

## From Branon Martindale

- The presidents of the National Academies said yesterday that the Bush administration was going too far in limiting publication of some scientific research out of concern that it could aid terrorists.
- Specifically, they said, the administration's policy of restricting the publication of federally financed research it deemed "sensitive but unclassified" threatened to "stifle scientific creativity and to weaken national security."
- The category of "sensitive but unclassified" was poorly defined, the presidents said in a "Statement on Science and Security in an Age of Terrorism."
- "Experience shows that vague criteria of this kind generate deep uncertainties among both scientists and officials responsible for enforcing regulations," the statement said.
- Indeed, the policy, experts said, had already resulted in the administration's withdrawing of thousands of reports and papers from the public domain.



COMP 6370 – Web Security II – Lecture 12



## Sensitive But Unclassified

- 9/11
- Combat Operations
  - Afghanistan
  - Philippines
  - Balkans
  - Future Operations in Southwest Asia
- Continued Computer Security Issues
- SBU
  - Unclassified
  - No criminal sanctions for disclosure
    - exception: information covered by Privacy Act, other legislation or court order



COMP 6370 – Web Security II – Lecture 12



## Cookies

- Where web servers store information about their customers
  - searching large customer databases on server costly
- HTTP requests do NOT automatically identify individual users
  - Thus easier to use a cooperating browsers' customer side
  - Server requests browser to store a cookie that contains information the server will use the next time the client calls
    - .netscape/cookies
- Cookies give browsers the chance to create stateful HTTP sessions
- Privacy
  - cookies stored by the browser create client profiles



COMP 6370 – Web Security II – Lecture 12



## Language Design Decisions (Java)

- The language itself should make it more difficult for programs to create damage.
- The execution environment provides mechanisms for access control
- The security policies enforced by the execution environment have to be set correctly



COMP 6370 – Web Security II – Lecture 12



## Java Review: Applets vs. Applications

From: *Java in a Nutshell – Flanagan*

- "A program in Java consists of one or more class definitions, each of which has been compiled into its own .class file of Java Virtual Machine object code."
  - One of these classes must define a method main(), which is where the program starts running.
  - To invoke a Java program you run the Java interpreter, java, and specify the name of the class that contains the main() method.
- A Java applet is NOT an application – it is a Java class that is loaded and run by an already running Java application such as a web browser or an applet viewer.
- Note: Ada 95 has this capability – i.e. "Adapplets."



COMP 6370 – Web Security II – Lecture 12



## Security for Executable Java Applets (Objectives)

- Applets do not get access to the user's file system
- Applets cannot obtain information about the user's name, email address, machine configuration, etc.
- Applets may make outward connections only back to the server they came from
- Applets can only pop-up windows that are marked "untrusted"
- Applets cannot reconfigure the system, e.g. by creating a new class loader or a new security manager



COMP 6370 – Web Security II – Lecture 12



## Applications versus Applets

- An applet loaded across the network it is not allowed to:
  - read/write/delete files on the client file system
    - no use of File.delete() method or sys calls rm or del
  - rename files on the client file system
    - no use of File.renameTo() or mv or rename commands
  - conduct directory operations
    - content listing
    - check for existence of a file
    - obtain file information – size, type and modification time stamp
  - conduct network operations
    - create a network connection to any computer other than the host from which it originated
    - listen for or accept network connections on any port in the client system
    - specify any network control functions – SocketImplFactory, etc.....
  - read or define any system properties
  - run or exit any program
    - no use of Runtime.exec(), System.exit() or Runtime.exit() methods
  - load dlls on the client system using load() or loadLibrary()
  - thread creation or manipulation
  - create a new ClassLoader or SecurityManager
  - define classes that are part of packages on the client system



COMP 6370 – Web Security II – Lecture 12



7

## Environment for Applets

- Users cannot rely on prior acquaintance and trust relationship with the source of an applet
- Few users are willing to rule personally on each access request made by an applet
- Client's operating system cannot be expected to offer any protection

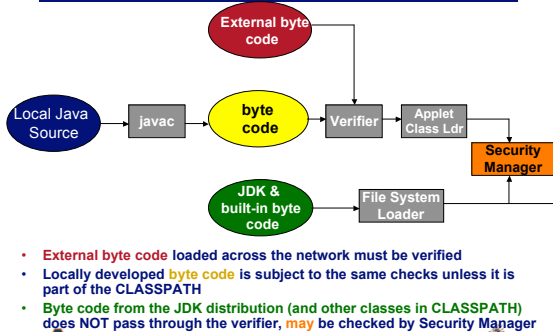


COMP 6370 – Web Security II – Lecture 12



8

## Three roads for Java byte code



- External byte code loaded across the network must be verified
- Locally developed byte code is subject to the same checks unless it is part of the CLASSPATH
- Byte code from the JDK distribution (and other classes in CLASSPATH) does NOT pass through the verifier, may be checked by Security Manager



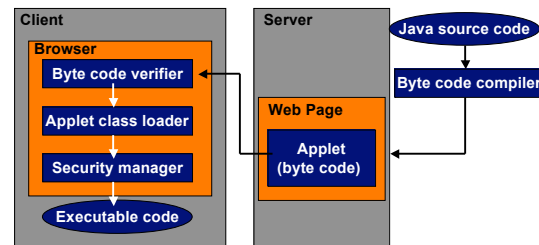
COMP 6370 – Web Security II – Lecture 12



9

## Java Sandbox

- Executable Content (applets) from remote web sites



COMP 6370 – Web Security II – Lecture 12



10

## Byte Code Verifier

- Checks for:
  - the class file is in the proper format
  - stacks will not overflow
  - all operands have the correct type
  - there will be no data conversion between types
  - all references to other classes are legal
- Byte code verifier reduces the workload on the interpreter
  - guaranteed code properties do not have to be checked again
- However, security still depends on the run-time environment

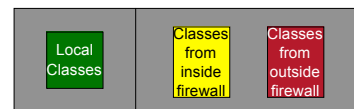


COMP 6370 – Web Security II – Lecture 12



11

## Class Loader in a Dynamic Environment



- The Java environment has classes arriving and departing dynamically
- The class loader divides classes that it loads into several distinct name spaces according to where the classes came from
- Local classes are kept distinct from classes loaded from other machines
- Furthermore, these outside classes are protected from each other.



COMP 6370 – Web Security II – Lecture 12



12

## Applet Class Loader

- Class loader protects the integrity of the run-time environment
- Applets must not be allowed to create their own class loaders
  - Applets are handled by the applet class loader
- Java comes with its own class library
  - The CLASSPATH environment variable specifies the location of built-in classes
  - The security issues associated with altering CLASSPATH should be obvious
- “Spoofing” of the CLASSPATH can be avoided by:
  - If the applet class loader first searches the built-in classes in the local name space
  - Then expand search to the class making the request



COMP 6370 – Web Security II – Lecture 12



13

## Security Manager

- Reference Monitor of the Java Security Model
  - Performs run-time checks on ‘dangerous’ methods
- Java classes are grouped into packages
  - packages facilitate rudimentary access control to classes
- Variables and methods can be declared as follows:
  - Private: only the class creating the variable or method has access
  - Protected: only the class creating the variable or method and its subclasses have access
  - Public: all classes have access
  - None of the above: only classes within the same package have access



COMP 6370 – Web Security II – Lecture 12



14

## Security Manager Functions

- Prevent installation of new Class Loaders.
  - The Class Loader’s job is to keep the name spaces properly organized.
  - Because things like file I/O permission will depend on whether or not a class is local, the Class Loader has an important job.
    - Must not be subject to spoofing
- Protecting threads and thread groups
  - Not fully functional....
- Controlling the creation of OS programs
- Controlling access to OS processes
- Controlling file system operations such as read & write
  - access to local files strictly controlled
- Controlling socket operations such as connect and accept
- Controlling access to Java packages (or groups of classes)



COMP 6370 – Web Security II – Lecture 12



15

## Some Compromises of the “Sandbox”

- MSIE Cache Exploit
  - <http://www.alcrypto.co.uk/java/>
- Advanced Type Systems in Computing
  - <http://www.cs.nps.navy.mil/research/languages/>
- Mark LaDue’s “Public Enemy”
  - <http://www.cigitalabs.com/resources/hostile-applets/>
- Others I chose not to experiment with:
  - diskhog.java
  - triplethreat.java
  - mutator.java



COMP 6370 – Web Security II – Lecture 12



16

## Microsoft Internet Explorer - "Where do you want (your data) to go today?"

- The object of the exercise here is to open a connection to a port on the local machine, and provide a two-way pipe back to a remote machine on the Internet.
  - This is achieved by using the Java net.socket class to talk to the local machine, and the showDocument() thingy for the remote.
  - This exploit relies on the fact that Java behaves differently when loaded across the net, to a load from local hard disk.
  - When loaded across the net, the applet is not allowed to open a network socket to anything other than the server that delivered it in the first place
    - (see <http://www.javasoft.com/sfaq/#socket> for details).
  - This is enforced by the centralized security manager class. However, if the applet is loaded from local disk, this limitation is relaxed, allowing a socket to be opened on the browsing machine.



COMP 6370 – Web Security II – Lecture 12



17

## Type Systems for Secure Remote Evaluation

- The project aims to improve our understanding of the role of type systems in programming languages.
  - Type systems provide a very elegant separation of concerns.
  - Static analyses are typically much easier to reason about when captured by a logical framework such as a type system.
  - Implementations of the analyses are separate algorithmic issues that have their own soundness and completeness proof obligations.
  - This project is concerned with developing new type systems and techniques for formal proofs of semantic soundness, algorithmic issues, and computational lower bounds for these systems.
- This effort aims to identify the rudiments of a provably-secure programming language.
  - It requires formulation of appropriate security and safety properties so that one can prove with respect to a formal semantics that every well-typed program cannot violate these properties.
  - For example, it would be nice to prove that every well-typed Java Applet when executed by Netscape does not cause Netscape to crash. Clearly, there isn’t such a proof as evidenced by enabling Java in them and [clicking here](#) to run a tiny (killerApp)let.



COMP 6370 – Web Security II – Lecture 12



18

## PublicEnemy.java by Mark LaDue

This Java application directly attacks Java class files. Given a target directory, it searches that directory and all subdirectories for Java class files. Once a class file is located, PublicEnemy alters the contents of its "access\_flags" for the class, its fields, and its methods. The results are the following:

1. The class becomes public.
2. Any "static" or "volatile" fields remain as such; "final" fields become "non-final"; "transient" fields become "non-transient;" and "private" or "protected" fields become "public," while "public" fields remain so.
3. Any "abstract," "native," "synchronized," or "static" methods remain as such; "final" methods become "non-final;" and "private" or "protected" methods become "public," while "public" methods remain so.

This should open the class to the maximum amount of inspection and abuse without directly affecting its ability to run. Note that the size of the resulting class is the same as the original. The ability to modify Java class files on the fly is just the skill that a Java Platform Virus will require. The fact that it's this easy bodes ill....



## Summation of Web Threats

	Threats	Consequences	Countermeasures
<b>Integrity</b>	<ul style="list-style-type: none"> <li>•Modification of user data</li> <li>•Trojan horse browser</li> <li>•Modification of memory</li> <li>•Modification of message traffic in transit</li> </ul>	<ul style="list-style-type: none"> <li>•Loss of Information</li> <li>•Compromise of machine</li> <li>•Vulnerability to all other threats</li> </ul>	<ul style="list-style-type: none"> <li>•Cryptographic checksums</li> </ul>
<b>Confidentiality</b>	<ul style="list-style-type: none"> <li>•Eavesdropping on the Net</li> <li>•Info theft from server</li> <li>•Info theft from client</li> <li>•Info about network configuration</li> <li>•Info about which clients talk to server</li> </ul>	<ul style="list-style-type: none"> <li>•Loss of Information</li> <li>•Loss of Privacy</li> </ul>	<ul style="list-style-type: none"> <li>•Encryption,</li> <li>•Web Proxy</li> </ul>
<b>Denial of Service</b>	<ul style="list-style-type: none"> <li>•Killing of user threads</li> <li>•Flooding machine with bogus threats</li> <li>•Filling up disk or memory</li> <li>•Isolating machines by DNS attack</li> </ul>	<ul style="list-style-type: none"> <li>•Disruptive</li> <li>•Annoying</li> <li>•Prevent user from getting work done</li> </ul>	<ul style="list-style-type: none"> <li>•Difficult to prevent</li> </ul>
<b>Authentication</b>	<ul style="list-style-type: none"> <li>•Impersonation of legitimate users</li> <li>•Data Forgery</li> </ul>	<ul style="list-style-type: none"> <li>•Misrepresentation of user</li> <li>•Belief that false information is valid</li> </ul>	<ul style="list-style-type: none"> <li>•Cryptographic techniques</li> </ul>



## Static versus Dynamic Type Checking

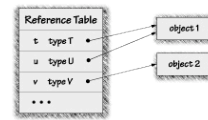
- Java has no dynamic memory allocation
  - does not allow you to cast object or array references into integers or vice-versa
  - does not allow "pointer arithmetic"
  - does not allow you to compute the size in bytes of any primitive type or object
- Dynamic type checking is inefficient
  - to improve performance, Java uses static type checking
    - faster, but less secure than say, Ada
- In a type-confusion attack, a malicious applet creates two pointers to the same object-with incompatible type tags.
  - When this happens, the Java system is in trouble.
  - The applet can write into that memory address through one pointer, and read it through another pointer.
  - The result is that the applet can bypass the typing rules of Java, completely undermining its security.



## Type Confusion Attack Example

- The applet has two pointers to the same memory: one pointer tagged with type T and one tagged with type U. Suppose that T and U are defined like this:

```
class T {
    SecurityManager x;
}
class U {
    MyObject y;
}
```



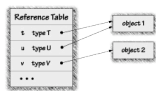
- Now the applet can run code like this:

```
T t = the pointer tagged T;
U u = the pointer tagged U;
t.x = System.getSecurity(); // the Security Manager
MyObject m = u.x;
```



## Exploit Results

- The result is that the object ends up with a pointer, tagged as having type MyObject, to the memory representing Java's Security Manager object.
- By changing the fields of m, the applet can then change the Security Manager, even though the Security Manager's fields have been declared private.
- While this example showed how type confusion can be used to corrupt the Security Manager, the tactic may be exploited to corrupt virtually any part of the running Java system.



<http://www.securingsjava.com/chapter-five/chapter-five-7.html>



## Conclusion

- Fundamental engineering tradeoff:
  - Functionality versus Security
  - Always an inverse relationship
  - Evident in many aspects of security

