SSM Java and SSL Configuration

What to do When it Happens to You

HPSS User Forum 2002
Indiana University
June 19, 2002

Vicky White
Oak Ridge National Laboratory

Java SSM Availability

- Java added to Data Server to support:
  - hpssadm, command line SSM, available 4.2
  - SSM GUI, available 5.1
- Java optional for releases 4.2, 4.3, 4.5
- Java required for release 5.1
- Try it now and get past one learning curve before DB2 arrives

General Hints

- "Up and Running: Quick Configuration"
  - Installation Guide 3.8.1.1 (HPSS 4.3)
- hpssadm debug option: -d

What we get from SSL

- Provides encryption for user's password as it is passed to the DS
- Provides digital signature for DS, preventing an imposter from posing as the DS and collecting user passwords

Definitions

- Symmetric key encryption
  - Two parties share a secret key
  - Encrypt and decrypt with same key
  - Faster than public key, authentication not as good

Definitions

- Public key / private key encryption
  - Everybody knows public key
  - Only I know my private key
  - Encrypt with public key, decrypt with private
  - Encrypt with private key, decrypt with public
  - Slower than symmetric key, better authentication

Definitions

- Public key / private key encryption, cont
  - Encrypt with public key, decrypt with private
    - Makes key management simpler:
      - You don't have to distribute your private key
      - You don't have to protect your public key; can publish
  - Encrypt with private key, decrypt with public
    - Makes digital signatures possible

Definitions

- Digital signature
  - Electronic document which identifies a party
  - If I encrypt some known piece of information with my private key, everybody can decrypt it with my public key and know I'm the only one who could have sent it
- X.509 certificate
  - A standard form of digital signature in wide use

Definitions

- Certificate authority
  - A company like Verisign who sells certificates
- Self-signed certificate
  - A certificate signed by its creator
  - Default certificate used by SSM.
  - Sites should be able to use certificate authority instead if they wish

Definitions

- Keystore
  - File where you store keys and certificates
  - keystore.ds, cacerts
- Trusted Store
  - Keystore where you store certificates
  - cacerts

Definitions

- keytool
  - Utility for managing keystores
  - Useful options:
    - -list list the keystore
    - -v verbose mode
    - -genkey create public/private key and certificate
    - -export export public key and certificate
    - -import import public key and certificate

Definitions

- SSL - Secure Socket Layer
  - Protocol which uses symmetric and public key
  - Public key:
    - For digital certificates
    - For negotiating a symmetric one-time session key
  - Symmetric key:
    - For remainder of session

Definitions

- JSSE - Java Secure Socket Extension
  - SSL for Java

Configuration Process

- Install Java and SSL
- Configure SSL (for anybody,not just SSM)
- Configure SSM for SSL
- Configure SSM for Java Security
- Configure SSM for user authentication
- Configure SSM for user authorization

Install Java and SSL

- JSSE issues:
  - Java 1.3:
    - SSL classes in vendor-specific packages
    - JSSE separate product on Sun, bundled on IBM
  - Java 1.4:
    - SSL classes in common packages
    - JSSE bundled into Java on Sun and IBM
  - SSM coded to Sun 1.3 packages

Install Java and SSL

- Java 1.3, not 1.4
  - Some minor programming differences
  - 1.4 not yet available on AIX (except as beta)
  - JSSE issues
- Sun JSSE 1.0.3 packages
  - Don't use IBM packages
    - Rename ibmjsse.jar
  - Don't use Java 1.4 on Sun, with JSSE built in

Configure SSL (for anybody)

- Reset password on trusted store:
  - $JAVA_HOME/lib/security/cacerts

Configure SSL (for anybody)

- Adding the security provider
  - $JAVA_HOME/lib/security/java.security
  - security.provider.N=
    - com.sun.net.ssl.internal.ssl.Provider
- Specifies a Java class to use for SSL:
  - $JAVA_HOME/jre/lib/ext/jsse.jar contains class:
    - com/sun/net/ssl/internal/ssl/Provider.class
- Does NOT make you go talk to a Sun site

Configure SSM for SSL

- Create DS public/private key and certificate
- Protect password to private key
- Distribute public key and certificate
- Verify distributed public key and certificate

Configure SSM for SSL

- Create DS public/private key and certificate
  - keytool -genkey \
    - -keystore /var/hpss/ssm/keystore.ds \
    - -dname "cn=HPSS Data Server" \
    - -alias hpss_ssmds -validity 365
  - Creates /var/hpss/ssm/keystore.ds
  - Prompts you for password for keystore.ds
    - You get to choose and set password

Configure SSM for SSL

- Protect password to keystore.ds
  - Store and protect online (default):
    - Store in /var/hpss/ssm/keystore.ds.pw
    - HPSS_SSMDS_KEYSTORE_PW=
      - /var/hpss/ssm/keystore.ds.pw
  - Type in at DS startup:
    - Let DS prompt you at startup to type in password
    - HPSS_SSMDS_KEYSTORE_PW="PROMPT"
- Protect Unix permissions on both files

Configure SSM for SSL

- Distribute public key and certificate
  - Export from keystore.ds into tmp file
    - keytool -export
      - keystore /var/hpss/ssm/keystore.ds \
      - -alias hpss_ssmds -file /tmp/ds.cer
  - Import from tmp file into trusted store
    - keytool -import
      - keystore $JAVA_HOME/lib/security/cacerts \
      - -alias hpss_ssmds -file /tmp/ds.cer

Configure SSM for SSL

- "keytool -import"prompts for verification:
  - Dumps fingerprints:
  - MD5:
  - 78:00:B0:E0:18:A4:CF:34:CF:19:2E:D2:DE:E0:60:6B
  - SHA1:
  - A7:8C:AF:9C:41:80:56:DD:5C:D8:06:0B:00:AF:F1:E4:DC:D7:C2:00
  - Compare with fingerprints from keystore.ds:
    - keytool -keystore /var/hpss/ssm/keystore.ds -list -v

Configure SSM for SSL

- Don't forget keytool -alias option
  - Install guide specifies "hpss_ssmds"
    - keytool -alias hpss_ssmds
  - This alias is the short tag used to identify the entry in the keystore
  - Without it, you get a default alias "mykey"

Configure SSM for SSL

- Don't try to set expiration date to "forever"
  - Install guide specifies 365 days:
    - keytool -validity 365
  - 100 years is too long
  - keytool does create the key and certificate
  - expiration date is invalid
  - DS will use certificate, but clients will reject it

Configure SSM for SSL

- Expired certificates
  - Verify: read the keystore with verbose option:
    - keytool -keystore cacerts -list -v
      - Valid from: Tue Sep 18 14:05:43 EDT 2001
      - until: Wed Sep 18 14:05:43 EDT 2002

Configure SSM for SSL

- Expired certificates
  - To replace:
    - Remove old certificate from trusted store:
      - keytool -keystore cacerts -delete -alias hpss_ssmds
    - Create new public/private key and redistribute

Configure SSM for Java

- Nothing to do with SSL
- Code imposes Java Security Manager which abides by policy files
  - /var/hpss/ssm/java.policy.ds
  - /var/hpss/ssm/java.policy.hpssadm
    - Renamed to java.policy.ssmuser in 5.1

Configure SSM for Java

- Policy files:
  - Use templates as starting files:
    - /opt/hpss/config/templates
      - java.policy.ds.template
      - java.policy.hpssadm.template
  - Make sure Unix permissions allow access

Configure SSM for Java

- Policy files, continued:
  - Customize SocketPermission
    - “*.hpss.acme.com:1024-”,
    - Wildcards allowed only for first field
    - Wildcards don’t work with numeric addresses

Configure SSM for User Authentication

- Keytab for each user
  - Create using rgy_edit
  - Store and protect on machine where user executes hpssadm

Configure SSM for User Authentication

- Why not let user type in his password?
  - Can't avoid echoing the password unless:
    - We use native (non-Java) code
      - Then it's less portable
    - We use graphics
      - Then it's no longer a pure ASCII application
  - keytab required for batch mode anyway
  - User community is small; sysadms/operators

Configure SSM for User Authentication

- Suggestion:
  - Run hpssadm only from DS machine
  - No real advantage running it elsewhere
- GUI won't require keytab
- GUI login screen will hide password

Configure SSM for User Authorization

- hpssadm.config
  - Lists authorized SSM users
  - Equivalent of Sammi user_authorization.dat
  - HPSS_SSMDS_AUTH_USER=joe
- HPSS 5.1:
  - Renamed to ssmuser.config
  - hpssuser will be modified to add users here

Configure SSM for User Authorization

- hpssadm.config, cont
  - /opt/hpss/config/templates:
    - hpssadm.config.template
  - Ignore old options:
    - #HPSS_SSMDS_LANGUAGE=en
    - #HPSS_SSMDS_COUNTRY=US
    - #HPSS_SSMDS_RMI_NAME=//arm1:1066/ssmds
    - #HPSS_SSMDS_INTERVAL=60000

Other Security Measures

- Protect the DS machine
  - It houses keystore.ds
  - It may house keystore.ds.pw
  - RMI registry writable by anybody on same machine

Other Security Measures

- Set the DS umask to 077
  - Keystore passwords show up in core files
  - 4.5 has umask fix in start_ssm script
  - Operational service bulletin for 4.2, 4.3

SSM 5.1 Security Enhancements

- Firewall navigation
  - Can get through ports your net admin allows
- NAT (Network Address Translation)
  - VPN, cable modems

Common Error Messages

- SSL implementation not available
  - JSSE is not installed
  - SSL provider not added to security file
    - $JAVA_HOME/lib/security/java.security file
  - Mixed JSSE versions and/or vendors

Common Error Messages

- Connection refused
  - DS is not executing
  - Non-Java version of DS is executing
  - Mismatch for RMI name and/or port
  - Policy file does not allow access to/from host
  - Firewall or VPN

Common Error Messages

- untrusted server cert chain
  - DS certificate is not in trusted store (cacerts)
  - DS certificate in cacerts doesn't match the one the DS is using from its keystore.ds file
  - DS certificate is expired

Common Error Messages

- java.io.FilePermission
  - Usually gives name of file and type of permission lacking
  - Example:
    - java.io.FilePermission keystore.ds read
      - Java policy file does not allow read access to file keystore.ds

Common Error Messages

- java.lang.ClassNotFoundException
  - CLASSPATH set wrong
    - config/hpss_env
  - Not all jar files installed
  - Need to do a make from clean:
    - /opt/hpss/src/ssm

Common Error Messages

- Almost anything
  - HPSS_ROOT set wrong
    - config/hpss_env
  - Not all jar files installed
  - Need to do a make from clean
  - Need to restart DS
    - Let it reread policy file, config file, etc.

References

- Introduction to Public-Key Cryptography
  - http://developer.netscape.com/docs/manuals/security/pkin/index.htm
- Introduction to SSL
  - http://developer.netscape.com/docs/manuals/security/sslin/contents.htm
- Java policy file syntax:
  - http://java.sun.com/products/jdk/1.2/docs/guide/security/PolicyFiles.html
- keytool utility man page:
  - http://java.sun.com/products/jdk/1.2/docs/tooldocs/solaris/keytool.html
  - http://java.sun.com/products/jdk/1.2/docs/tooldocs/win32/keytool.html