Security in Java Byte-code

Dr. KR Chowdhary,Professor
Dept. of CSE,
MBM Engg. College, Jodhpur

-web browser may not be secure for untrusted applet code

- applet code may try to observe, alter, use information it is not authorized

- may cause unauthorized information flow

Java Security

-VM verifies byte code for consistency, prior to execution

-verifier checks: type correctness, stack over/under flow, registers and object initialization

-java security manager assigns access privileges to code and provide sand box in which byte code runs

Java Security..

-Standard java security model may be some times too restrictive

-disallows unrestricted code to perform every operation and

-allows trusted code to perform every operation

-this requires a security policy

-for example, multiple levels of security

read, write O1

⇑

read, write O2

O1 has security level > O2

Java Security flaw

-O2.write(o1.read())
-if (O1.read() == 0) then O2.write(1)
else O2.write(0)

This shows in first explicit write into O2, and in second - implicit write into O2. Information from O1 -> O2.