Distributed Systems

COMP90015 2015 SM1

Tutorial 9

Adel Nadjaran Toosi
Email: anadjaran@unimelb.edu.au

SSL/TLS - Basics

- Shared secret vs Public/Private key;
- Secure Sockets Layer (SSL);
- Transport Layer Security (TLS);
- Goals:
  - Encryption;
  - Identification;
- SSL Handshake – establish common secret;

SSL Java Sockets – certificate and env. vars

- Build your own certificate:
  - Keytool – part of the JSE;
  - Located in $JAVA_HOME/bin or %JAVA_HOME%\bin;
  - keytool -genkey -keystore <Certificate-name> -keyalg RSA;
- Server:
  - javax.net.ssl.keyStore=<Certificate-name>
  - javax.net.ssl.keyStorePassword=<password>
- Client:
  - javax.net.ssl.trustStore =<Certificate-name>
  - javax.net.ssl.trustStorePassword=<password>
- In terminal:
  - java -jar -Djavax.net.ssl.keyStore=<Certificate-name> -Djavax.net.ssl.keyStorePassword=<password> server.jar
  - java -jar -Djavax.net.ssl.trustStore=<Certificate-name> -Djavax.net.ssl.trustStorePassword=<password> client.jar

SSL Java Sockets

- Server:
  - SSLServerSocketFactory;
  - SSLServerSocket;
  - SSLSocket;
- Client:
  - SSLSocketFactory;
  - SSLSocket;