Internet and Intranet Protocols and Applications

Lecture 9b:
How Java Supports SSL
March, 2004
Arthur Goldberg
Computer Science Department
New York University
artg@cs.nyu.edu
How Java Supports SSL

• Implementation: Java™ Secure Socket Extension (JSSE)
• For the Java™ 2 SDK, Standard Edition, v 1.4.2
• Supports SSL 3.0 and TLS 1.0
• JSSE Standard API
  – In the javax.net, javax.net.ssl and javax.security.cert packages
Java SSL Class Dependencies

Key Material
  - KeyManagerFactory
  - MyCM
  - KeyManager

Key Material
  - MyTM
  - TrustManagerFactory
  - TrustManager
  - SecureRandom

SSLContext
  - SSLServerSocketFactory
  - SSLSession

SSLServerSocketFactory
  - SSLServerSocket
    - accept()
SSL Socket and SSL Server Socket Classes

• `javax.net.ssl.SSLSocket`
  – Subclass of `java.net.Socket`
  – Supports all of the standard socket methods
  – An instance encapsulates the SSL Context under which it was created

• `javax.net.ssl.SSLServerSocket`
  – Subclass of `java.net.ServerSocket`
SSL_SOCKET_FACTORY and
SSL_SERVER_SOCKET_FACTORY Classes

- **javax.net.ssl.SSLSocketFactory**
  - A factory for creating secure sockets
- **javax.net.ssl.SSLServerSocketFactory**
  - A factory for creating secure server sockets
- **To obtain an SSLSocketFactory**
  - Get the default factory from `SSLSocketFactory.getDefault`
  - Construct a new factory with specifically configured behavior.
SSLSession Interface

• Represents a security context negotiated between the two peers of an SSLSocket connection
• Can be shared by future SSLSockets connected between the same two peers
• Contains
  – The cipher suite
  – A hint for the network address of the remote peer
  – The shared secret
See example code
Key Managers and Trust Managers

- **Key managers** (see [KeyManagerFactory](#)) and **trust managers** (see [TrustManagerFactory](#)) use keystores for their key material. A key manager manages a keystore and supplies public keys to others as needed, e.g., for use in authenticating the user to others. A trust manager makes decisions about who to trust based on information in the truststore it manages.

Keystores and Truststores
References

• Java™ Secure Socket Extension (JSSE) Reference Guide,
  http://java.sun.com/j2se/1.4.2/docs/guide/security/jsse/JSSERefGuide.html

• The TLS Protocol version 1.0 Internet Draft:
  http://www.ietf.org/rfc/rfc2246.txt
