УДК 004.7+65.428

ДОСЛІДЖЕННЯ ЗАХИСТУ JAVA ТЕХНОЛОГІЇ У ВЕБ-БРАУЗЕРАХ

Гнініашвілі Т. З., Баранов А.А.
Державний ВНЗ «Національний гірничий університет», nmu.org.ua, g_tanya@ua.fm

У даній статті досліджено методи захисту Java технології у веб-браузерах та ворожі Java-аплети, описані їх принцип дії та можливі загрози. Запропоновані можливі шляхи вирішення зазначених проблем.

Ключові слова – веб-браузер, Java, аплет, захист.

ВСТУП

Аплети використовуються для надання динамічного характеру Web-документа. Класичним прикладом використання java-аплетів є надання статичним картинкам певних ефектів (падаючого снігу, руху хвиль по поверхні води і т.п.), а також різні способи анімації динамічно задаються текстових написів. Інші мови компілюються в об'єктний код для конкретної операційної системи і процесора. Тому, наприклад, скомпільована для Windows програма не може працювати на Macintosh. На відміну від них, Java не залежить від платформи, оскільки він створює проміжний код (bytecode - байт-код, який не залежить від конкретного процесора. Віртуальна машина Java (JVM - Java Virtual Machine) потім конвертує байт-код в машинний код, який розуміє процесор на даній конкретній системі.

ПРОЦЕС СТВОРЕННЯ І ВИКОНАННЯ JAVA-АПЛЕТІВ

1. Програміст створює java-аплет і виконує його компіляцію.
2. Компілятор Java перетворює вихідний код у байт-індекс (не залежить від конкретного процесора).
3. Користувач завантажує java-аплет.
4. JVM конвертує байт-код в машинний код (для відповідного процесора, встановленого на комп'ютері користувача).
5. Аплет запускається при зверненні до нього.

Для запуску аплету, JVM створює віртуальну машину в рамках користувача середовища, звану пісочницею (sandbox). Ця віртуальна машина є замкнутою середовищем, в якій аплет виконує свої дії. Аплети зазвичай відправляються по запитам від веб-сторінок, тому аплет виконується відразу, як тільки він приходить. Такий аплет може виконувати шкідливу діяльність навмисно або випадково, якщо розробник аплету зробив щось неправильно. Тому пісочниця строго обмежує доступ аплету до будь-яких системних ресурсів. JVM є посередником між аплетом і ресурсами системи, перехоплюючи, перевіряючи і виконуючи запити аплету до системних ресурсів і залишаючи при цьому сам аплет всередині пісочниці.

ЗАХИСТ JAVA-ТЕХНОЛОГІЇ

Найбільш уразливими з точки зору безпеки компонентом Java-технології є аплети, оскільки їх може використовувати будь-який клієнт, який зовсім не зобов'язаний знати правила "техніки безпеки при роботі з цими невеликими програмами. Саме тому аплетів для передбачені самі жорсткі методи захисту. Хоча різні браузери та програми перегляду аплетів можуть по-різному захищати інформацію користувача від нападу, але в загальному випадку аплету має бути заборонено наступне:

– читати, змінювати, видаляти і перейменовувати локальні файли;
– створювати локальні директорії і читати їх вміст;
– перевіряти існування і параметри певного файлу;
– здійснювати доступ по мережі до віддаленого комп'ютера;
– отримувати список мережевих сеансів зв'язку, які встановлює локальний комп'ютер з іншими комп'ютерами;
– відкривати нові вікна без повідомлення користувача (це необхідно для запобігання "емуляції" аплет інших програм);
– отримувати відомості про користувача або його домашньої директорії;
– визначати свої системні змінні;
– запускати локальні програми;
– виходити з інтерпретатора Java;
– завантажувати локальні бібліотеки;
– створювати потоки, які не перераховані в ThreadGroup (клас, керуючий виконанням потоків різних частин програми) цього аплету, і керувати ними;
– отримувати доступ до ThreadGroup іншого аплету;
– визначати свої об'єкти Class-Loader (Завантажувач Java-об'єктів) і SecurityManager (Диспетчер безпеки для аплетів);
– переобозначать системні об'єкти ContentHandlerFactory, SocketImplFactory і URLStreamHandler-Factory (ці класи управляють мережевий роботою Java);
– отримувати доступ до будь-якої упаковці, що відрізняється від стандартних;
– визначати класи, які входять до локальну упаковку.

Ці правила забезпечують наступні компоненти Java-технології:

– віртуальний Java-процесор, який постійно контролює свій стан;

– завантажувач аплетів і Java-програм, який контролює завантажувані коди;

– диспетчер безпеки (SecurityManager), контролює і блокуючий небезпечні дії аплетів.

У класі SecurityManager перелічені методи, які використовуються системою для контролю дій аплету в залежності від характеристик навколишнього середовища. Програма, яка застосовується для перегляду аплету, створює підклас SecurityManager, який і реалізує необхідну політику безпеки. Посилання на цей SecurityManager записується в об'єкті System.

Ще один механізм безпеки вбудований в завантажувач аплетів і програм (ClassLoader). Браузер перевизначають цей клас і реалізує свої власні правила роботи з мережевими протоколами. Одна з основних функцій завантажувача об'єктів – розділення простору імен різних аплетів і операційної системи, що дозволяє уникнути їх взаємного впливу.

Інша, не менш важлива функція завантажувача – верифікація байт-кодів, тобто перевірка правильності отриманого елемента Java-програми і його цілісності. У процесі верифікації з'ясовується наступне:

– чи відповідає версія отриманого блоку версіями інших елементів системи;

– збережений чи формат байт виконуваного-коду;

– чи відповідає програма специфікації конкретного віртуального Java-процесора;

– чи може виникнути переповнення або вичерпання стеку;

– чи всі регістри Java-процесора використовуються правильно;

– чи немає некоректних перетворень типів.

Метою такої перевірки є виявлення неправильного використання непрямої адресації, яке може призвести до порушення в роботі віртуального процесора, і перевірка цілісності аплету. Цей механізм забезпечує захист і надійну роботу розподіленої програми, що дозволяє не завантажувати в браузер всю Java-програму цілком, а довантажувати її невеликими блоками по мірі необхідності.

Сам віртуальний Java-процесор також має вбудовані механізми захисту від нападу. Наприклад, оскільки байт-коди Java інтерпретуються, то можна контролювати індекси масивів, що дозволяє уникнути переповнення буфера – найпоширенішою і небезпечною помилки. Вбудовані прилади обробки виняткових ситуацій дозволяють ефективно вирішувати конфлікти, а "збирач сміття", який очищає невикористану пам'ять, не дає можливості "нападаючому" переглянути "відходи", які містять корисну інформацію.

Найбільш уразливими з точки зору безпеки компонентом Java-технології є аплети, оскільки їх може використовувати будь-який клієнт, який зовсім не зобов'язаний знати правила "техніки безпеки при роботі з цими невеликими програмами. Саме тому аплетів для передбачені самі жорсткі методи захисту.

ВИСНОВКИ

Підводячи підсумок, можна констатувати, що в міру зростання масштабів використання мобільних кодів все більше уваги приділятиметься атакам на основі зловмисних java-аплетів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Глушаков С. В., Бабенко М. И., Тесленко Н. С. Секреты хакера. Атака и защита. Учебный курс. – АСТ Москва, 2008. – 544 с.: ил.

2. Гаевский А. Ю., Романовский В. А. Создание Web-страниц и Web-сайтов. HTML и JavaScript – СПб., БХВ-Петербург – 2008. – 427 с.: ил.

3. Java (Електроний ресурс) Спосіб доступу: URL http://ru.wikipedia.org/wiki/Java /.– Загол. з екрана;