No 256 bit ciphers for Java apps

Problem

If you use Tomcat to run Java apps such as Atlassian Confluence (the page you're looking at now), JIRA, etc, via HTTPS, you might have noticed that your app will not support any 256 bit ciphers, however it will support 128 and 168 bit ciphers, as well as the lame 40 and 56 bit ciphers. The sslscan tool confirms this, and reports:

Accepted	SSLv3	128 bits	DHE-RSA-AES128-SHA
Accepted	SSLv3	128 bits	AES128-SHA
Accepted	SSLv3	168 bits	EDH-RSA-DES-CBC3-SHA
Accepted	SSLv3	56 bits	EDH-RSA-DES-CBC-SHA
Accepted	SSLv3	40 bits	EXP-EDH-RSA-DES-CBC-SHA
Accepted	SSLv3	168 bits	DES-CBC3-SHA
Accepted	SSLv3	56 bits	DES-CBC-SHA
Accepted	SSLv3	40 bits	EXP-DES-CBC-SHA
Accepted	SSLv3	128 bits	RC4-SHA
Accepted	SSLv3	128 bits	RC4-MD5
Accepted	SSLv3	40 bits	EXP-RC4-MD5
Accepted	TLSv1	128 bits	DHE-RSA-AES128-SHA
Accepted	TLSv1	128 bits	AES128-SHA
Accepted	TLSv1	168 bits	EDH-RSA-DES-CBC3-SHA
Accepted	TLSv1	56 bits	EDH-RSA-DES-CBC-SHA
Accepted	TLSv1	40 bits	EXP-EDH-RSA-DES-CBC-SHA
Accepted	TLSv1	168 bits	DES-CBC3-SHA
Accepted	TLSv1	56 bits	DES-CBC-SHA
Accepted	TLSv1	40 bits	EXP-DES-CBC-SHA
Accepted	TLSv1	128 bits	RC4-SHA
Accepted	TLSv1	128 bits	RC4-MD5
Accepted	TLSv1	40 bits	EXP-RC4-MD5

So what's the problem here?

The issue lies in the so-called *policy files* of JDK6. According to Sun:

Due to import control restrictions for some countries, the Java Cryptography Extension (JCE) policy files shipped with the Java SE Development Kit and the Java SE Runtime Environment allow strong but limited cryptography to be used.

Enable 256 bit ciphers

From the Sun website, download the JCE Unlimited Strength Jurisdiction Policy Files 6 Release Candidate. Unpack the ZIP file - it will contain two jar files: local_policy.jar and US_export_policy.jar. On our Ubuntu boxes we use the packages sun-java6-jdk, sun-java6-bin, and sun-java6-jre. The files in question are stored in /usr/lib/jvm/java-6-sun/jre/lib/security. Replace the default jar files with the ones you downloaded, then restart your app. It should now support 256 bit ciphers:

Accepted	SSLv3	256 bits	DHE-RSA-AES256-SHA
Accepted	SSLv3	256 bits	AES256-SHA
Accepted	TLSv1	256 bits	DHE-RSA-AES256-SHA
Accepted	TLSv1	256 bits	AES256-SHA

Disable 40 and 56 bit ciphers

By default, also 40 and 56 bit ciphers are supported - you probably want to disable these. To do so you have to explicitly configure the allowed ciphers: take the previous list, include the 256 bit ciphers, leave out the 40 and 56 bit ones, then put the official names (not the OpenSSL equivalent) of the remaining ciphers in your HTTPS config (in my case at the bottom of server.xml). This will look like this:

<connector< th=""></connector<>
port="443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" useBodyEncodingForURI="true"
URIEncoding="UTF-8" SSLEnabled="true"
keystoreFile="/etc/ssl/private/tracker.jks"
keystorePass="hackme"
ciphers="SSL_DHE_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_AES_256_CBC_SHA,
SSL_DHE_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_AES_128_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_RC4_128_MD5,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5" />

After restarting your app, you can verify with sslscan that now 256 bit ciphers are supported and preferred, and no 40 and 56 bits ones are available anymore:

```
./sslscan --no-failed my.site.org:443
[...]
 Supported Server Cipher(s):
   Accepted SSLv3 256 bits DHE-RSA-AES256-SHA
   Accepted SSLv3 256 bits AES256-SHA
   Accepted SSLv3 128 bits DHE-RSA-AES128-SHA
   Accepted SSLv3 128 bits AES128-SHA
   Accepted SSLv3 168 bits EDH-RSA-DES-CBC3-SHA
   Accepted SSLv3 168 bits DES-CBC3-SHA
   Accepted SSLv3 128 bits RC4-SHA
   Accepted SSLv3 128 bits RC4-MD5
   Accepted TLSv1 256 bits DHE-RSA-AES256-SHA
   Accepted TLSv1 256 bits AES256-SHA
   Accepted TLSv1 128 bits DHE-RSA-AES128-SHA
   Accepted TLSv1 128 bits AES128-SHA
   Accepted TLSv1 168 bits EDH-RSA-DES-CBC3-SHA
Accepted TLSv1 168 bits DES-CBC3-SHA
   Accepted TLSv1 128 bits RC4-SHA
   Accepted TLSv1 128 bits RC4-MD5
 Prefered Server Cipher(s):
   SSLv3 256 bits DHE-RSA-AES256-SHA
   TLSv1 256 bits DHE-RSA-AES256-SHA
```

For apache the following will have the same result:

SSLCipherSuite ALL: !ADH: !EXP: !DES: RC4+RSA: +HIGH: +MEDIUM!SSLv2