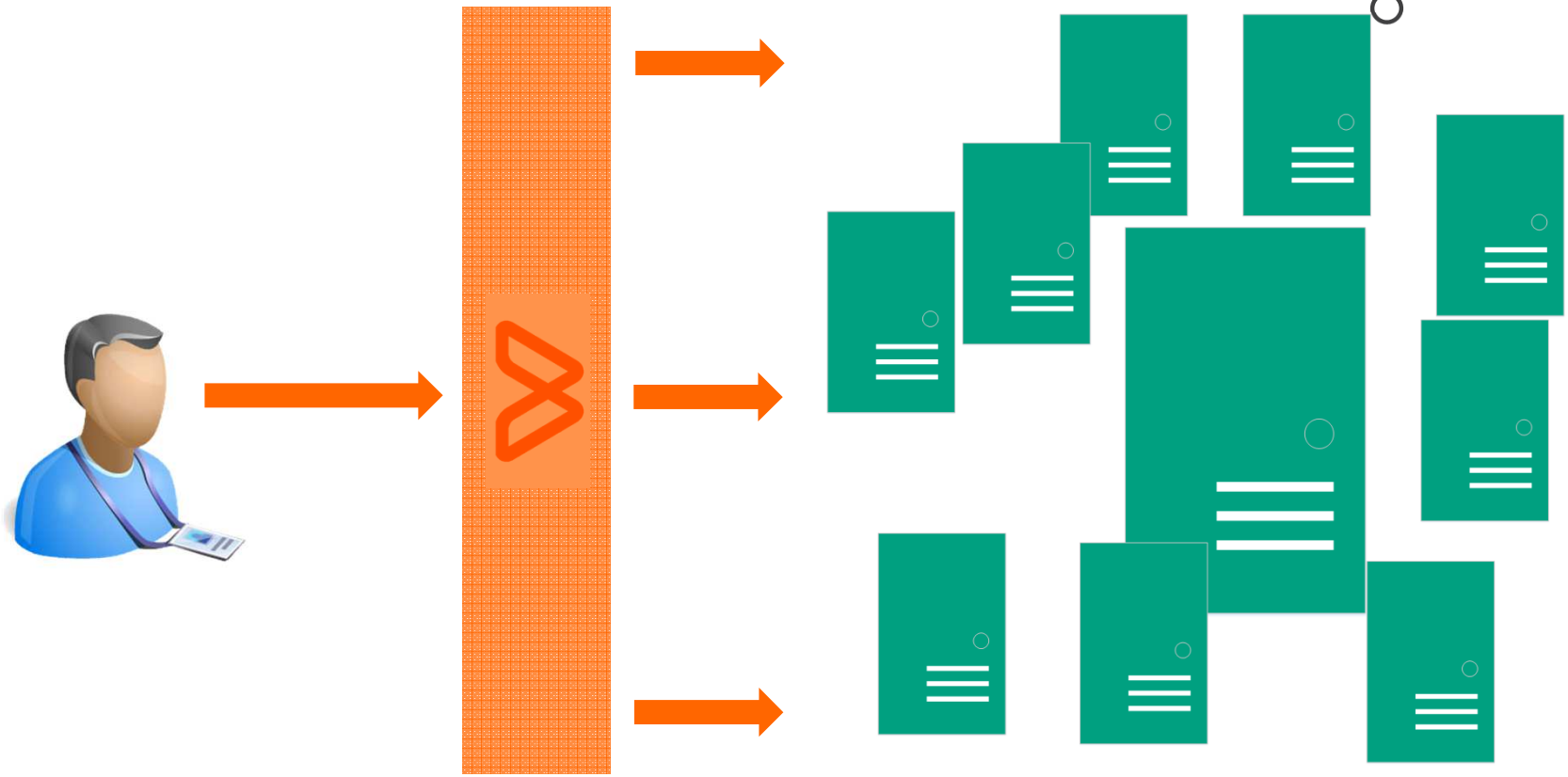
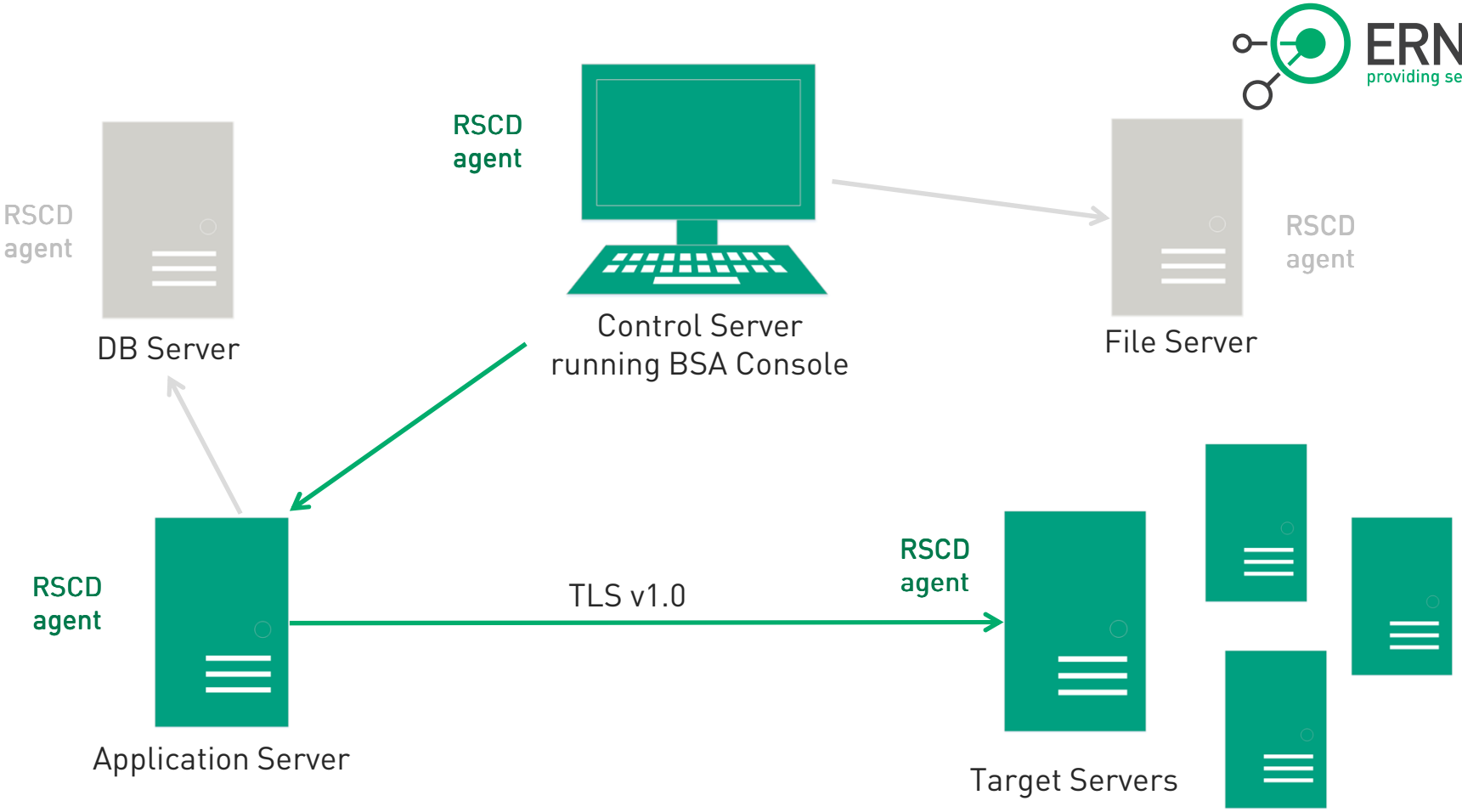
One Tool to Rule Them All – and what can it lead to

Olga Yanushkevich

Product

- BMC Software, Inc.
- BMC BladeLogic:
- Database Automation
- Middleware Automation
- Network Automation
- Server Automation




RSCD
agent
DB Server
RSCD
agent
Control Server
running BSA Console
RSCD
agent
File Server
RSCD
agent
TLS v1.0
RSCD
agent
Application Server
RSCD
agent
Target Servers

BSA: RSCD agent

- Running daemon
- Handles connections from Application Server
- By default runs with root privileges
- Secure files:
  - exports
  - users
  - users.local
  - secure & securecert

BSA: RSCD agent

```
:tc/rsc$ sudo netstat -plnt
nections (only servers)
 Local Address           Foreign Address         State       PID/Program name
 0.0.0.0:22              0.0.0.0:*               LISTEN      6501/sshd
 :::22                   :::*                    LISTEN      6501/sshd
 :::4750                 :::*                    LISTEN      1266/rscd
:tc/rsc$ _
```

Wireshark

```
TCP      62 55874 > ssad [SYN] Seq=0 Win=65535 Len=0 M
TCP      62 ssad > 55874 [SYN, ACK] Seq=0 Ack=1 Win=29
TCP      60 55874 > ssad [ACK] Seq=1 Ack=1 Win=65535 L
SSL      60 Continuation Data
TCP      54 ssad > 55874 [ACK] Seq=1 Ack=4 Win=29200 L
SSL     132 Client Hello
TCP      54 ssad > 55874 [ACK] Seq=1 Ack=82 Win=29200
TCP      54 ssad > 55874 [RST, ACK] Seq=1 Ack=82 Win=2
```

```
da 22 00 08  e3 ff fd 90 08 00 45 00   ..'..".. ......E.
40 00 7c 06  24 6c 0a 14 38 b0 0a 57   .+.r@.|. $l..8..W
12 8e c4 14  43 e7 a7 a4 cf 05 50 18   ...B.... C.... P.
00 00 54 4c  53 00 00 00               ......TL S...
```

"TLS" or "TLSRPC"

Communication functions in rscd

- SSL_read()

```
(gdb) c
Continuing.

Breakpoint 1, 0x00007f85c9619c00 in SSL_read ()
   from /opt/bmc/bladelogic/NSH/lib/libblssl.so.0.9.8
(gdb) x/ls $rsi
0x7fffa66a83b0: "POST /xmlrpc HTTP/1.1\r\nHost: 172.18.1.21:4750\r\nContent-Length: 358\r\nC
ontent-Type: application/x-www-form-urlencoded\r\nAccept-Encoding: identity, deflate, compre
ss, gzip\r\nAccept: */*\r\nUser-Agent: python"...
(gdb)
```

- SSL_write()

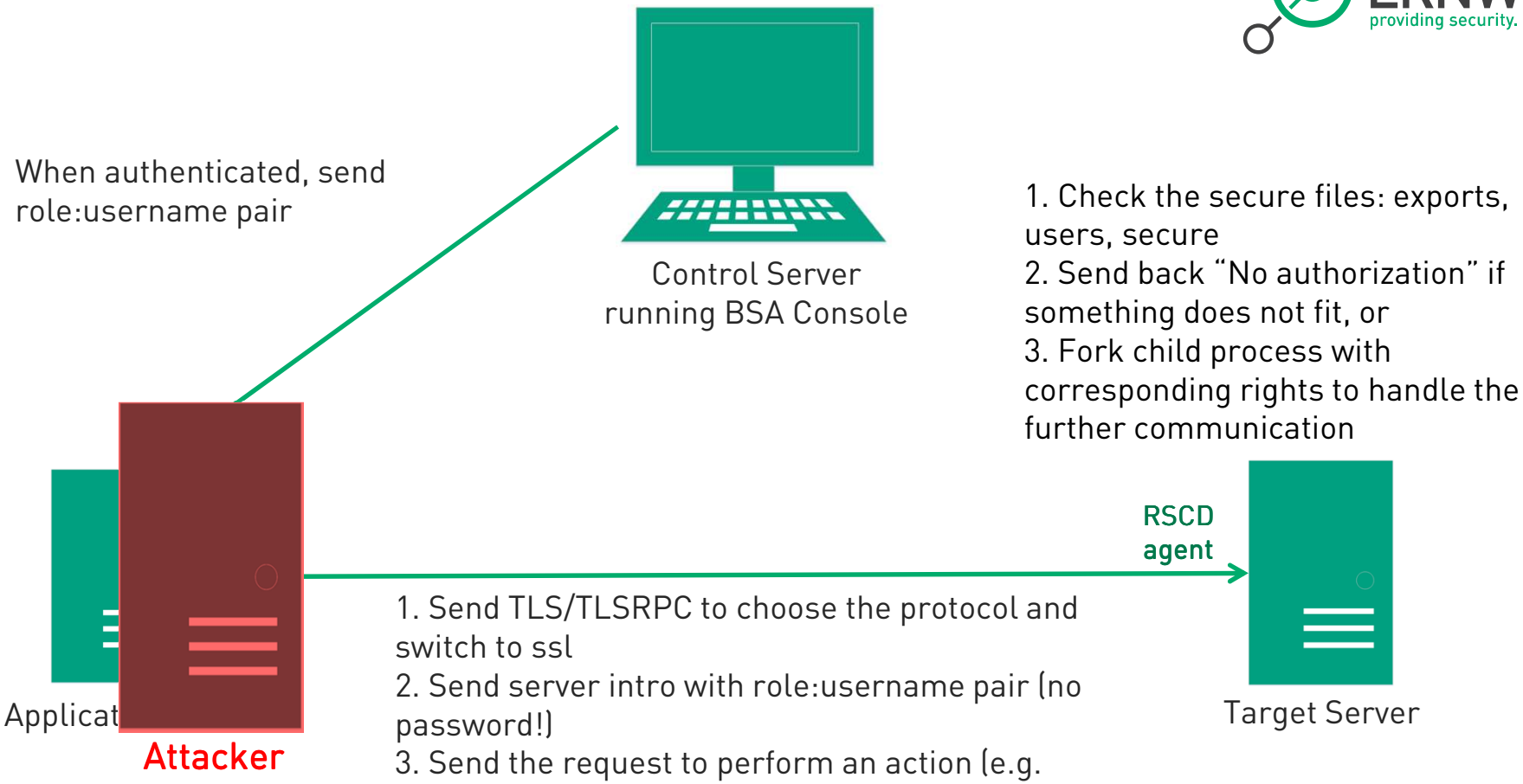
```
Breakpoint 2, 0x00007f0eeaf3ecc0 in SSL_write ()
   from /opt/bmc/bladelogic/NSH/lib/libblssl.so.0.9.8
(gdb) x/ls $rsi
0x94ba18:       "HTTP/1.1 200 OK\r\nServer: XMLRPC++ 0.7\r\nContent-Encoding: gzip\r\nConten
t-Type: text/xml\r\nContent-length: 197\r\n\r\n\037\213\b"
(gdb)
```

Pin tool

- Pin: dynamic binary instrumentation framework
- Pintools contain C++ code
- We used it to dump communication of the functions SSL_read() and SSL_write() mentioned before

Result

- TLS case
  - Some proprietary binary protocol
  - Paddings, number of symbols to read, some values…
- TLSRPC case
  - XMLRPC protocol
  - XMLRPC++ 0.7 server used in the agent
  - POST requests with XML body


When authenticated, send role:username pair
Control Server running BSA Console
1. Check the secure files: exports, users, secure
2. Send back "No authorization" if something does not fit, or
3. Fork child process with corresponding rights to handle the further communication
RSCD agent
Applicat
Attacker
1. Send TLS/TLSRPC to choose the protocol and switch to ssl
2. Send server intro with role:username pair (no password!)
3. Send the request to perform an action (e.g. update the password of a system user)
Target Server

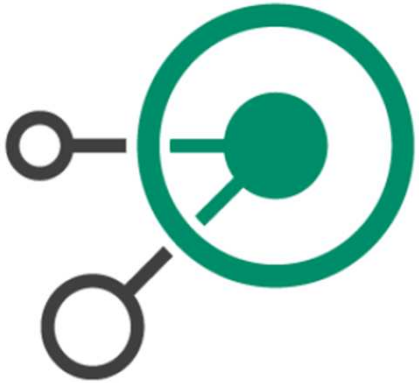
Summary

- Remote password change
  - Password of any user including root
  - No need to know the previous password
- User enumeration
  - Get information on all the system users
- No authorization needed!
- RCSD is not the one who decides to continue or not

BMC Software is alerting users to a security problem in the RSCD agent on UNIX® and Linux platforms for **all** versions of BMC Server Automation, as well as in any BMC solution that includes this technology. This topic includes the following

What's now?

- We reached the vendor
- BMC approved the issue and developed the patch
  - We can only confirm it works on our set-up
- CVE-2016-1542 and CVE-2016-1543 were assigned
- Thank you BMC for supporting responsible disclosure!



THANK YOU