Security issues surrounding the Java programming language

S. Gritzalis

J. Iliadis

V. Oikonomou

- Department of Informatics, Technological Educational Institute of Athens

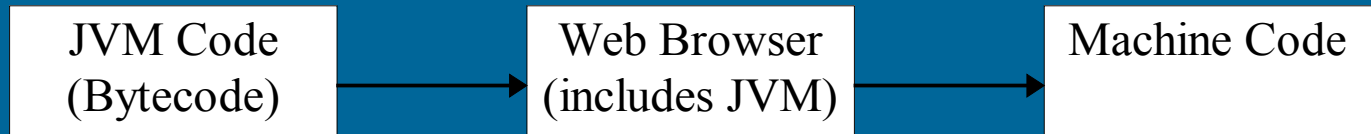- Department of Informatics, University of Athens

- Department of Information & Communication Systems, Research Unit, University of the Aegean

Java overview

- Java Virtual Machine -> portability
- Compilation

JAVA program source file	→	Compiler (Software)	→	JVM Code (Bytecode)

- Execution

JVM Code (Bytecode)	→	Web Browser (includes JVM)	→	Machine Code

Security Issues

- Mobile code use arises security concerns

- Hostile applets
  - attack the *Integrity* of the system
  - violate the *Privacy* of the user
  - limit the *Availability* of system resources
  - achieve user's *Annoyance*

Java Security

- JVM
  - applet classloader
  - bytecode verifier
  - security manager

- JDK 1.2
  - security policy
  - access permissions
  - protection domains

Java Security - Extensions

- User authentication
- Policy enforcement methods
  - capabilities
  - extended stack introspection
  - namespace management
- Secure Code Distribution
- Confining the use of Java in a network domain
- Digital Signatures

Proposed Security Enhanements

- configurable audit system
- facing degradation of service
- "authorisation fatigue" -> modification of security-related user interface

Conclusions

- integrated security scheme
  - new JDK1.2 features
  - SSL, RMI/SSL
  - need for a TTP infrastructure
  - expandability
- "…the only good locks are open, public and accessible ones"