In Internet-Based Visualization System Study about Breakthrough Applet Security Restrictions

Jie Chen, Yan Huang

IN INTERNET-BASED VISUALIZATION SYSTEM STUDY ABOUT BREAKTHROUGH APPLET SECURITY RESTRICTIONS

Jie Chen [1,*], Yan Huang [1]
1 China Agricultural University College of Information and Electrical Engineering

Abstract: In the process of realization Internet-based visualization system of the protein molecules, system needs to allow users to use the system to observe the molecular structure of the local computer, that is, customers can generate the three-dimensional graphics from PDB file on the client computer. This requires Applet access to local file, related to the Applet security restrictions question. In this paper include two realization methods: 1.Use such as signature tools, key management tools and Policy Editor tools provided by the JDK to digital signature and authentication for Java Applet, breakthrough certain security restrictions in the browser. 2. Through the use of Servlet agent implement indirect access data methods, breakthrough the traditional Java Virtual Machine sandbox model restriction of Applet ability. The two ways can break through the Applet's security restrictions, but each has its own strengths.

Key words: e-government, knowledge management, frameworks, e-governance

1. INTRODUCTION

In network applications development, because of Java language have cross-platform, the program simple, suitable for network transmission, etc(Zhou Hang et at., 1997), applications prepared by Java is increasing. In many applications need to use Java Applet procedures to operate the client resources, but by default, even if the client to confirm the java procedure is "reliable", the browser will refuse the web Java program to operate client resources(William Stallings et at., 2001). We can through the following two

methods to achieve this functionality: 1.Applet through Servlet agent indirect access to the database: in the Applet, we can use the url to establish a connection with the Servlet, and then through the Servlet access to the database client database and the results return to Applet, Indirectly through this process to achieve the Applet access to the client database. 2. Through the digital signature break the JVM sandbox, in java we can through increase the signature of Applet package to achieve Applet access to the client database.

2. CONCRETE REALIZATION OF APPLET AND SERVLET COMMUNICATION

The communication process include the following two aspects: achieve Applet Access to the Servlet and the transmission parameters and realization of transfer the data from Servlet to Applet.

2.1 Achieve Applet Access to the Servlet and the transmission parameters

2.1.1 Create a URL object

In JAVA Procedures, you can use the following method to create URL object:

URL servletURL=new URL (http://localhost:
8080/servlet/dbServlet.DbServlet).

2.1.2 Establish a connection with the URL address

After the successful creation of a URL object, you can type in the URL call openConnection () function to establish a connection. openConnection () function in the establishment of connections at the same time, to communicate the work of connection initialization:

URLConneCtion servletConnection=servletURL_()pen Connection();

2.1.3 Use URLConnection object to read and write operation

2.1.3.1 Using URLConneCtion object read the information that return from Servlet

After get URLConnection object, if the Servlet sent JAVA object to Applet, you can use URLConnection object openStream () methods to obtain input stream, and then generate a new ObjectInputStream object, use object ObjectInputStream readObject () method can get the JAVA object that Servlet returned.

If the Servlet sent Plain text to the, you can use URLConnection object getInputStream () method to obtain input stream, and then generate a new DataInputStream object, use the DataInputStream object readLine () method to obtain text that Servlet returned.

2.1.3.2 Using URLConnection objects delivery the value to the Servlet

Applet sent the parameters to Servlet through the following two methods to achieve:

Through URL addresses add parameters GET method to achieve transmission parameters :

Another method is to obtain the output stream connection from the URLConnection, the output stream to be connected to the standard input stream which belong to the Common Gateway process (server-side), and then write relevant data into the output stream, when the transmission is over ,close the output stream.

2.2 Realization of transfer the data from Servlet to Applet

Servlet request object's getParameter method can get the parameters that transmission from Applet:

String sql= request.getParameter(" sql");

the output stream Servlet that Servlet request object's getOutputStream () method get generate a new output stream, and then through the object's writeObject () method output JAVA type of object:

```
Class.forName( "sun:jdbc}:odbcdriver");
Connection  conn=DriverManager.getConnection(connectionString);
Statement st=conn.createStatement()
ResultSet rs=st.execute(sql)
dbStream= new ObjectOutputStream( response.getOut-putStream())；
／／Write the object...
dbStream.writeObject(rs);
```

Through the request's getWriter () method PrintWriter types of output, this object println () method can be output from the Servlet to Applet text:

```
PrintWriter out= response.getWriter0;
out.println(" <head> <title> DataCenter</title> </head>");
```

3. APPLET'S DIGITAL SIGNATURE AND CLIENT AUTHENTICATION

Java security guarantee by the following three aspects:

1, Language features (including border checks of array, type conversion, pointer-type variables).

2, Control Resource Access (including access the local file system, socket to connect and visit).

3, Code digital signature (digital signature to verify the source code and the code is complete).

This article discusses the combination of two technologies to achieve beyond the Applet security restrictions.

When a class file of the Applet is loading the JVM by the default class loader, JVM immediately loading a called for security manager (Security Manager) Class's sub-class Applet Security for it, by the manager to verify the operation. all the action of Code (such as file reading and writing) must be verified by the Security Manager, only be accepted the action can be completed, otherwise Security Exception will be thrown out Exception. Security Manager Class uses the Policy document to determine the code authority.

After JDK1.1, the JDK improved the division of permissions, the introduction of Permission Set concept. It designated the permissions detailed in every aspects, you can have a combination of selective permissions you need to meet special requirements. Figure 1 shows such a division:

Basic Permission in Figure 1 can be further broken down into more details of permissions, such as: AWT Permission, Runtime Permission and so on.

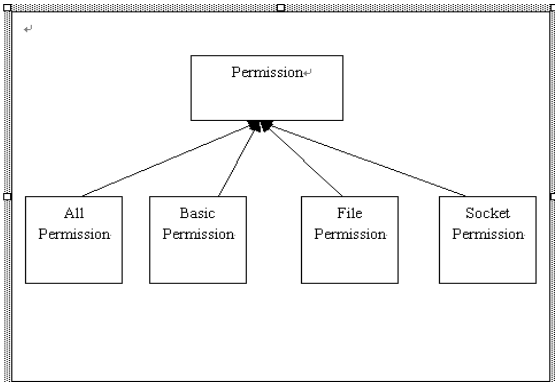

Fig.1 The division of Java security permissions

Java through a name suffix. Policy documents combination of these permissions. After The installation of JRE (Java Runtime Environment) there are two default permissions files, they are:

${java.home}/lib/security/java.policy

${user.home}/.java.policy

we have to create a policy document for the Applet, use the policy document the Applet will have the permission to read all the local documents .Only a policy document is not enough, the customer can not determine whether the executed code is your, there is no guarantee that the code in the course of transmission have not been malicious damaged. Therefore, digital signature technology needed to ensure these two aspects.

The realization of the system, we must first generate a key database, then we must have a certificate that be used when signature, finally, we use the generated certificate signature the Applet's jar files (Harvey M.Deitel et al.,2003).This completes digital signature the Applet. Digital signature technology to ensure the executed code is released by you and have not been malicious damaged.

4. CONCLUSION

Through the above analysis, the first method through the Servlet to achieve access client database, Servlet and Applet communication provides a language-level facilitate that the transmission of JAVA objects with each other, the second method use JDK tools digital signatures for Java Applet Program that do not have to modify existing Program, this is a practical, simple and reliable method.

ACKNOWLEDGEMENTS

This study was supported by the national 863 projects: Biological veterinary drug new product research and creation (2006AA10A208). The author would also like to thank Yan Huang, for her contribution to the project.

REFERENCES

Zhou Hang ,Cai WenSheng. JAVA Language Programming. Beijing: Publishing House of Electronics Industry,1997.10

William Stallings. Encryption and network security: Principles and Practice.[M]- Beijing: Publishing House of Electronics Industry,2001

Harvey M.Deitel,Paul J.Deitel,Seam E. Santry.Advanced Java 2 Platform How to Program[M] - Beijing: Publishing House of Electronics Industry,2003