or run on the organization's systems. Also, an organization can use application whitelisting technologies to keep an inventory of the applications and application versions installed on each desktop, laptop, and server. This inventory can then be used to identify unauthorized applications that need to be removed and outdated software that needs to be updated, upgraded, or replaced because of known vulnerabilities.

[1] Karen Scarfone is a Guest Researcher from Scarfone Cybersecurity.
[2] Larry Feldman is a Guest Researcher from G2, Inc.



Other common functions for application whitelisting technologies include the following:

- **File Integrity Monitoring.** Most application whitelisting technologies can monitor application files and identify all attempts to change those files. Depending on the whitelisting product and its configuration, it may be possible to stop the changes, but at a minimum, the product can immediately report all such changes.

- **Incident Response.** If an incident occurs and an organization has already deployed application whitelisting technologies, incident responders could configure the whitelisting technology to recognize the characteristics of a malicious application and its files and to immediately check all systems for files that match those characteristics, indicating that the systems have been similarly compromised.

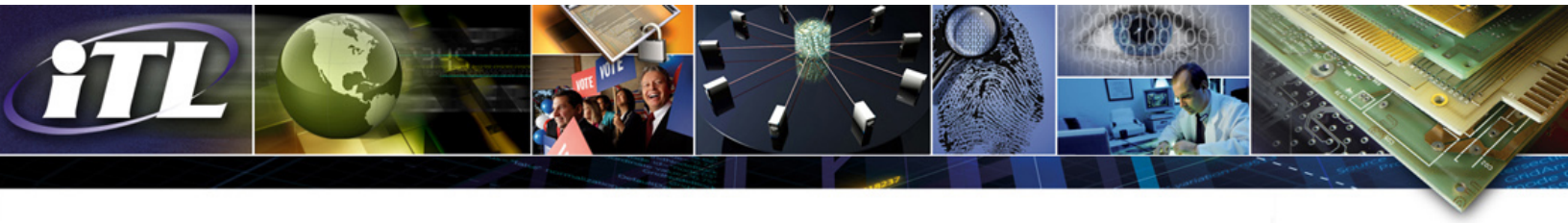
- **Access Control.** Some application whitelisting technologies can restrict file usage on removable media, such as prohibiting the execution of applications stored on unauthorized USB flash drives.

- **Software Reputation Services.** An application whitelisting technology may support the use of software reputation services. Such a service may, for example, indicate that a particular application is often bundled with malware, so the presence of that application means that it is more likely that malware is also present on the system.

Considerations for Choosing an Application Whitelisting Solution

Application whitelisting technologies are best suited to desktops, laptops, and servers in highly managed environments, as well as specialized devices such as point of sale (POS) terminals that have a single function and are frequently targeted by attackers. In these cases, the organization has a great deal of control over the configuration and security of its systems. An organization considering application whitelisting usage in a managed environment should perform a risk assessment to determine whether the security benefits will outweigh its possible negative impact on operations. An application whitelisting solution running in enforcement mode will automatically block execution of all applications and application components that are not on its whitelist, so if that whitelist is not 100 percent accurate and up to date, some benign applications will inadvertently be blocked, preventing users from doing their jobs.

An organization may require additional resources to maintain application whitelists for its systems. Generating a whitelist is easy; use vendor-provided information on benign off-the-shelf applications and supplement it with organization-specific information on custom applications. A second approach is to scan the files on a freshly built desktop, laptop, server, or other device to generate a known good baseline for applications. Maintaining a whitelist is more time-consuming. When a new application is brought into the organization or an existing application is patched, updated, or upgraded, there is a new set of application file characteristics that the whitelisting technology has to be updated to recognize.



There are multiple approaches to solving this problem. One approach is for the organization to manually review each new application and application file change, record the affected files' characteristics, and update the whitelists accordingly. This tends to be labor-intensive and to cause delays in allowing execution of new and updated software, which may not be acceptable. Another approach, chosen by most organizations, is to use maintenance options offered by most application whitelisting technologies. For example, the whitelisting administrator could designate certain services, such as the organization's patch management solution, as being trusted application updaters. Any changes they make to application files are automatically accepted by the whitelisting technology. Similar options are often available for designating trusted software publishers, users (such as system administrators), and software source locations.

All organizations are encouraged to test any prospective application whitelisting technology to see how it behaves before deploying it. Application whitelisting can be deployed in an audit or monitoring mode that indicates which application activity would be blocked without actually blocking that activity. This gives an organization a chance to see how well the whitelist maintenance functions work and what impact any deficiencies in whitelist maintenance may have on operations.

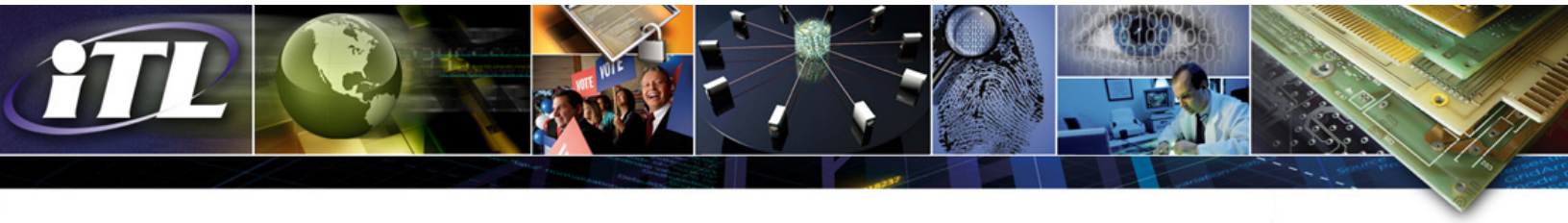
Although the focus of NIST SP 800-167 is on protecting desktops, laptops, and servers, it does mention the rapidly emerging field of applying application whitelisting to mobile devices. Today this is primarily achieved through mobile device management (MDM) and mobile application management (MAM) solutions. Organizations that wish to implement application whitelisting for their mobile devices should look to MDM and MAM products for potential solutions.

Solution Design

Once an organization has chosen the application whitelisting technologies that best meet its needs, the next step is to design an overall whitelisting solution. In addition to addressing whitelist maintenance, organizations should also carefully consider the following.

Cryptography is used to generate and verify cryptographic hashes for application components, to validate digital signatures for application files, and to protect the confidentiality and integrity of communications between hosts using application whitelisting and centralized whitelisting management systems. Federal agencies must use Federal Information Processing Standards (FIPS)-approved or NIST-recommended algorithms contained in validated cryptographic modules to perform all of these cryptographic functions.

Most application whitelisting technologies can operate only as a centrally managed solution; although there may be copies of whitelists on individual systems, enterprise management of the whitelists and the whitelisting functionality is centralized. Each desktop, laptop, and server must have software either built into the operating system or added through a whitelisting application that performs the application whitelisting enforcement and auditing.



Conclusion

NIST SP 800-167 gives insights into how application whitelisting technologies work and provides recommendations for selecting, implementing, and maintaining these technologies to prevent malware execution on desktops, laptops, servers, and specialized devices.

Deploying application whitelisting is generally straightforward in highly managed environments and in environments with POS terminals and other single-function devices that are frequently targeted by attackers. Maintaining effective application whitelisting requires updating the whitelists to include new applications and authorized changes to existing applications. Organizations have to balance the need to prevent execution malware or other unauthorized software from being executed with the need to enable users to run legitimate applications in a timely manner, without having to wait for whitelists to be updated.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov