Your Independent HP Business Technology Community

Setting up a secure PATHWAY environment

Closing the most dangerous backdoor to your NonStop system

Carl Weber
GreenHouse Software & Consulting

NS-06-NH, 10. Nov 2008, 14:30 – 15:25
Room Name: Ignaz Holzbauer 4

Intro

- Carl Weber
  - 1978 – 1994 Tandem Germany
  - 1994 – today GreenHouse
  = 30 years on the best platform available
- Specialized in security and system software
  - Security Reviews
  - Security Product Development
  - Security related Gift-, Free-, Share- and PayWare

Why is PATHWAY the ideal back door?

- To find security attributes, you need to know, that they exists – and plenty of time, to find them in the documentation.
- Still (H06.12) wrong default security settings
  (shame on Tandem ...)
- You probably have NO clue what might go wrong
  (do you understand OWNER, SECURITY, CAID, PAID, Process_Create_ etc.?)
- Easy to discover, and (mis-)use
  (ANY interactive TACL is sufficient)

PATHWAY external Security

The ID, used to start PATHMON, becomes the CAID and PAID, and is the base for all subsequent security relevant actions

Process Access ID (PAID) is used and propagated by PATHMON to

- Start processes (Servers, TCP's)
- Check file access (e.g. open)

PATHWAY internal Security

Two security attributes

- Owner, e.g. 100,5
- Security, e.g. “O”

are available for

- Programs (semi critical)
- Server process (critical)
- PATHMON process (highly critical)

PATHWAY Program

- Owner and Security defines the execution rights on a PATHWAY program, started by a PATHCOM RUN command.
- Not critical, in case the application has its own authentication system (highly suggested).
- When no authentication system available, set it to:
  - Owner = PATHMON owner
  - Security = “O”

PATHWAY Program Owner

- **`owner-id`** specifies the user ID authorized to issue the RUN PROGRAM command. The user ID must be known to the system on which PATHCOM is running. Use this attribute in conjunction with the SECURITY attribute.

PATHWAY Program Owner

- The value of **owner-id** is one of the following:
  [\system-number.]group-number,user-number
  [\node.]group-name.user-name

PATHWAY Program Security

- SECURITY **`security-attribute`** specifies the PATHCOM users who can issue a RUN PROGRAM command for this PROGRAM object. This attribute controls only who can execute a RUN PROGRAM command; it does not control who can execute a CALL statement from another SCREEN COBOL program unit.
- **`Security-attribute`** is one of **`A,G,O,-,N,C`** or **`U`**
- If you omit this attribute, the default is **`"N"`**.

PATHWAY Servers

- GUARDIAN process
- PAID used to check access to data

- Owner and Security defines access rights to a PATHWAY server through PATHSEND.

PATHWAY Server Owner

- OWNER-ID specifies the user ID that controls access from a PATHSEND process to a server class (the TCPs ignore this server attribute).
  The user ID must be known to the system in which PATHCOM is running.
  Use this attribute in conjunction with the SECURITY attribute.

PATHWAY Server Owner

- The value of **owner-id** is one of the following:
  [\system-number.]group-number,user-number
  [\node.]group-name.user-name

PATHWAY Server Security

- SECURITY **`security-attribute`** specifies the users, in relation to the OWNER attribute, who can access a server class from a PATHSEND requester. (TCPs ignore this attribute.)
- **`Security-attribute`** is one of **`A,G,O,-,N,C`** or **`U`**
- If you omit this attribute, the default is **`"N"`**.

PATHWAY Server Security

- When no PATHSEND is needed/allowed, close this access path!
  e.g.
  - Owner = PATHMON owner
  - Security = “O”

PATHWAY Monitor

- PAID

- Owner
- Security

PATHWAY Monitor - PAID

- Passed on by the starting ID
  - prevent SUPER.SUPER from starting PATHWAY applications – except you know, what you do

- PAID is propagated to all processes, started from PATHMON
  - independent of a possibly defined PATHWAY Owner

PATHWAY Monitor Owner

- Defines the owner, allowed to manage PATHMON - add/delete/start of subsystems
- Can be different from the PAID

PATHWAY Monitor Security

- SECURITY **`security-attribute`** specifies the users, in relation to the OWNER attribute, who can manage a PATHMON.
- **`Security-attribute`** is one of **`A,G,O,-,N,C`** or **`U`**
- If you omit this attribute, the default is **`"N"`**.

Security Attributes

- Can only be set or changed with a cold load!

What might go wrong?

- Manipulation of PATHWAY system
  - shut down
- Manipulation of information
  - change, delete
- Disclosure of information
  - copy
- Compromising the entire system
  - getting access to everything

What might go wrong?

- Access to SERVERS by PATHSEND
  - manipulation of the data base
  - disclosure of information

What might go wrong?

- Worst case: Management access to PATHMON
  - manipulation of the PATHWAY system

    e.g. shut-down = DoS
  - manipulation of servers (add, delete, replace)
  - read/write access to the data base

    e.g. through introduced servers like FUP. SQLCI etc.

What about LOG1 and LOG2 logging?

- Forget about it …
  LOG1 and LOG2 do NOT report security critical events, such as the add, start and delete of a server.

- No audit – no security …

Find the back door

- **`STATUS *,PROG $SYSTEM.SYS*.PATHMON`**
  displays all PATHWAY systems

- **`STATUS *,PROG $SYSTEM.SYS*.PATHMON,user SUPER.SUPER`**
  displays all PTHWAY systems with a potential threat to the system

Exhaustive PATHWAY search made easy

- **GETPWSS**
  displays all security attributes of all PATHWAY systems including my security estimation (http://www.greenhouse.de/freeware)

Show time

- Find a weak PATHWAY system and compromise the system
- Harden the weak PATHWAY system and prevent the problem

Show time

- System is
  - \GINKGO
  - Type NS1002
  - GUARDIAN version H06.12
- Connection is by LAN/WLAN/UMTS using VPN

Suggestions

- Never start a PATHWAY system using SUPER.SUPER, except you know what you do
- Never make use of the security default “N”, but set the security attributes as tight as possible to “O”
- Use one GUARDIAN group for all PATHWAY systems
- Do not share IDs, but make use of Command Level Security products to manage PATHWAY systems (add of auditing)

Suggestions

- Use one user group (e.g. 100) for all PATHWAY systems
- Use IDs 0 .. 255 for up to 256 individual PATHWAY systems

Suggestions

- e.g.:
  - PATHWAY application 0 = PAID of 100,0
  - PATHWAY application 1 = PAID of 100, 1
  etc.

which allows >>>

Suggestions

>>> a security of

- “O”
  for an isolated local PATHWAY system (no PATHSEND)
- “G”
  for a communicative system (PATHSEND between PATHWAY systems)
- “U”
  for an isolated network PATHWAY system
- “C”
  for a communicative network system (PATHSEND between PATHWAY systems)

Suggestions

- In case access to remote PATHWAY systems is required:
  - run PATHMON's with an ID (PAID), that has remote passwords
  - freeze that User/ID to prevent individual access
  - set the security to "U"/"C"

Suggestions

- Optional set an ACL on the PATHMON name
  - controls access to the entire PATHWAY system!

General

- Do not license objects, or set the PROGID flag – except there is a reason

PATHWAY System deliveries you should demand

- Configuration files
- Program code (POBJ and servers)
- Documentation

- **Security settings for EVERYTHING, that makes the PATHWAY application**

- **P.S.: Make sure PATHTCL is secured to OOOO and owned by the PATHMON PAID**

Thanks for listening!

Questions?

You can reach me at:
Carl.Weber@GreenHouse.de

The tools are available at:

www.GreenHouse.de