Q&A with the Security Group

Sean Mullan, Bradford Wetmore, Frances Ho
Java Security Libraries Team
Oracle
September 29, 2014

Who we are

- Members of the Java Security Libraries Team at Oracle and the OpenJDK Security Group
- Responsible for the maintenance and evolution of the core security libraries in Java SE/JDK
  - Security Manager
  - APIs and Libraries: Cryptography (JCE), PKI, SSL/TLS (JSSE), SASL, JAAS, GSSAPI/Kerberos, XML Signature
  - Tools: keytool, jarsigner, policytool

New JDK 8 Security Features Highlights

- **13** new features!
  - New features span the entire security stack
- **Significant** crypto improvements
  - Hardware-accelerated crypto performance improvements
  - Support for new and stronger algorithms
- **Significant** JSSE (SSL/TLS) improvements
  - More secure out of the box defaults
  - Support for the SNI Extension
  - New GCM cipher suites

13 New Security Features

http://openjdk.java.net/jeps

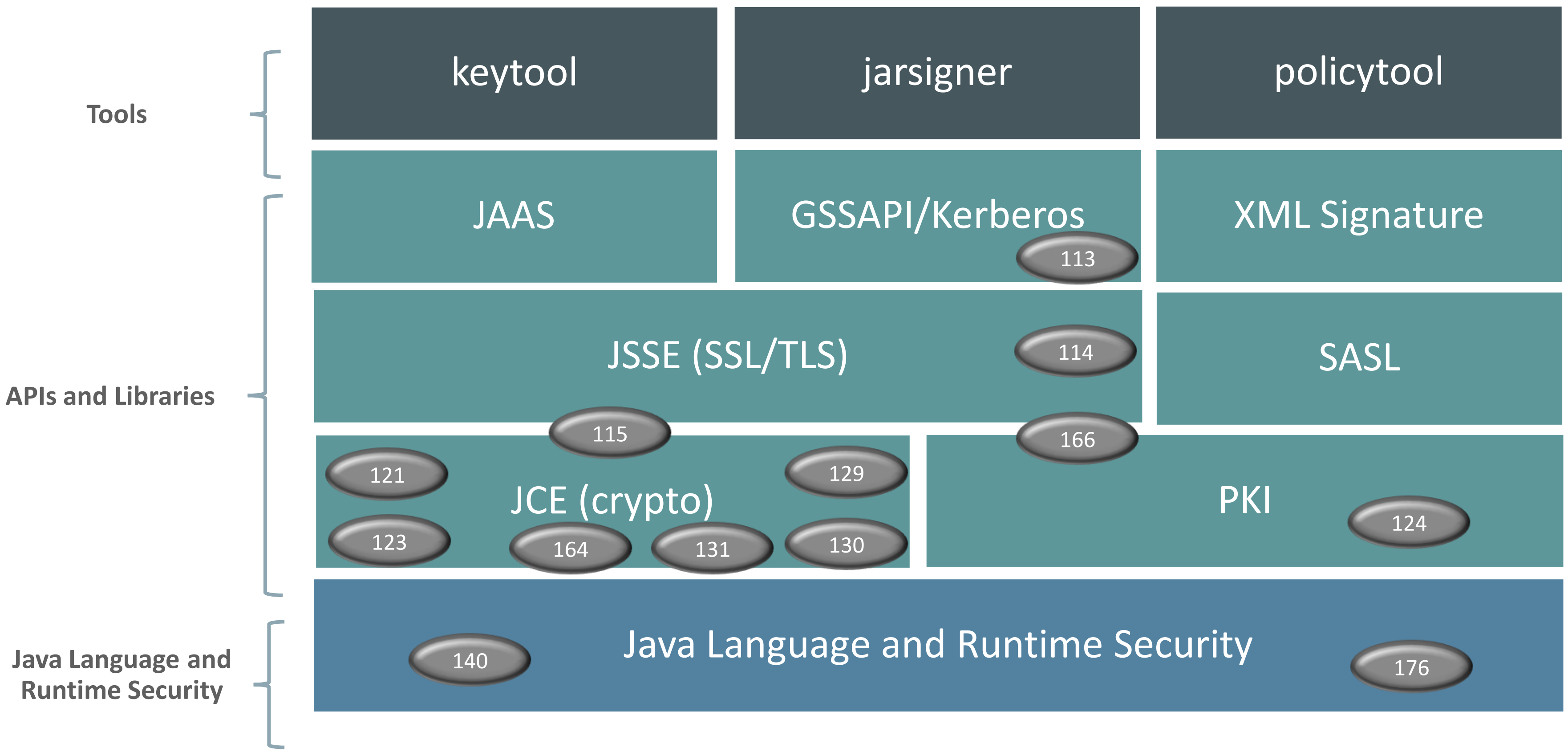
JEP	Title
113	MS-SFU Kerberos 5 Extensions
114	TLS Server Name Indication (SNI) Extension
115	AEAD CipherSuites
121	Stronger Algorithms for Password-Based Encryption
123	Configurable Secure Random-Number Generation
124	Enhance the Certificate Revocation-Checking API
129	NSA Suite B Cryptographic Algorithms

13 New Security Features (continued)

http://openjdk.java.net/jeps

JEP	Title
130	SHA-224 Message Digests
131	PKCS#11 Crypto Provider for 64-bit Windows
140	Limited doPrivileged
164	Leverage CPU Instructions for AES Cryptography
166	Overhaul JKS-JCEKS-PKCS12 Keystores
176	Mechanical Checking of Caller-Sensitive Methods

Java SE Security Conceptual Diagram
Where the features are



Tools

keytool

jarsigner

policytool

APIs and Libraries

JAAS

GSSAPI/Kerberos

113

XML Signature

JSSE (SSL/TLS)

114

SASL

115

166

121

129

JCE (crypto)

123

164

131

130

PKI

124

Java Language and Runtime Security

Java Language and Runtime Security

140

176

JEP = JDK Enhancement-Proposal

JDK 8 Cryptography Features

- SHA-224 MessageDigests
- `SecureRandom` improvements
  - New `SecureRandom.getInstanceStrong API`
- Strengthened DSA and Diffie-Hellman support
  - 2048-bit keypairs and SHA256WithDSA Signature algorithm
- Hardware-accelerated AES crypto performance
  - JVM intrinsics dramatically improve performance on x86 and SPARC (8u20)
- Authenticated AES GCM `Cipher` mode
- Stronger Algorithms for Password-Based Encryption (PBE)

JDK 8 TLS/SSL Features

- Authenticated GCM Cipher Suites
- Server Name Indication (SNI) Extension
  - Indicates the hostname of the server the client wants to establish a session with
  - Useful when a server has multiple domains that share the same IP address
- TLS 1.1 and 1.2 enabled by default on client
- Server Cipher Suite Preference
  - New `SSLParameters.setUseCipherSuitesOrder()` method
- Stronger Server Ephemeral Diffie-Hellman Parameters

Other Notable JDK 8 Security Features

- Major KeyStore enhancements
  - New DKS (Domain) KeyStore type
- New Revocation Checking `PKIXRevocationChecker` API
- Support for MS-SFU Kerberos 5 Extensions
- Limited doPrivileged
- X.509 Certificates with RSA keys less than 1024 bits disabled by default
- Kerberos 5 DES encryption types are disabled by default

New JDK 8 Update Security Features

- 8u20
  - AES intrinsics on Solaris/SPARC
  - New root CA certificates for Buypass, Chunghwa, Trend Micro and Trustwave
- 8u40
  - Leverage CPU Instructions to Improve SHA Performance on SPARC (http://openjdk.java.net/jeps/207)

Potential JDK 9 Security Features

- Cryptography
  - JVM Hardware Crypto Acceleration (http://openjdk.java.net/jeps/8046943)
  - Transition the default keystore type from JKS to PKCS12
- TLS/SSL
  - DTLS (http://openjdk.java.net/jeps/8043758)
  - OCSP Stapling
  - Application-Layer Protocol Negotiation Extension
- Improve Security Manager Performance (http://openjdk.java.net/jeps/8043631)

Other Recommended Sessions

- CON5778: Understanding the New JDK 8 Security Features
  - Wednesday 11:30 AM - Hilton - Imperial Ballroom A
- CON6693: Java Secure Coding Guidelines
  - Wednesday 10:00 AM – Hilton – Golden Gate 6/7/8
- CON2368: Inside the CERT Oracle Secure Coding Standard for Java
  - Thursday 4:00 PM – Hilton – Golden Gate 6/7/8
- CON3326: Applying Java's Cryptography
  - Wednesday 4:30 PM – Hilton – Golden Gate 6/7/8
- HOL6325: Java Native Interface: Harden Your Native Code
  - Tuesday 7:00 PM – Hilton – Franciscan A/B

More Information

- Security Guides and Overview
  - http://docs.oracle.com/javase/8/docs/technotes/guides/security/index.html
- OpenJDK Security Group: http://openjdk.java.net/groups/security/
  - Mailing list: security-dev@openjdk.java.net
- JEPs: http://openjdk.java.net/jeps
- JDK 8 downloads: http://www.oracle.com/technetwork/java/javase/downloads/index.html
- JDK 8 docs: http://docs.oracle.com/javase/8/
- Twitter: @seanjmullan

Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Q & A