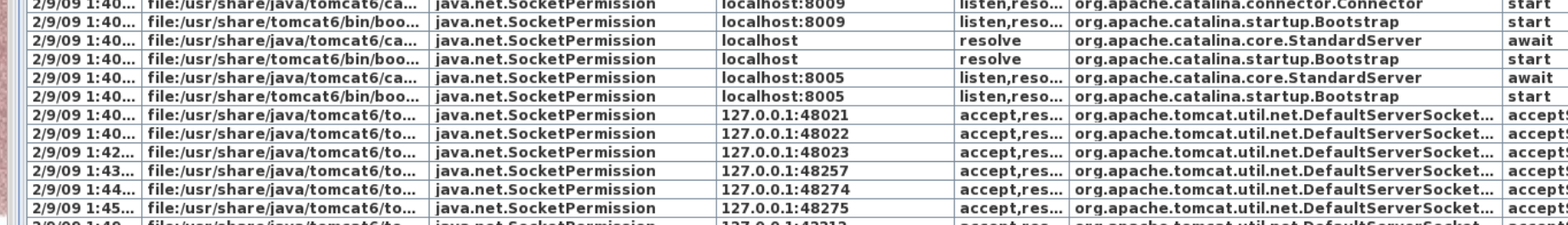
Jchains

Analyzing Java Permissions on the fly



Time	Codebase	Permission	Target	Actions	Class	
2/9/09 1:39...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	localhost:8080	listen,reso...	org.apache.tomcat.util.net.DefaultServerSocket...	createS
2/9/09 1:39...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:8080	listen,reso...	org.apache.catalina.connector.Connector	initializ
2/9/09 1:39...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:8080	listen,reso...	org.apache.catalina.startup.Bootstrap	load
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.hibernate.id.AbstractUUIDGenerator	<clinit>
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.hibernate.cfg.AnnotationConfiguration	buildSe
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.hibernate.ejb.Ejb3Configuration	buildEn
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.jboss.seam.persistence.EntityManagerFactory	createE
2/9/09 1:39...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost.localdomain	resolve	org.apache.catalina.core.StandardContext	listener
2/9/09 1:39...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost.localdomain	resolve	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost:5001	listen,reso...	org.apache.axis.monitor.SOAPMonitorService	init
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:5001	listen,reso...	org.apache.catalina.security.SecurityUtil$1	run
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:5001	listen,reso...	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	localhost:8009	listen,reso...	org.apache.jk.common.ChannelSocket	init
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:8009	listen,reso...	org.apache.catalina.connector.Connector	start
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:8009	listen,reso...	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost	resolve	org.apache.catalina.core.StandardServer	await
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost	resolve	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:8005	listen,reso...	org.apache.catalina.core.StandardServer	await
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:8005	listen,reso...	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48021	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptS
2/9/09 1:40...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48022	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptS
2/9/09 1:42...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48023	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptS
2/9/09 1:43...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48257	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptS
2/9/09 1:44...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48274	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptS
2/9/09 1:45...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48275	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptS

Motivation

- The java security manager is helpful to block unauthorized accesses
- Unfortunately in 99% of installations it is
  - Deactivated
  - Or configured by giving the entire code AllPermissions

The problem with j.s.AllPermission

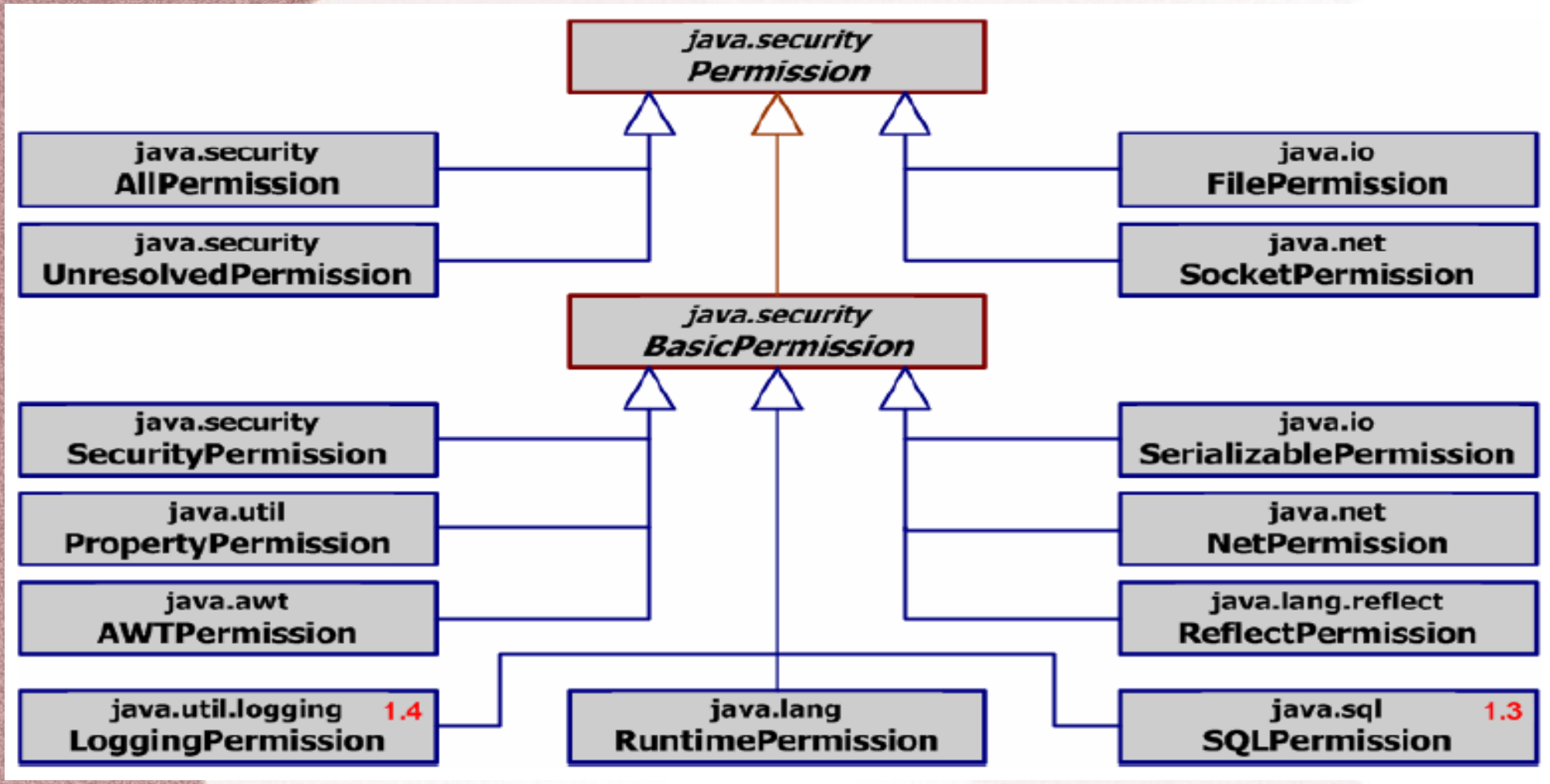
It is difficult to identify the specific permissions needed by code (exspecially when using undocumented 3rd party libs)

- To quickly get rid of the “security adminstration problem”, admins often decide to grant “AllPermissions” to libraries

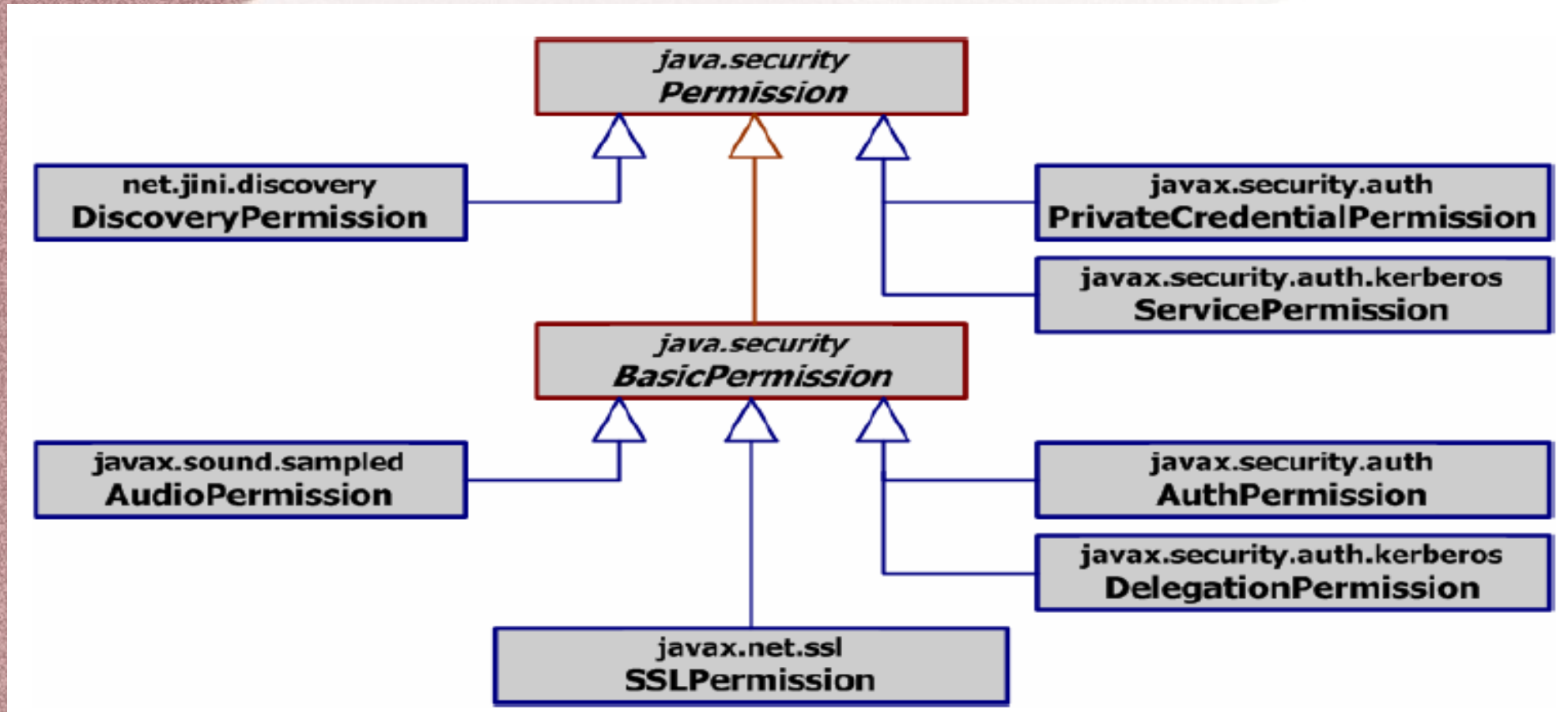
A short introduction to Java Permissions

- Java **permissions** control which resources are available to codebases
- A **codebase** is the location of a jar like
  - file:/usr/share/tomcat6/bin/bootstrap-6.0.18.jar
- A permission controls access to Socket, Files, Properties, privileged actions (System.exit) , etc.

Standard-Permissions



Optional Permissions



Policy-File (like the default sandbox)

```
// Standard extensions are granted full access !
grant codeBase "file:${java.home}/lib/ext/*" {
    permission java.security.AllPermission;
};
// default permissions granted to all domains
grant {
      permission java.lang.RuntimePermission "stopThread";
      permission java.net.SocketPermission "localhost:1024-", "listen";
      permission java.util.PropertyPermission "java.version", "read";
      permission java.util.PropertyPermission "java.vendor", "read";
      permission java.util.PropertyPermission "java.vendor.url", "read";
      permission java.util.PropertyPermission "java.class.version", "read";

      permission java.util.PropertyPermission "os.name", "read";
      permission java.util.PropertyPermission "os.version", "read";
      permission java.util.PropertyPermission "os.arch", "read";
      permission java.util.PropertyPermission "file.separator", "read";
    […]
};
```

Two parts of jchains

- Jchains **Emitter** logs permissions that are requested by the JVM
- Jchains **Receiver** provides a graphical user interface to browse the log

Jchains intercepts the Java SecurityManager

- The app to observe
  - Add a few properties
  - Add jchains.jar
- It overrides the JavaSecurity
  - Djava.security.manager= org.jchains.intercept.JChainsSecInterceptor
- It writes to a log file (CSV)
  - Dorg.jchains.file=tomcat.csv

Example using jchains with Tomcat

- JCHAINS_LIB=../jchains.jar
- JAVA_OPTS="
  - ...
  - Xbootclasspath/a:${JCHAINS_LIB}
  - Dorg.jchains.always=true
  - Dorg.jchains.emitClass=StandardEmitter
  - Dorg.jchains.file=tomcat.csv
  - Djava.security.policy=test.policy
  - Djava.security.manager= org.jchains.intercept.JChainsSecInterceptor"

How to prepare the app to observe

tomcat_jchains.sh + (~/workspace/JChains/sampleconf) - GVIM

File Edit Tools Syntax Buffers Window Help

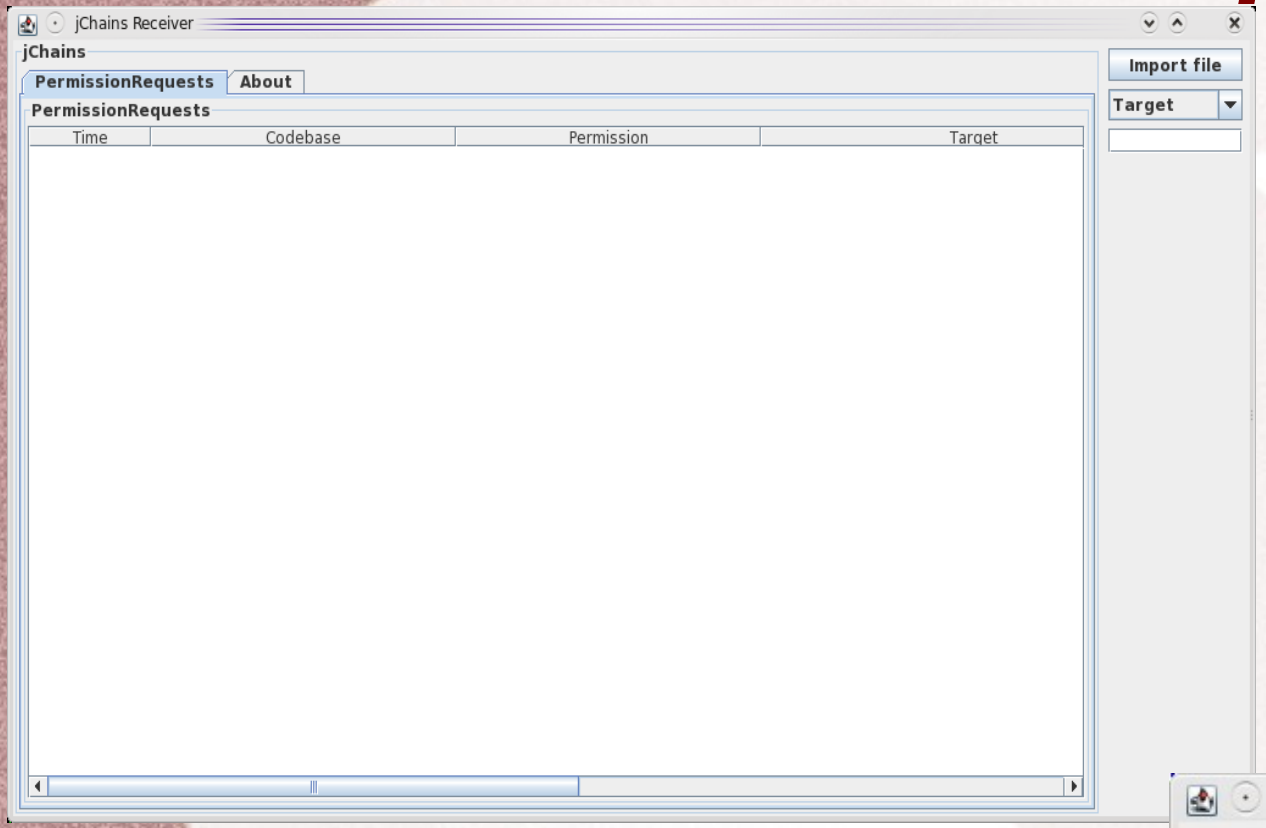
```
JAVA_HOME_LINUX=/usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0/jre/
TOMCAT_SCRIPT_LINUX=/usr/sbin/tomcat6
#JAVA=${JAVA_MAC}
#JAVA_HOME=${JAVA_HOME_MAC}

JAVA=${JAVA_LINUX}
JAVA_HOME=${JAVA_HOME_LINUX}
TOMCAT_SCRIPT=${TOMCAT_SCRIPT_LINUX}

JCHAINS_LIB=../jchains.jar

DIRNAME=.
#:FOUND_RUN_JAR
JCHAINS_CLASSPATH=${JCHAINS_LIB}

JAVA_OPTS="-Dcom.sun.management.jmxremote -Xbootclasspath/a:${JCHAINS_LIB} -Xmx1024M -Dorg.jchains.always=true -Dorg.jchains.emitClass=StandardEmitt
er -Dorg.jchains.file=tomcat.csv -Djava.security.policy=test.policy -Djava.security.manager=org.jchains.intercept.JChainsSecInterceptor"

CLASSPATH=${JCHAINS_CLASSPATH}

echo ================================================================================
echo   JAVA: ${JAVA}
echo   JAVA_OPTS: ${JAVA_OPTS}
echo   CLASSPATH: ${CLASSPATH}
echo ================================================================================

mkdir tombase
mkdir tombase/tomcat6/conf

cp /etc/tomcat6/tomcat6.conf tom.cfg.orig
cp --copy-contents --preserve=timestamps  -R /usr/share/tomcat6/ tombase/
rm tombase/tomcat6/webapps
mkdir tombase/tomcat6/webapps
cp --copy-contents -R /usr/share/tomcat6/webapps/* tombase/tomcat6/webapps
rm  tombase/tomcat6/logs
mkdir tombase/tomcat6/logs
rm  tombase/tomcat6/work
mkdir tombase/tomcat6/work
rm  tombase/tomcat6/temp
mkdir tombase/tomcat6/temp

cp ${TOMCAT_SCRIPT} tomcat.sh
cat tom.cfg.orig| sed -e "s,CATALINA_BASE=\"/usr/share/tomcat6,CATALINA_BASE=\"./tombase/tomcat6,g"  | sed -e "s,/var/run/tomcat6.pid,tomcat6.pid,g"
 > tomcat.cfg
```

16,0-1 62%

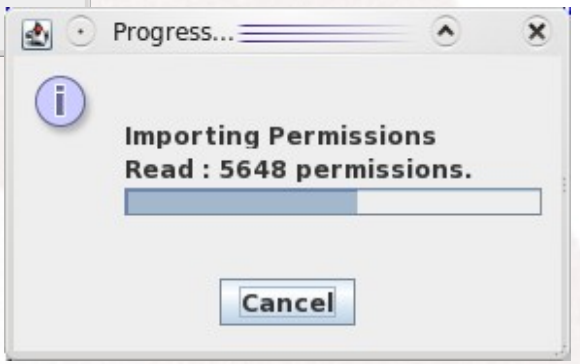
The GUI

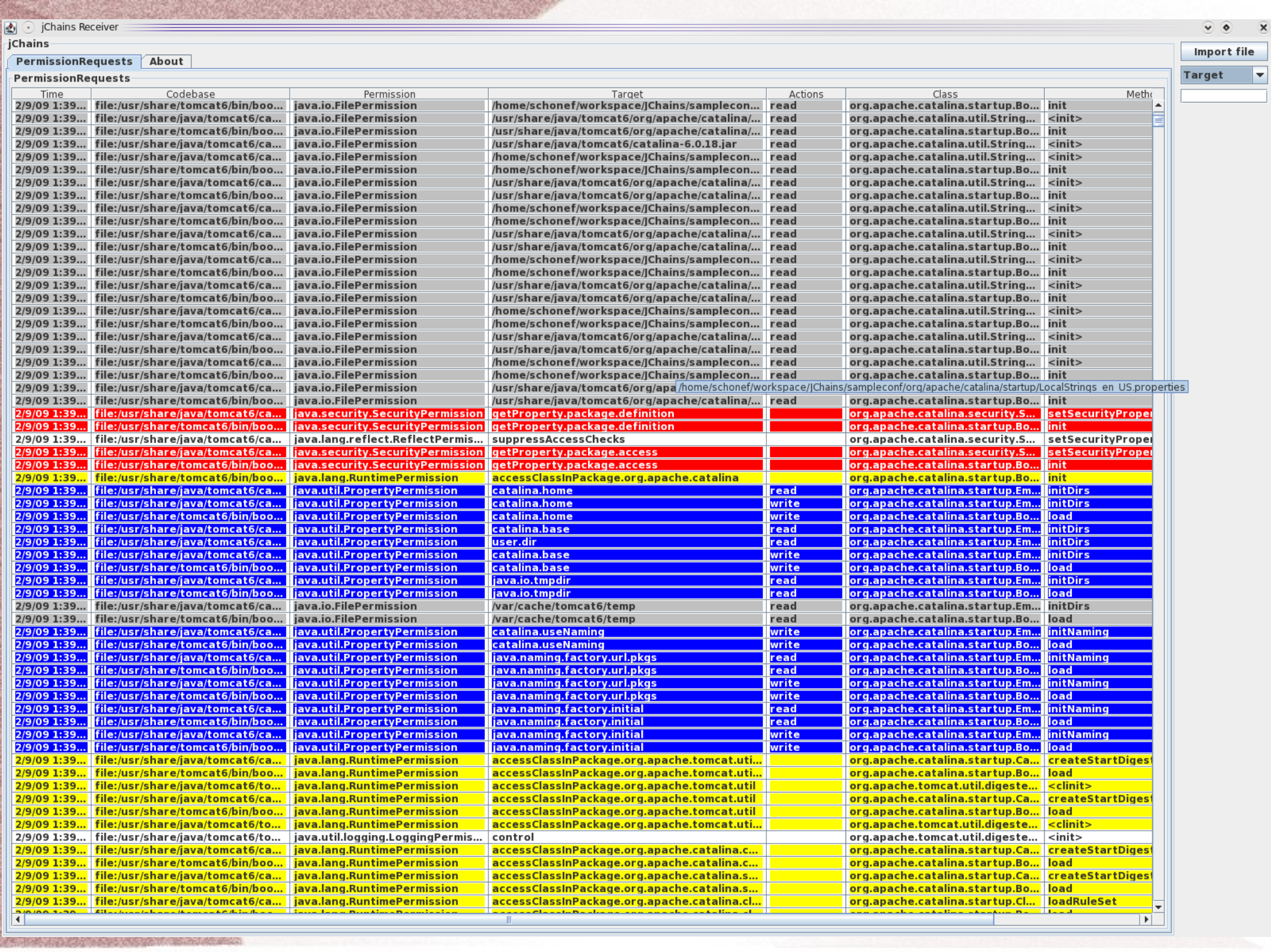
- Displays the recorded permissions
- Allows sorting and filtering (context and time based)
- Startup with
  - java -Dorg.jchains.file=tomcat.csv -jar jchains.jar -file

Starts up with an empty window



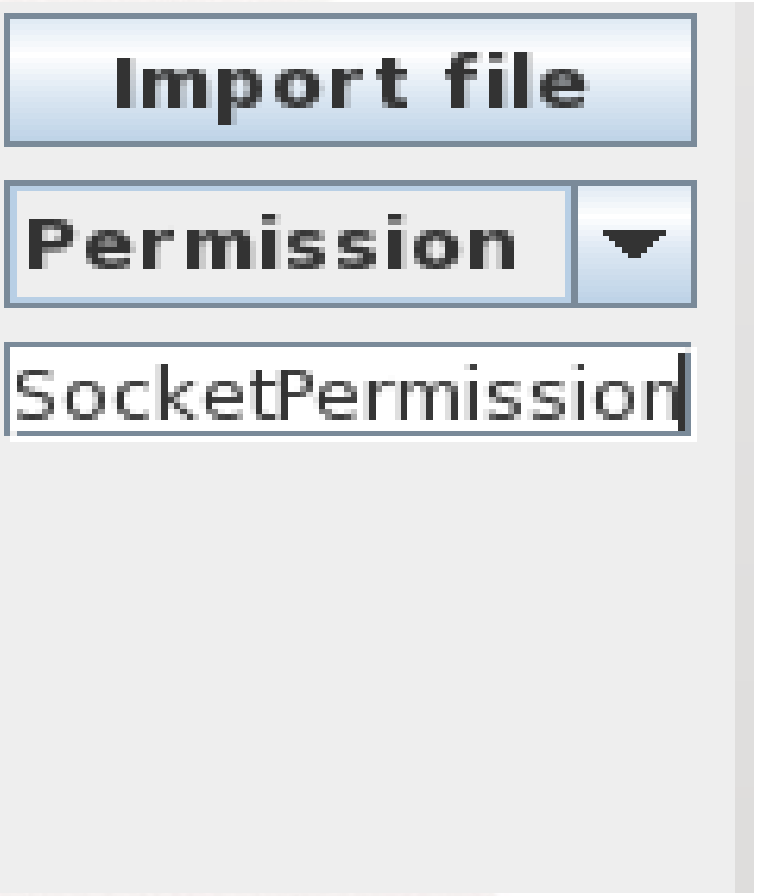
- Click “Import file” to retrieve file of recorded permissions

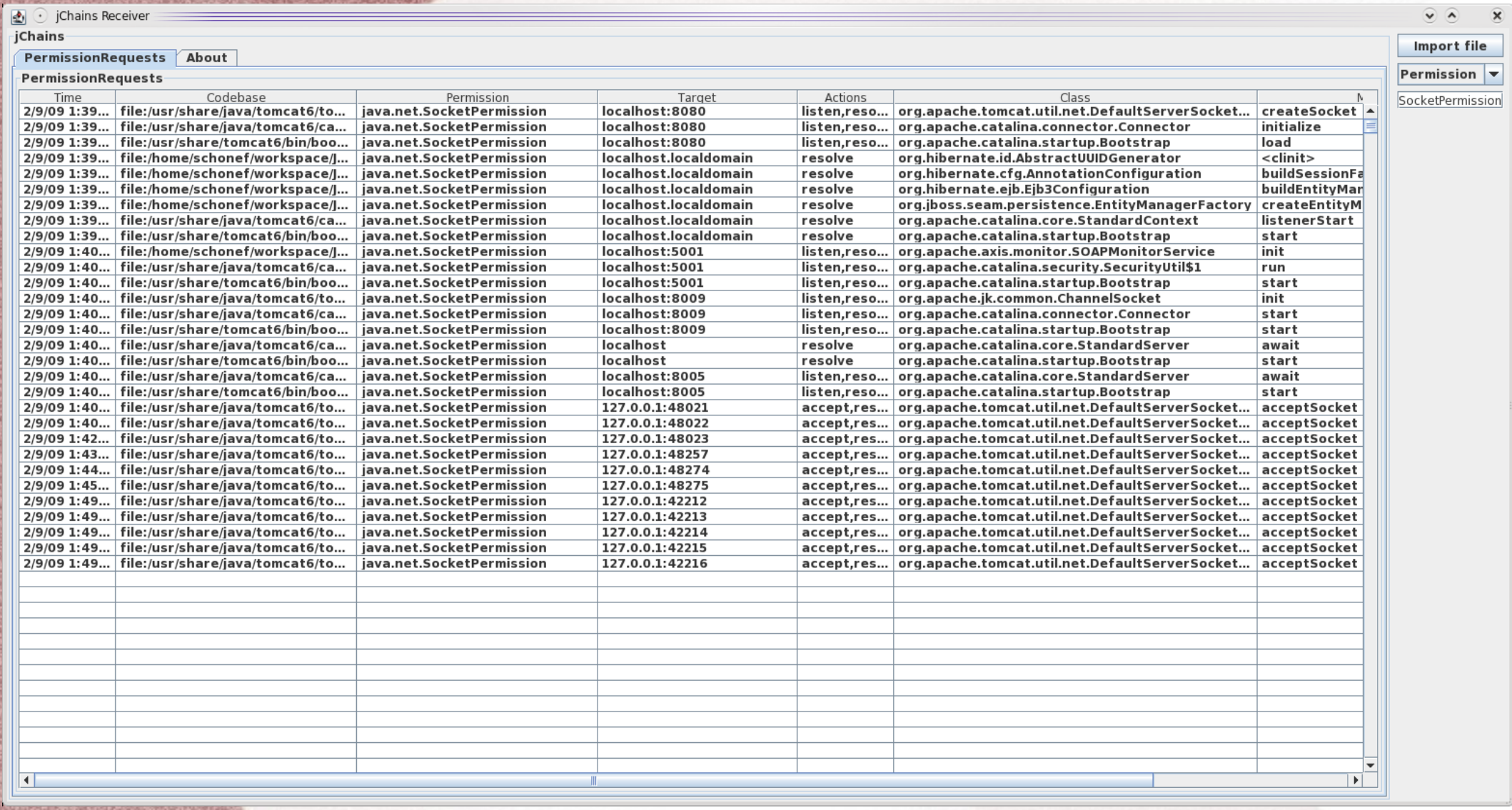



jChains Receiver
jChains
PermissionRequests
About
PermissionRequests
Import file
Target
Time
Codebase
Permission
Target
Actions
Class
Meth
/home/schonef/workspace/JChains/sampleconf/org/apache/catalina/startup/LocalStrings_en_US.properties

Also allows filtering

- Let's look for all opened sockets
- Choose Filter for the “Permission” column
- Enter “SocketPermission” as filter criteria





Time	Codebase	Permission	Target	Actions	Class	M
2/9/09 1:39...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	localhost:8080	listen,reso...	org.apache.tomcat.util.net.DefaultServerSocket...	createSocket
2/9/09 1:39...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:8080	listen,reso...	org.apache.catalina.connector.Connector	initialize
2/9/09 1:39...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:8080	listen,reso...	org.apache.catalina.startup.Bootstrap	load
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.hibernate.id.AbstractUUIDGenerator	<clinit>
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.hibernate.cfg.AnnotationConfiguration	buildSessionFa
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.hibernate.ejb.Ejb3Configuration	buildEntityMar
2/9/09 1:39...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost.localdomain	resolve	org.jboss.seam.persistence.EntityManagerFactory	createEntityM
2/9/09 1:39...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost.localdomain	resolve	org.apache.catalina.core.StandardContext	listenerStart
2/9/09 1:39...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost.localdomain	resolve	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/home/schonef/workspace/J...	java.net.SocketPermission	localhost:5001	listen,reso...	org.apache.axis.monitor.SOAPMonitorService	init
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:5001	listen,reso...	org.apache.catalina.security.SecurityUtil$1	run
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:5001	listen,reso...	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	localhost:8009	listen,reso...	org.apache.jk.common.ChannelSocket	init
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:8009	listen,reso...	org.apache.catalina.connector.Connector	start
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:8009	listen,reso...	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost	resolve	org.apache.catalina.core.StandardServer	await
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost	resolve	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/ca...	java.net.SocketPermission	localhost:8005	listen,reso...	org.apache.catalina.core.StandardServer	await
2/9/09 1:40...	file:/usr/share/tomcat6/bin/boo...	java.net.SocketPermission	localhost:8005	listen,reso...	org.apache.catalina.startup.Bootstrap	start
2/9/09 1:40...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48021	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:40...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48022	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:42...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48023	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:43...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48257	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:44...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48274	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:45...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:48275	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:49...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:42212	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:49...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:42213	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:49...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:42214	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:49...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:42215	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket
2/9/09 1:49...	file:/usr/share/java/tomcat6/to...	java.net.SocketPermission	127.0.0.1:42216	accept,res...	org.apache.tomcat.util.net.DefaultServerSocket...	acceptSocket

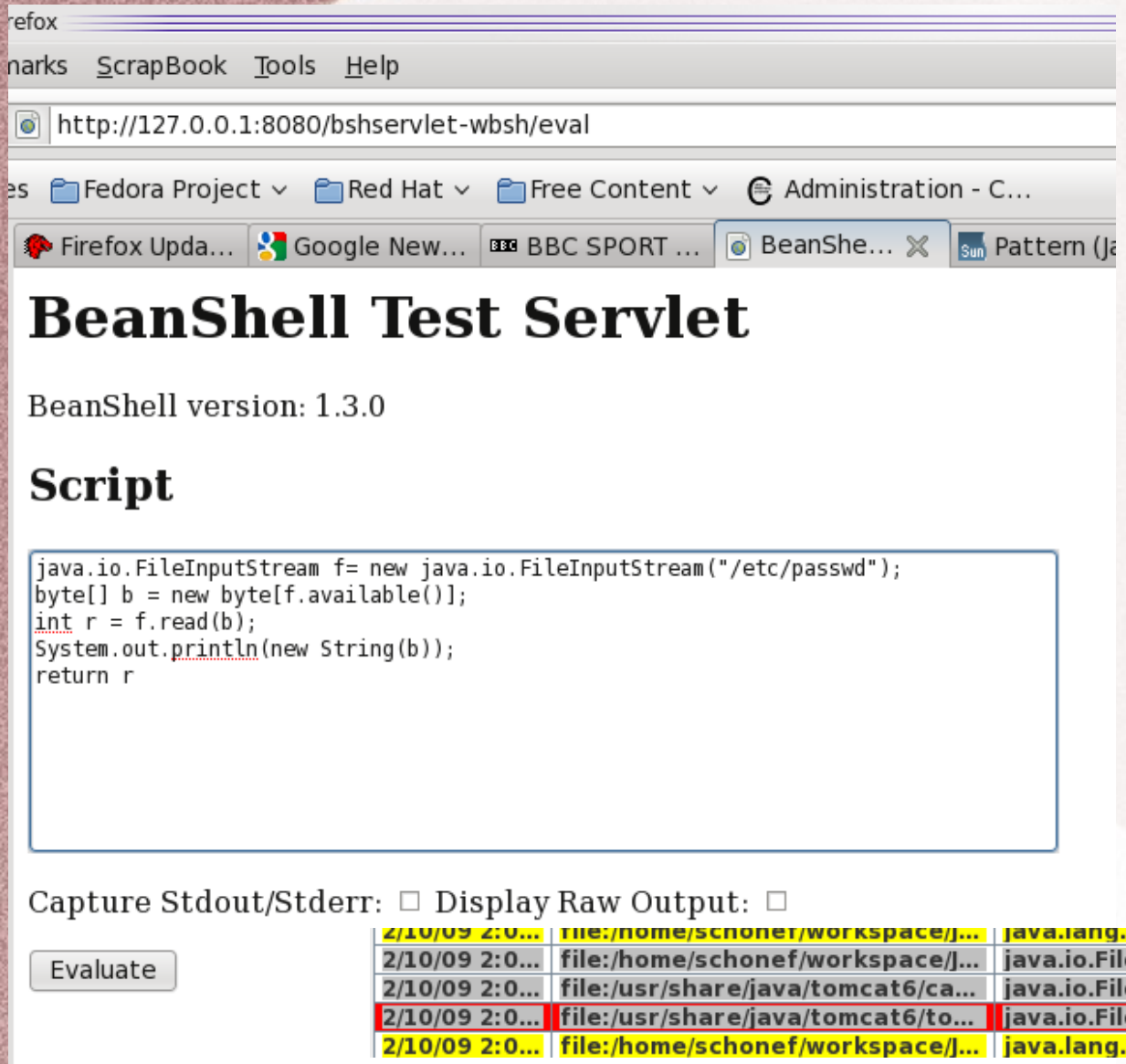
Communication between Emitter and Receiver

- **File-based**
  - Emitter drops CSV file, Receiver simply grabs the file
  - For distributed environments simply share a dir
  - Most practical for most purposes
- **Socket**
  - Serialized Permission objects passed to a port opened by the Receiver (slow)
- **CORBA**
  - Jchains can bind to a CORBA nameservice and be activated via POA mechanisms (slowest)

Further features

- No modification of application code neccessary
- Export to CSV also allows deeper analysis with spreadsheet software
- Jchains library allows to generate a policy file from a subset of the recorded permissions, will be integrated to the GUI soon
- Memory is all you need, already tested with Tomcat, EAP and Portal

Spotting suspicious patterns



2/10/09 2:0...	file:/home/schonef/workspace/J...	java.lang.RuntimePermission	accessDeclaredMembers
2/10/09 2:0...	file:/home/schonef/workspace/J...	java.io.FilePermission	/etc/passwd
2/10/09 2:0...	file:/usr/share/java/tomcat6/ca...	java.io.FilePermission	/etc/passwd
2/10/09 2:0...	file:/usr/share/java/tomcat6/to...	java.io.FilePermission	/etc/passwd
2/10/09 2:0...	file:/home/schonef/workspace/J...	java.lang.RuntimePermission	accessClassInPackage.org.apache

Further questions

- Drop me a mail if you want to try the bits
  - mschoene@redhat.com