April 2008

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

USING ACTIVE CONTENT AND MOBILE CODE AND SAFEGUARDING THE SECURITY OF INFORMATION TECHNOLOGY SYSTEMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Private and public sector organizations face complex challenges every day in protecting the security of their information technology (IT) systems and their information. By adopting new technologies, organizations often can perform mission-critical functions and serve their customers more efficiently. But the new technologies that enable organizations to improve their system capabilities and provide better services can also introduce new threats and risks to IT systems.

Active content is a technology that offers great convenience to the users who download files and electronic documents from the Internet. The Web pages that they retrieve are used as electronic counterparts to paper documents. However, the electronic documents that are downloaded are often more than just text. They are programs or they contain programs that can carry out or trigger actions automatically without the user directly or knowingly invoking the actions. Examples of electronic documents with active content are Web pages with digitally encoded multimedia information, such as interactive weather maps, stock ticker information, live camera views, and programmed broadcasts. Loading an encoded document into a word processor can have the same effect as executing a program.

Active content is a form of mobile code -- a program such as a script, macro, or other portable instruction that can move from one platform to another where it is processed. The user is often unaware of the transfer of the code, which can contain malicious code inserted by an attacker. It is generally impractical for organizations to prohibit the use of active content by their staff members, but appropriate controls can be employed to minimize the risks and maintain the appropriate levels of security.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently updated its guidelines on active content to help organizations protect their IT systems and information from the security risks that accompany the use of active content. The revised guidelines discuss the technology, the new security risks introduced, and the recommended secure solutions.

NIST Special Publication (SP) 800-28 Version 2, *Guidelines on Active Content and Mobile Code: Recommendations of the National Institute of Standards and Technology*

NIST SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code: Recommendations of the National Institute of Standards and Technology*, replaces an earlier version of the guidelines which had been issued in 2001. The revised publication, written by Wayne A. Jansen and Karen Scarfone of NIST and by Theodore Winograd of Booz Allen Hamilton, provides updated information about active content and mobile code technologies, and discusses the components of the IT system's browsers and servers that handle active content. One major section of the publication covers the threats associated with the use of active content and mobile code. Threats are possible dangers to a computer system,

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since March 2007:
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*
- *Forensic Techniques for Cell Phones, June 2007*
- *Border Gateway Protocol Security, July 2007*
- *Secure Web Services, August 2007*
- *The Common Vulnerability Scoring System, October 2007*
- *Using Storage Encryption Technologies to Protect End User Devices, November 2007*
- *Securing External Computers and Other Devices Used by Teleworkers, December 2007*
- *Secure Web Servers: Protecting Web Sites that are Accessed by the Public, January 2008*
- *Federal Desktop Core Configuration (FDCC): Improving Security for Windows Desktop Operating Systems, February 2008*
- *Handling Computer Security Incidents: NIST Issues Updated Guidelines, March 2008*

which may result in the interception, alteration, obstruction, destruction, or other disruption of computational resources.

Another principal section discusses the risks to systems that process active content. Risks are a measure of the likelihood and the consequence of events or acts that could cause a system compromise, including the unauthorized disclosure, destruction, removal, modification, or interruption to the availability of system assets. The safeguards that can protect system resources from attacks are covered in detail. Safeguards are approved security measures taken to prevent or reduce the risk of system compromise, and include management, operational, and technical controls.

NIST's recommendations for managing and improving the security of IT systems that process active content are summarized in a section of the guide. NIST SP 800-28 Version 2 includes a list of references for both in-print and online resources that can be consulted for more information on active content and mobile code. The appendices provide a summary of available browser request methods, the categories of server response codes, a glossary of terms, and an explanation of the acronyms used in the publication.

This ITL Bulletin summarizes NIST SP 800-28 Version 2, which is available at http://csrc.nist.gov/publications/nistpubs/800-28-ver2/SP800-28v2.pdf.

Background on Active Content

Active content technologies include built-in macro processing, scripting languages, and virtual machines. The use of these technologies blurs the distinctions between code and data. Examples of active content documents are PDF documents; Web pages conveying or linking to mobile code such as JavaScript, VBScript, Java applets, and ActiveX controls; desktop application files containing macros; Flash and Shockwave media files; and Hypertext Markup Language (HTML)-encoded e-mail bearing executable content or attachments. Web pages with active content can deliver digitally encoded multimedia information or even an interactive experience enabled by embedded computer instructions.

For many people, being able to download files and electronic documents from the Internet is a useful function and a common practice. Users consult Web pages for items such as forms, brochures, magazines, and newspapers that they might previously have used in a paper format. Today, desktop and laptop computers, portable handheld devices, such as cell phones and personal digital assistants (PDAs), and Internet appliances can access the Web.

Users are generating content for display on Web pages. Social networking, photo and video sharing, bookmarking, and knowledge-sharing sites are becoming increasingly popular. Many organizations operate knowledge-sharing Web site sites for both their internal and their external users. These Web sites are more interactive than previous Web pages, allowing users, who could be legitimate or malicious, to modify or add to existing content. This situation challenges organizations to secure their computer systems against potential threats that are associated with user-generated content.

In the past, the flow of information on the Web was from Web sites to the user. Now user-generated content allows information to flow freely in both directions and makes it more difficult for an organization to control what information leaves or enters its networked systems. Both system browsers that allow users to view pages from various sources and the servers that interconnect to the Internet are associated with the processing of active content and mobile code.

In addition, many different components of a system may be involved. For example, each implementation of active content technology may require a different interpreter to be installed as a browser component on the user's computer. This further complicates the security configuration position for organizations because each interpreter may be supplied by a different manufacturer. The installed browser components must be monitored and updated whenever vulnerabilities are discovered. If organizations do not have a centralized configuration management system to track these changes, they may be using systems that have not been patched with new controls. Similarly, new versions of active content implementations may alter how the interpreter presents active content. Patches to active content components may be incompatible with the active content generated by an organization's Web sites. To deal with these complex situations, organizations may have to choose between two potentially costly alternatives: to continue using incompatible and possibly vulnerable browser components, or to update the Web site.

Active content technology provides excellent capabilities to the user, but it also results in vulnerabilities that an attacker could exploit. Many of the problems that organizations experience with malware on their systems may result from active content, which can be the delivery mechanism for mobile code.

Risks and Threats Associated with Active Content

Many computer technologies involve risk. Flaws or weaknesses in the technologies' design, implementation, or configuration can introduce vulnerabilities to a system. Vulnerabilities also result from the absence of security controls or weaknesses of controls, leading to violations of the organization's security policy for a system. While technology-related vulnerabilities are often subtle and do not affect either the overall functionality or performance of a product, they may be discovered and exploited by an attacker. Risk analysis can determine the impact of the vulnerability, depending on factors such as the value of the resource affected or the perceived harm to one's reputation.

Organizations are exposed to technology-based risks because active content and mobile code allow systems to execute code that may not be trustworthy. All software contains defects, and some of these defects may be the source of vulnerabilities that an attacker could exploit. When determining the risks associated with active content, organizations have to consider the capabilities of the software to be implemented and the security controls provided by the environment. In some situations, it may be necessary to utilize an active content technology regardless of the determination of risk. For example, a critical system may require JavaScript or PDF support.

Many threats are a result of security issues that were not addressed when Internet protocols were developed. These problems are exacerbated by the scale of the Internet, the complexity of software, and the prevalence of mobile code. Many Web interactions rely on mobile code, either running on a Web server or Web browser. These interactions are susceptible to the threats associated with mobile code.

Attackers may exploit vulnerabilities in connected hosts, as well as other vulnerabilities existing in an operating system, Web server software, or a Web protocol. Voluntary standards efforts are addressing these issues to reduce the risks involved. Standards for Internet Protocol Security (IPsec), Secure Domain Name Server (DNS), and Public Key Infrastructure (PKI) have been implemented in products. Government-certified security evaluation laboratories have been established under regional and worldwide mutual recognition schemes. Organizations have established incident response teams, which have improved their effectiveness in combating intrusions. Commercial software is available for detecting and eliminating malware, filtering network protocols, patching computer systems, and detecting and preventing intrusions.

By assessing the threats associated with the use of active content and mobile code, organizations can take steps to reduce them. The possibility of attacks, which can impact the confidentiality, integrity, accountability, or availability of IT resources, can then be reduced.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to Hlistproc@nist.govH with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to Hlistproc@nist.govH with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at

NIST'S Recommendations for Managing Active Code

NIST recommends that organizations adopt security policies based on their assessments of security needs and their level of acceptable risks. To mitigate the risks that are specifically associated with the use of active content, organizations should:

Examine the concept of active content and understand how it affects the security of IT systems.

The use of products with capabilities for producing and handling active content contributes to the functionality of a system as a whole and thus is an important factor in IT procurement and implementation decisions. Active content technologies allow code, in the form of a script, macro, or other kind of portable instruction representation, to execute when a document is rendered. Active content technology can be used to deliver essential services, but it can also become a source of vulnerability for exploitation by an attacker.

E-mail and Web pages accessed through the Internet provide efficient ways to convey active content, but they are not the only means. Active content technologies span a broad range of products and services and involve various computational environments, including those of the desktop, workstation, server, and gateway devices. To understand their security ramifications, organizations are encouraged to consult needed technical information that is available from many information resources and to gain a sound understanding of the security implications of active content. NIST SP 800-28 Version 2 contains an extensive reference list of these information sources.

Develop organizational policies regarding the implementation and use of active content.

Information security in any organization is largely dependent on the quality of the security policy and the processes that an organization imposes on itself, including policy awareness and enforcement. As appropriate to their situation, organizations should develop policy for the procurement and use of products involving active content technologies. Active content should only be applied where it specifically benefits the quality of the services delivered and not simply for its ready and easy availability within products. Both the consumption and production of active content should be addressed by the policy. A badly implemented, poorly planned, or nonexistent security policy can have a serious negative security impact. The policy should be stated clearly and consistently, and made known and enforced throughout the organization. Putting an organizational security policy on active content in place is an important first step in applying effective safeguards and mitigating the risks involved.

Assess the specific benefits that are gained from the use of active content, balance the benefits against the associated risks, and select appropriate controls.

Since the use of active content brings both benefits and risks to the organization, it is essential that organizations analyze and manage the risks that are associated with the use of active content, as well as all other threats, on a continuing basis. Organizations should conduct periodic risk analyses to identify the threats to their systems and their systems' vulnerabilities to the threats. They should assess potential attacks and the chances of success, and estimate the potential damage to systems and information that could result from successful attacks. Then organizations can adopt policies and procedures to reduce the risks cost-effectively to an acceptable level and to maintain security throughout the life cycle of the system.

See NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, for details on the risk management process. Security involves continually analyzing and managing risks. A risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses their likelihood of success, and estimates the potential damage from successful attacks. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.

Every organization must take into account its own needs for protecting the ability to carry out its mission and safeguarding assets, its budget, and its culture. As new products are selected and procured, organizations should consider the risk environment, cost-effectiveness, assurance level, and security functional specifications, and then make their decisions. Organizations should also be aware of the interconnectivity and associated interdependence of external as well as internal organizations. A risk may be accepted by one organization, but this acceptance may inadvertently expose other organizations with which the organization interoperates to the same risk. Moreover, since active content is heavily oriented toward rendering information for an individual, the decisions made by an organization may affect the customers who are served by the organization's electronic pages. Once an assessment is made, safeguards can be put in place against those risks deemed significantly high, by either reducing the likelihood of occurrence or minimizing the consequences.

Maintain consistent system-wide security when configuring and integrating products involving active content into system environments.

When they procure new products, organizations should collect and analyze information about the features of those products that can be used to control active content. Products and software applications that handle active content often have built-in controls that can be used to control or prevent activation of related features. E-mail, spreadsheet, word processor, database, presentation graphics, and other desktop software applications have similar configuration settings that can be used to control the security capabilities of active content documents. It is important to examine the configuration settings carefully since many products are delivered with insecure default settings.

Network devices or other special purpose software should be used to supplement existing application-oriented controls. For example, firewalls can be augmented by gateway devices that filter certain types of e-mail attachments and Web content with known malicious code characteristics and that reject them at a point of entry. Desktop anti-malware software has also been developed with increasing capabilities for detecting malicious code signatures within active content. In addition, many active content technologies provide mechanisms for dynamically restraining the behavior of mobile code by quarantining it within a logical sandbox. Organizations should become familiar with available security options and use them in accordance with their organizational policies.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. See NIST's Web page for information about NIST standards and guidelines that are referenced in the *Guidelines on Active Content and Mobile Code*, and other security-related publications, covering related topics, such as security planning, risk management procedures, security controls, intrusion detection systems, incident handling, and firewalls. See http://csrc.nist.gov/publications/index.html

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.