THREATS IN JAVA APPLET

Ankit Bhatt
Dronacharya College of Engineering

***Abstract*— The advantages brought about by the use of Java in network management answer some critical problems existing in an Applet. Java applets is a piece of software designed to be executed in a user's browser by a Java virtual machine. Applets are embedded into web pages. They are automati- cally loaded and executed if the browser has a Java plugin installed (once the page has loaded), and graphical content is appropriately displayed by the browser. But it may contain some harmful content that affect the user privacy and security.**

***Index Terms*—Applet, GUI, hosts, JVM, malicious, packages, security.**

INTRODUCTION

From its beginning, Internet has experienced a huge increase in the number of users, services and data transferred. Different Internet access characteristics lead to very diverse levels of Quality of Service, which can have a great impact on service performance. The explosion in the size and complexity of today's local and wide area networks, combined with the increasing demands placed upon them for their resources has resulted in establishing Network Management as a factor of paramount importance. To further complicate matters, the concept of a single vendor network has vanished into history. Even if a company's network is provided by a single vendor, very soon the requirement to interconnect with related companies by using a mixture of public and/or private networks make the single vendor objective unrealistic. Therefore, an important goal of network management is to support the heterogeneous integrated environment of a network that contains multi-vendor hosts, software packages and carriers. Java was chosen as the baseline programming language for this project. The entire GUI (Graphical User Interface) for this system has been designed using the Java SWING packages. Java is the language of the internet. In addition to the programming language itself, Java has a rich library that makes it possible to write portable programs that are operating system independent. Java also has a rich set of security features that help in learning the language faster.

THREATS IN JAVA APPLET

The java virtual machine can catch many kinds of mistakes and report them accurately. Instead of producing executable code, a Java compiler produces byte code. The Java run-time system is an interpreter for byte code. Once the Java run-time package exists for a given system, the byte code version of any Java program can run on it. Therefore, Java produces truly portable programs.The combination of the World Wide Web and Java increases the prominence of Internet in information systems planning and implementation. The World Wide Web makes tremendous amounts of information available to anyone with a web browser. Applets are java programs that can be embedded in HTML documents and can run inside a web browser. The applet code resides on the web server and gets downloaded in the browser whenever the web page containing the applet is requested by the browser. This project is part of an ongoing effort to create a Java Applet that acts as an interface for creation and management of an SQL compliant database over a network. The intuition behind this is that since Java Applets can run inside a web browser, it will be possible to use this interface for creating and managing databases remotely over a network. Malicious content is a major attack vector on the Internet. Typically, the attacker's goal is to install and run a piece of malware on the victim's computer, turning it into a member of a botnet. To this end, attackers try to lure users onto malicious web pages that contain malicious code. This code might trick the victim into downloading and running a malware program (through social engineering). Alternatively, the malicious code might try to exploit a vulnerable part of the victim's browser, such as an ActiveX control, the JavaScript engine, or the Java plugin. Attacks that exploit (browser or plugin) vulnerabilities when users visit malicious web pages are called drive-by download attacks. Applets that are digitally signed with a certificate (that is, certificates trusted by the user) run effectively outside the sandbox. In such cases, the previously-described restrictions do not apply. The browser, encountering an applet with a signature, will usually display a dialog window asking the user if he trusts the applet's certificate or not. If the user accepts the certificate, the applet runs with full privileges, otherwise, it is sandboxed. An applet that is started from JavaScript remains always sandboxed. Malicious applets try to escape the sandbox and install malware on a victim's computer. To achieve this, some ap- plets try to trick careless users into trusting their certificates. Others target the JVM itself by trying to exploit a vulnerability in the Java plugin, effectively disabling the sandbox and turning the applet into a full-fledged, non- restricted program with permissions equal to that of the user running the browser.

REFERENCES

[1] David M. Geary (1999). Graphic Java 2, Volume II: Swing. Upper Saddle River, New Jersey: Prentice Hall

[2] Peter J. Hall, Security and threats in Java

[3] Dr. R Nageswar Rao, Core Java an integrated approach

[4] Dr. Phil W. Johnes, Applets in Java