Information Security and Java Cryptography

Ray Kresman

Department of Computer Science
Bowling Green State University
Bowling Green OH 43403

Java is becoming the preferred language of choice for both stand-alone and web enabled applications. However, aspects of Java Cryptography are less well understood. Java Cryptography has relevance in network security, and in the design and deployment of real-life secure Java application by software developers. For example, the Java Cryptographic Extension (JCE) promises plug-in cryptographic libraries and seamless addition of a number of security components and services such as message digests, digital signatures, random number generators and algorithms for symmetric and public key cryptography. This talk provides an overview of network security and Java cryptographic library features. We will describe some of the cryptographic mechanisms, and their use in Java.

This talk is of an introductory nature and is geared for computer professionals, students, and software developers who want to understand security mechanisms. Proficiency in object-oriented concepts in Java and/or C++ programming languages. Exposure to security concepts such as digests, encryption and certificates, while a plus, is not necessary.