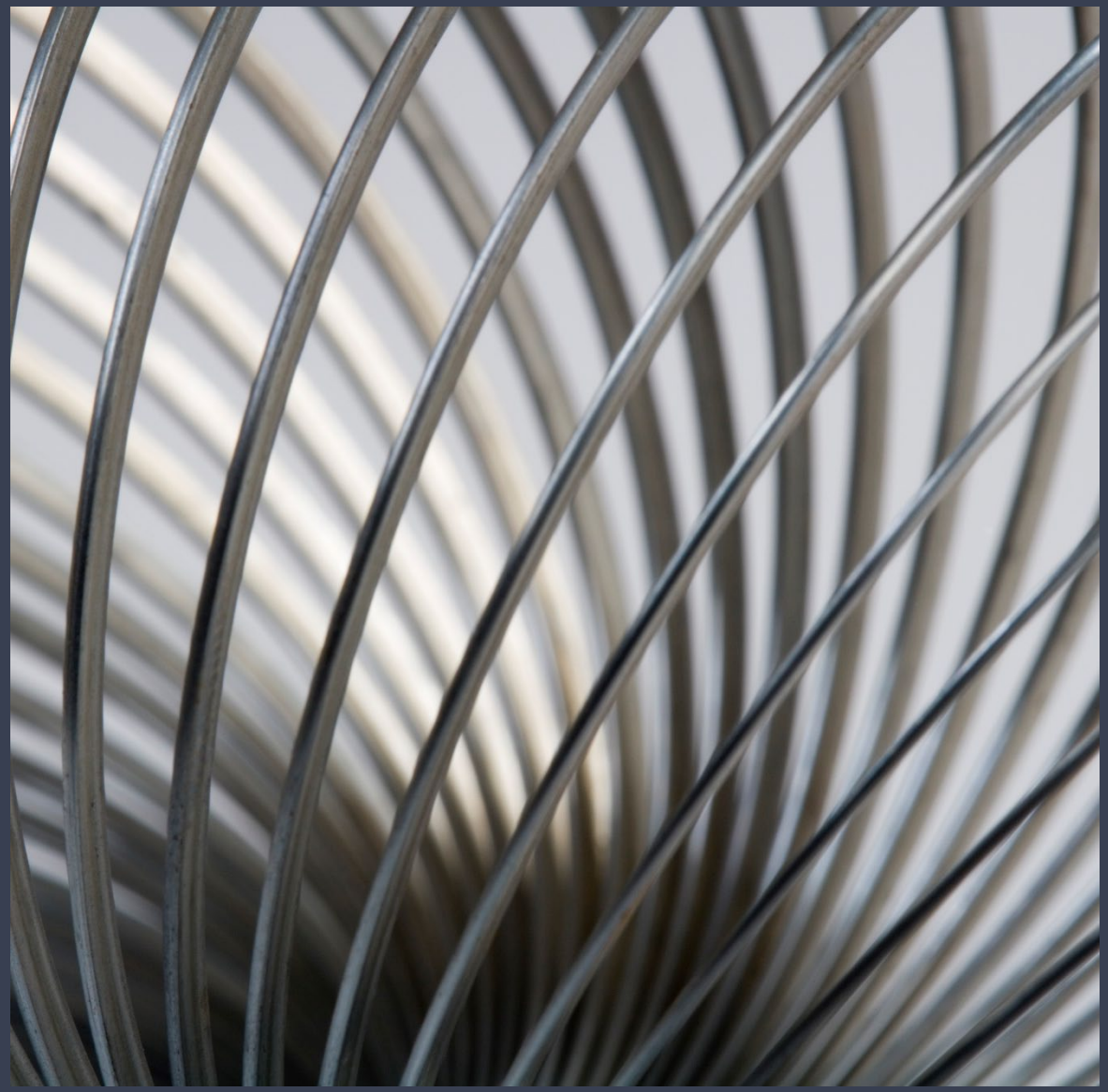
NUGM 2024

MANAGE 2000 APPLICATION SECURITY



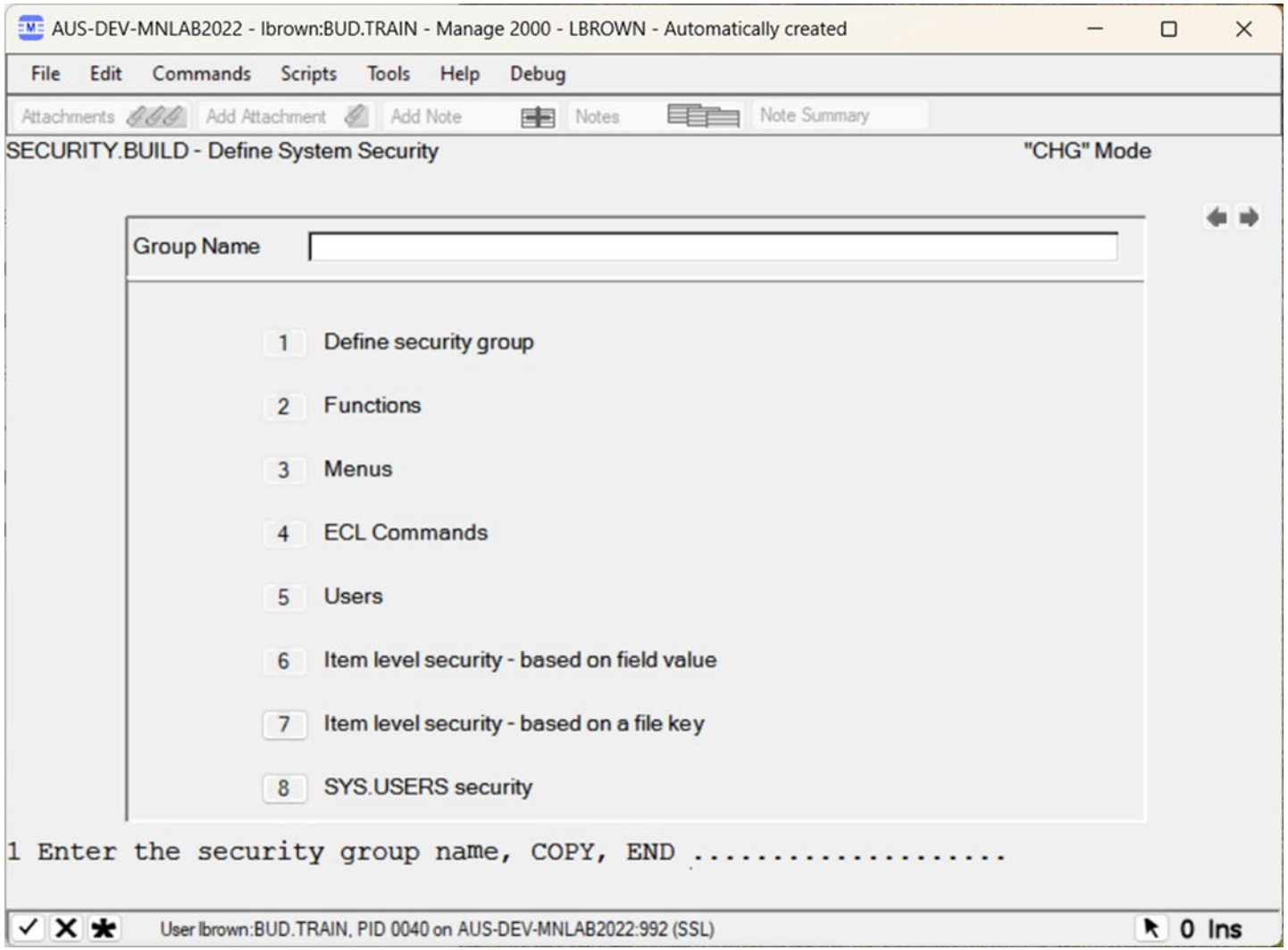
Bud Brown, Epicor Software

AGENDA

- How Security Works
- Menu Security
- Menu structure
- Menu Security exceptions
- Function Security
- Locking down backdoors
- Field Level Security
- TCL Security
- \SD to show why security failed
- Why not to use ALL when setting up security
- Best Practices
- There are 6 handouts that show step by step instructions for doing everything in this presentation, so notes do not need to be taken

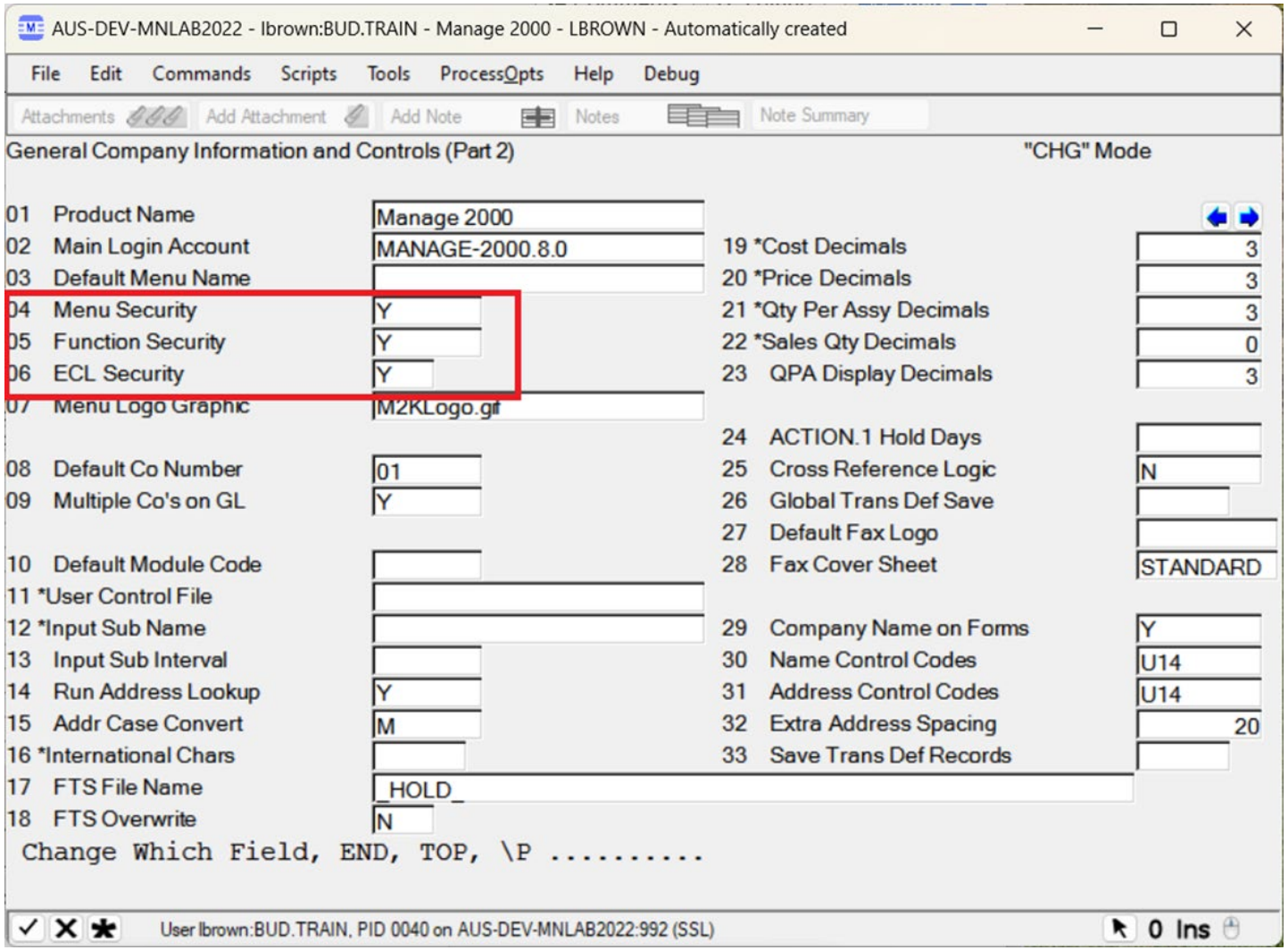
HOW SECURITY WORKS

- A security group grants the users in the group access to the functions and menus listed
- Users not in this security group are locked out of those functions and menus



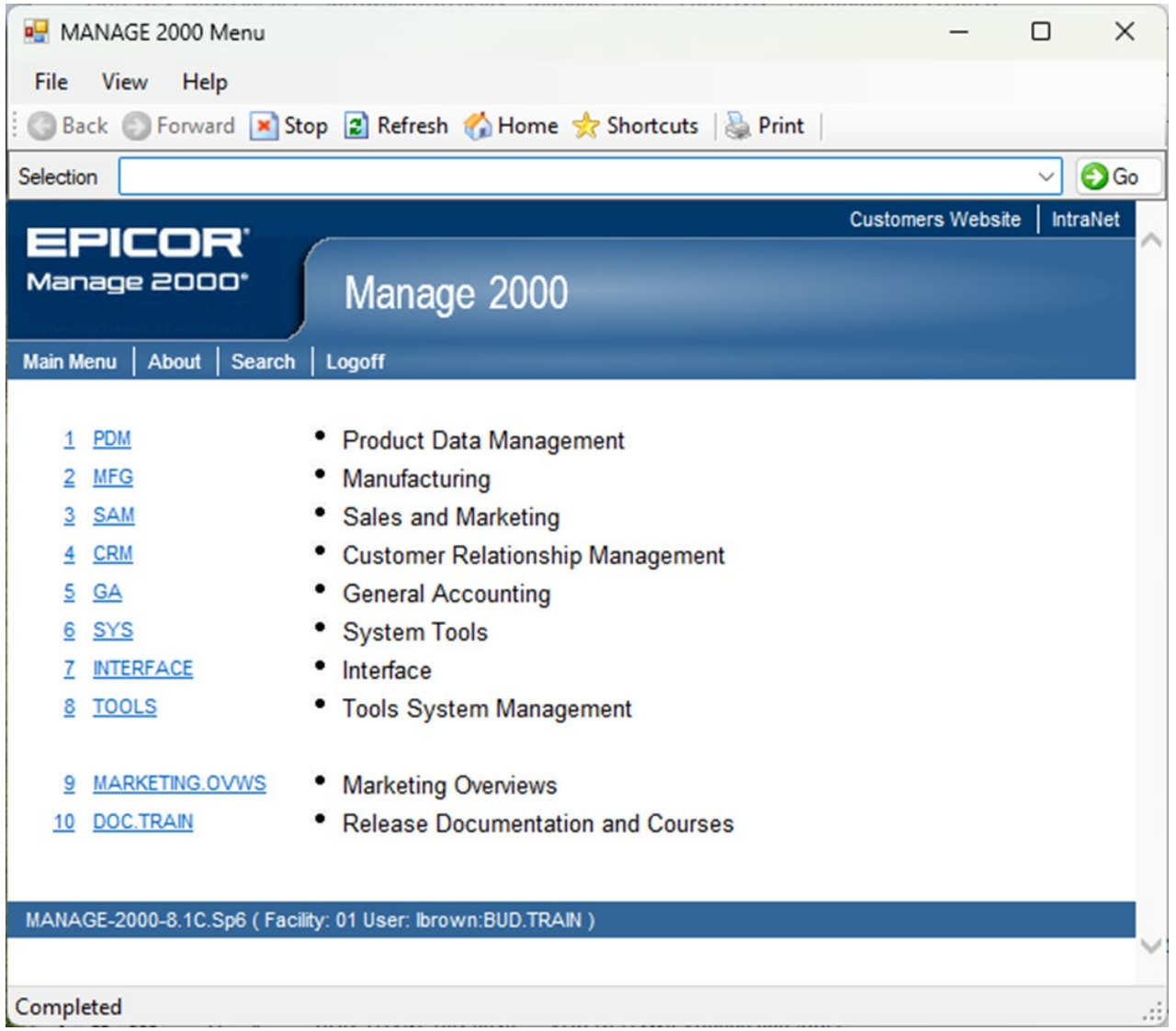
TURNING ON/OFF SECURITY

- Menu, Function and TCL/ECL security can be turned on/off in COMPANY.NAME screen 2



MENU SECURITY

- The menu system is like a tree
- The trunk of the tree is the MANAGE-2000 menu – PRINT.MENU.PATHS
- You can branch down to any submenu from here

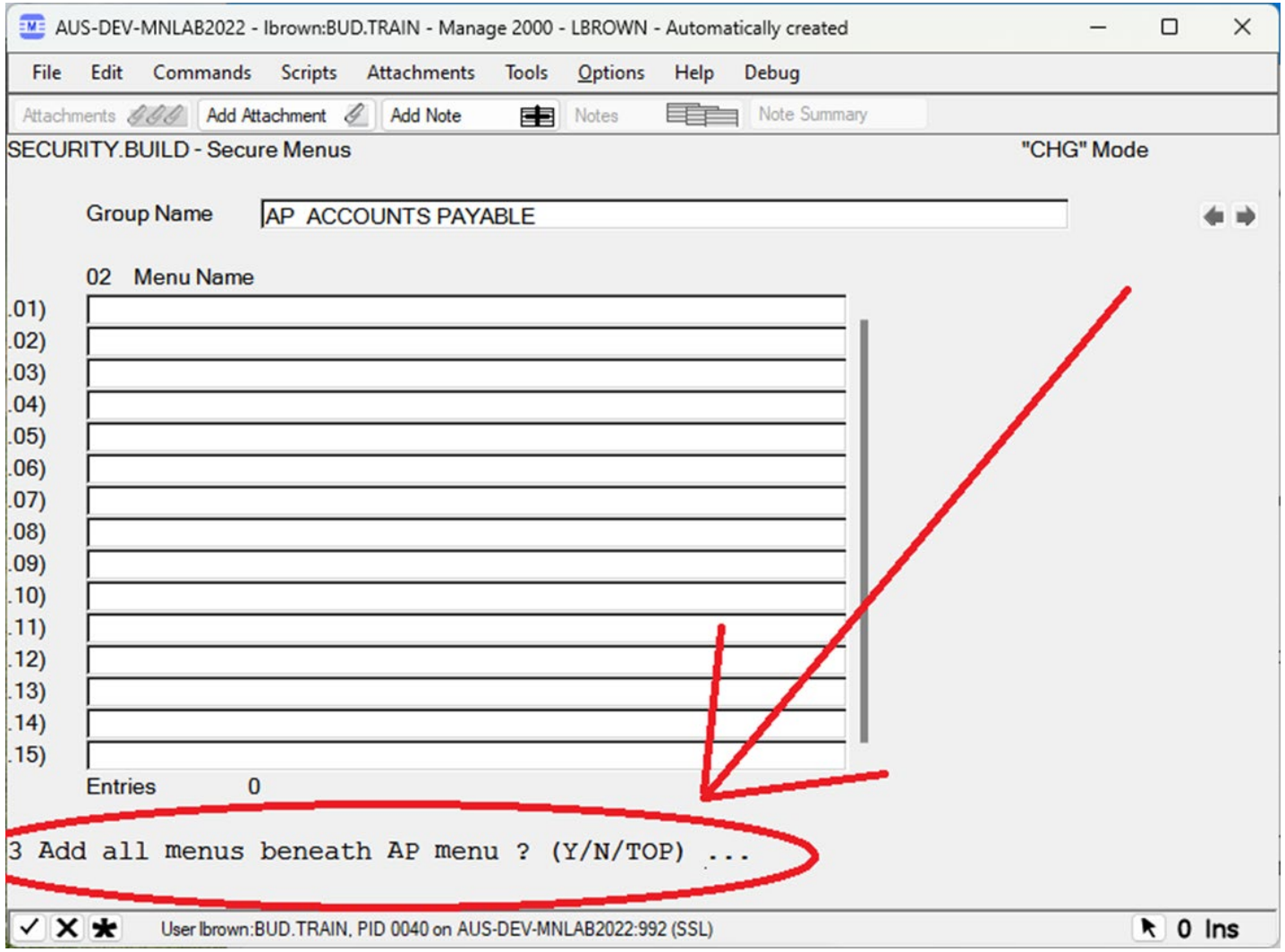


MENU SECURITY

- If I click on the GA (General Accounting) menu, everything under it is accounting related
- We can even branch down farther to AP (Accounts Payable) or AR (Accounts Receivable) and everything under these submenus are either AR or AP related

MENU SECURITY

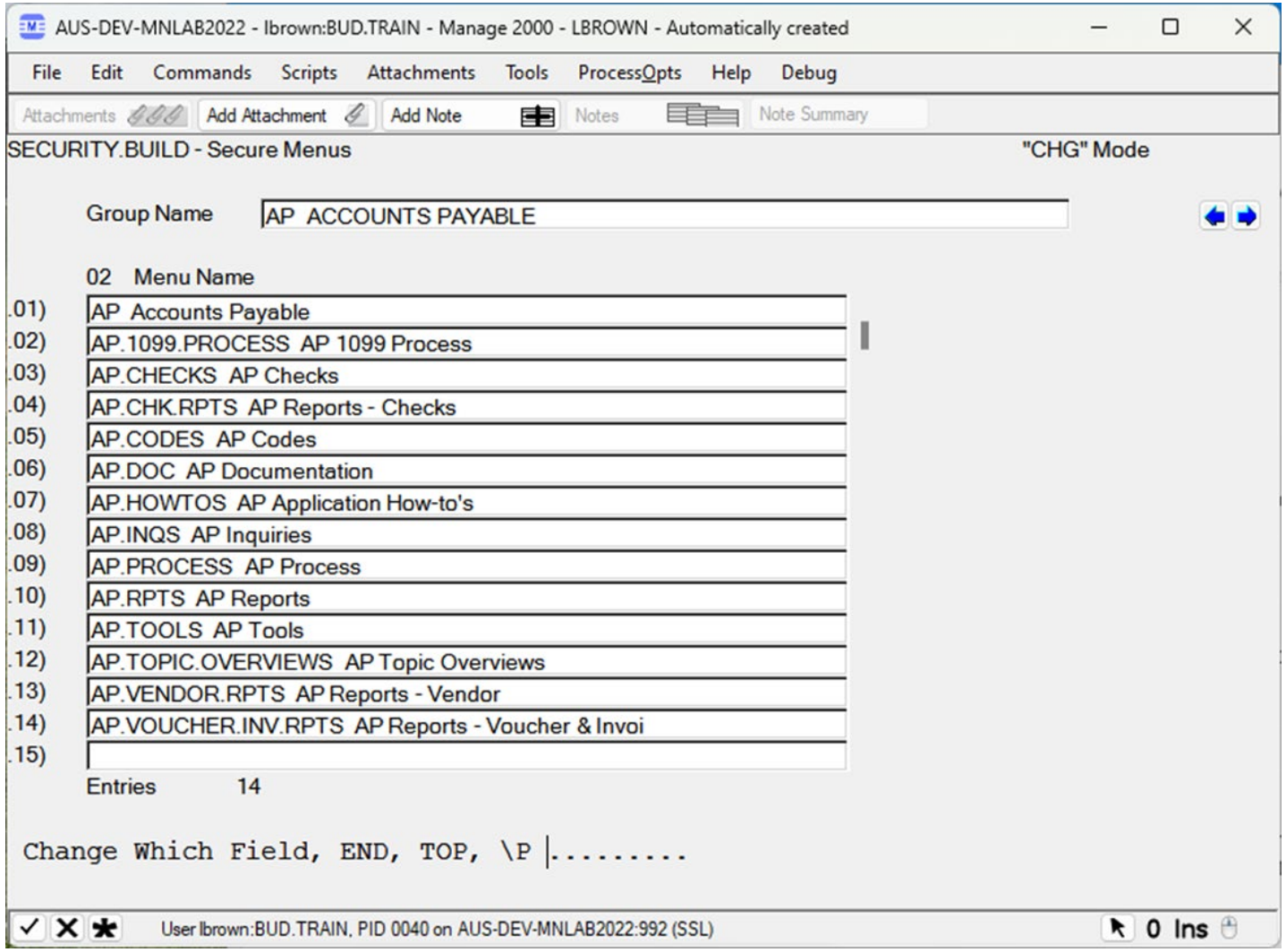
- Creating a security group in SECURITY.BUILD will automatically prompt us to add the sub menus
- If I put in the AP menu, it will prompt for submenus
- Now this security group will grant access to everything AP related



NovoRoi Systems, LLC

MENU SECURITY

- It will add all the submenus and now this security group locks down everything related to Accounts Payable

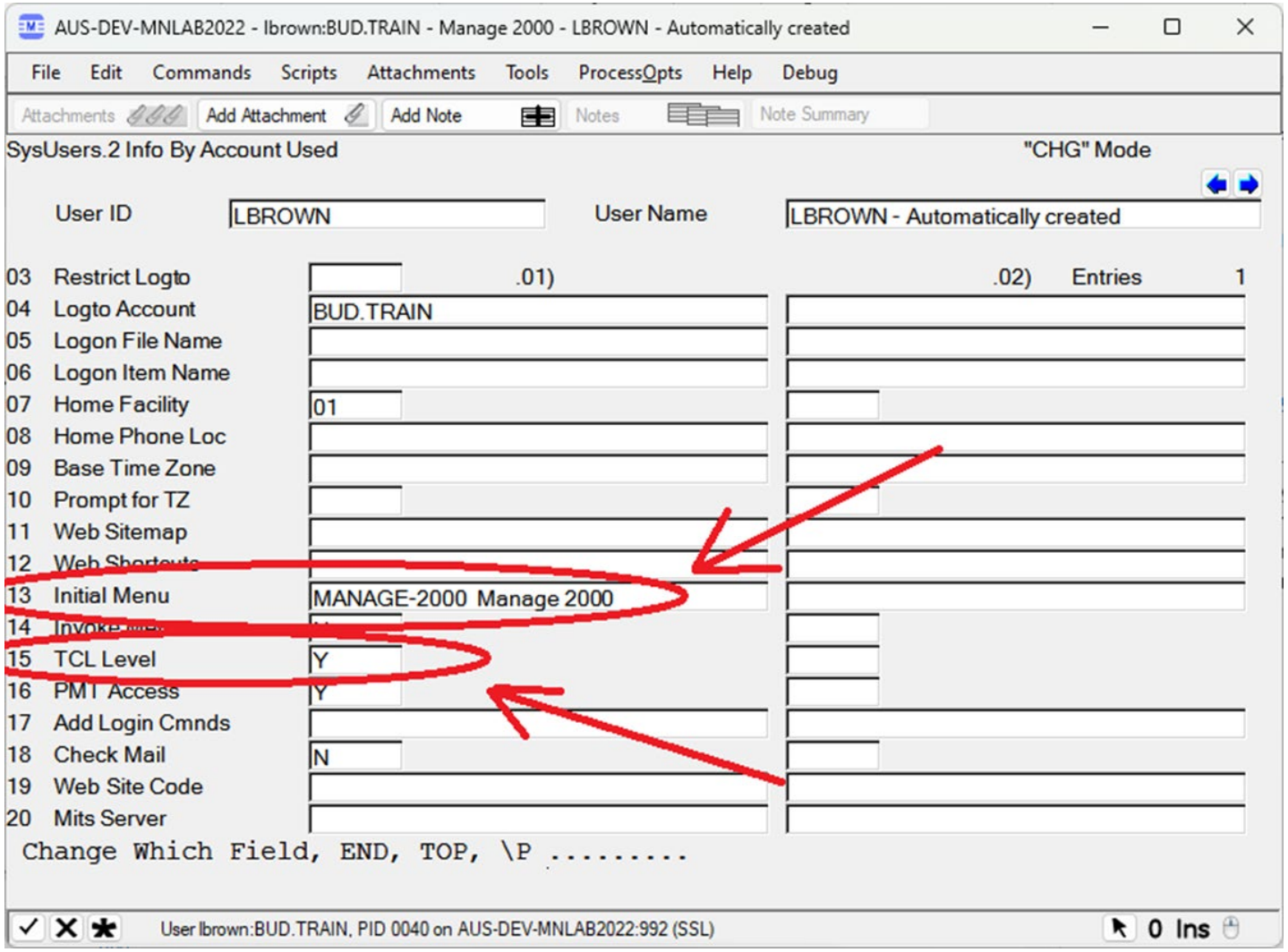


LOCKING DOWN A FUNCTION

- See Handout 1 for steps to lock down a function with Menu or Function Security

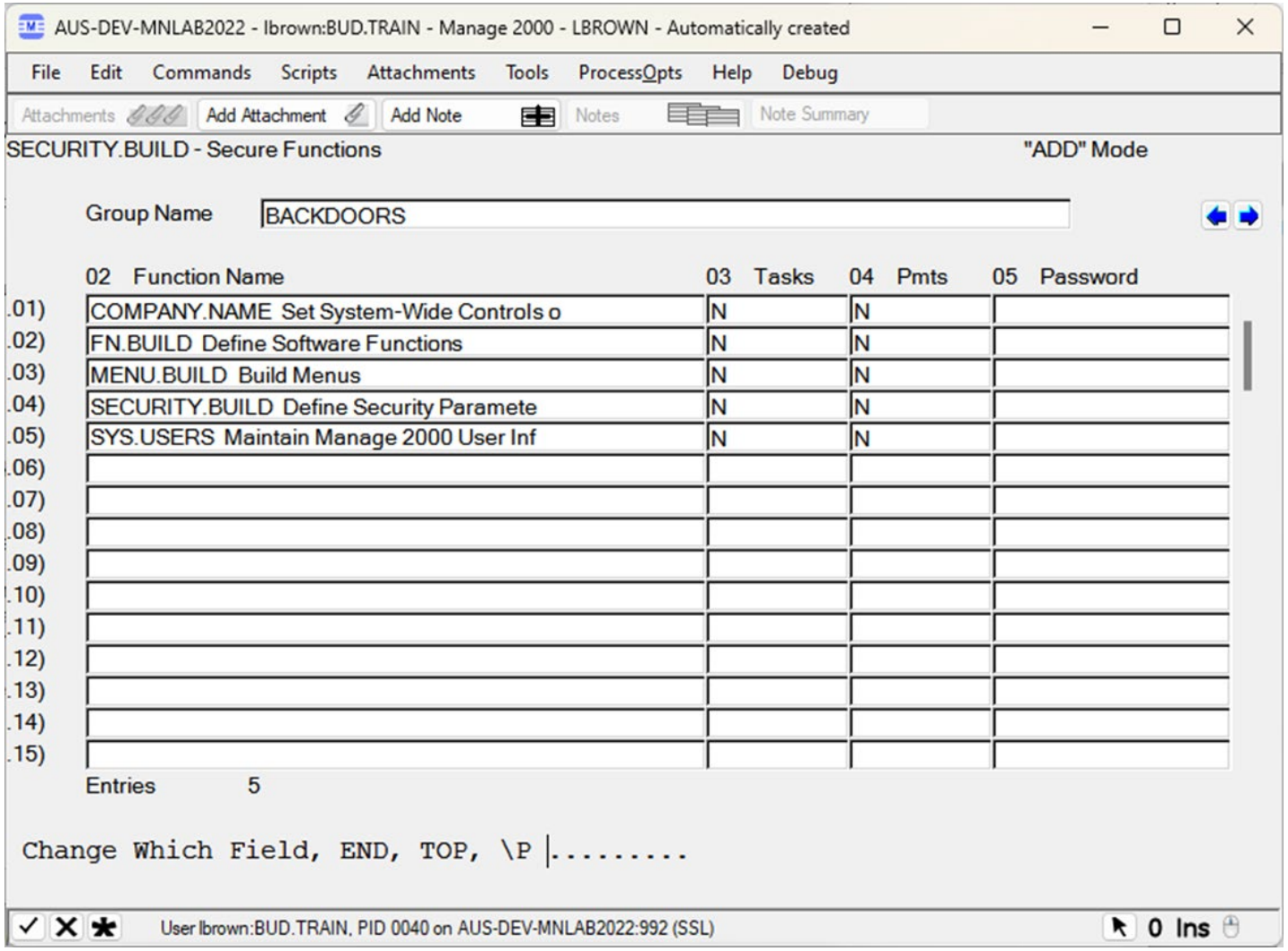
MENU SECURITY EXCEPTIONS

- Granting TCL Level in SYS.USERS makes a user immune to Menu Security
- Initial Menu set in SYS.USERS automatically grants access to that menu



FUNCTION SECURITY

- Very straight forward
- Just put in the functions
- Very slow
- Each function must be entered manually



LOCKING DOWN BACKDOORS

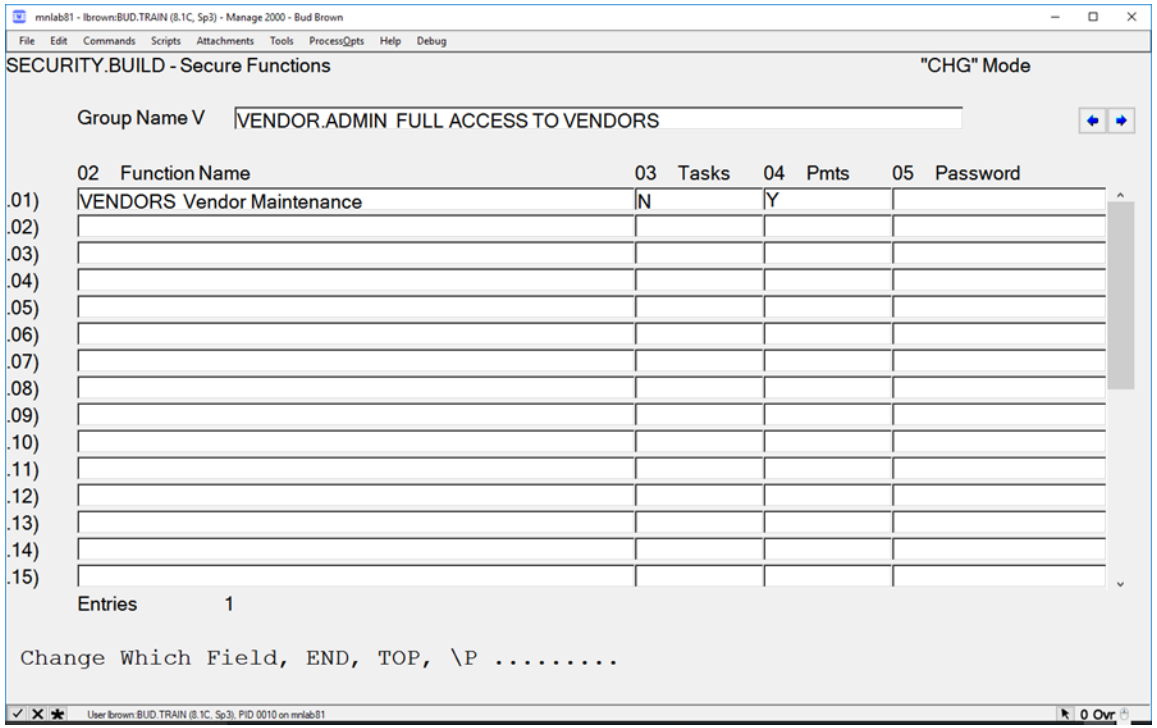
- Use Function Security to lock down backdoors
- COMPANY.NAME – Users can turn off security in COMPANY.NAME
- SYS.USERS – Users can set their Initial Menu
- FN.BUILD – Users can add themselves to access Functions
- MENU.BUILD – Users can add functions to their menus to gain access
- SECURITY.BUILD – Users can add themselves to security groups

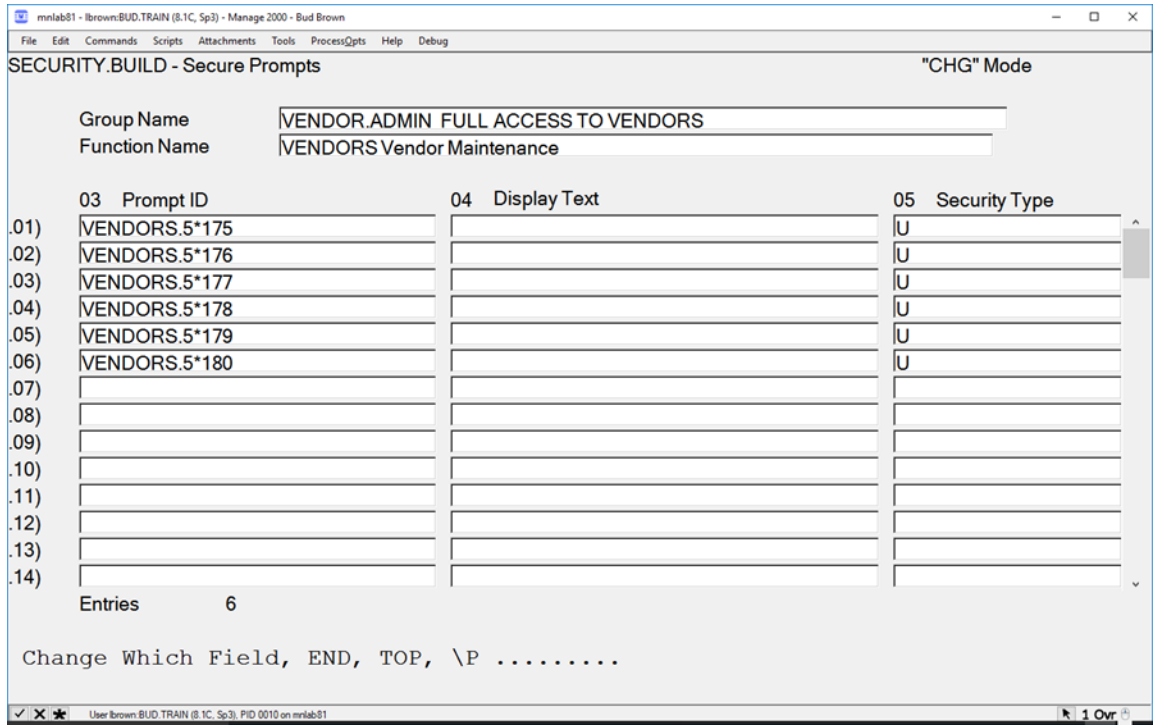
FIELD LEVEL SECURITY

- Field Level security was added in M2K 7.3 and above
- Gives the ability to Lock a field
- Gives the ability to hide data in a field
- See Handout 2

FIELD LEVEL SECURITY

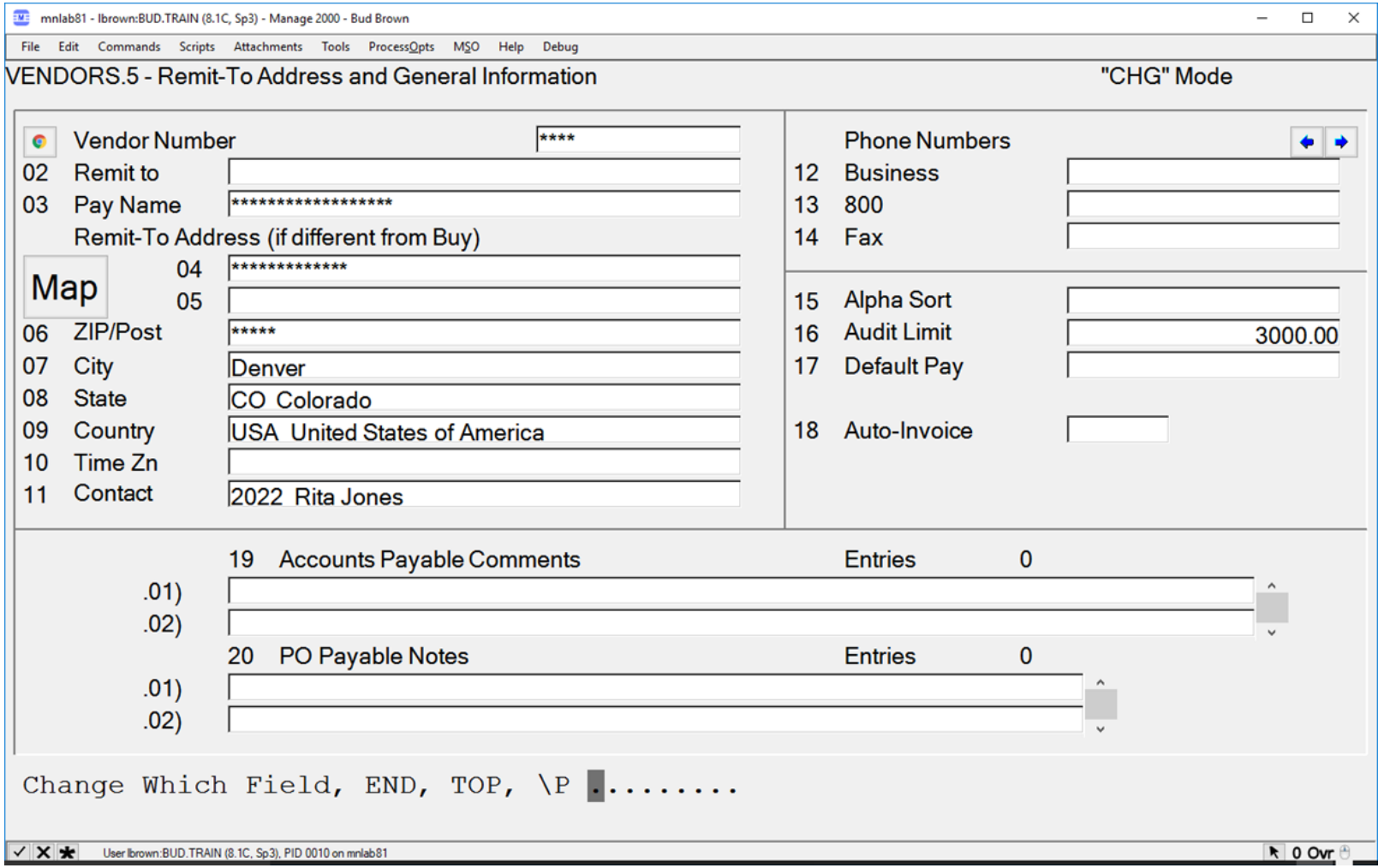
- First create an Admin security group and specify all fields to be locked down, but give this security group “Update” access
- Giving Update access to this Admin Security group locks other users from seeing or updating the field





FIELD LEVEL SECURITY

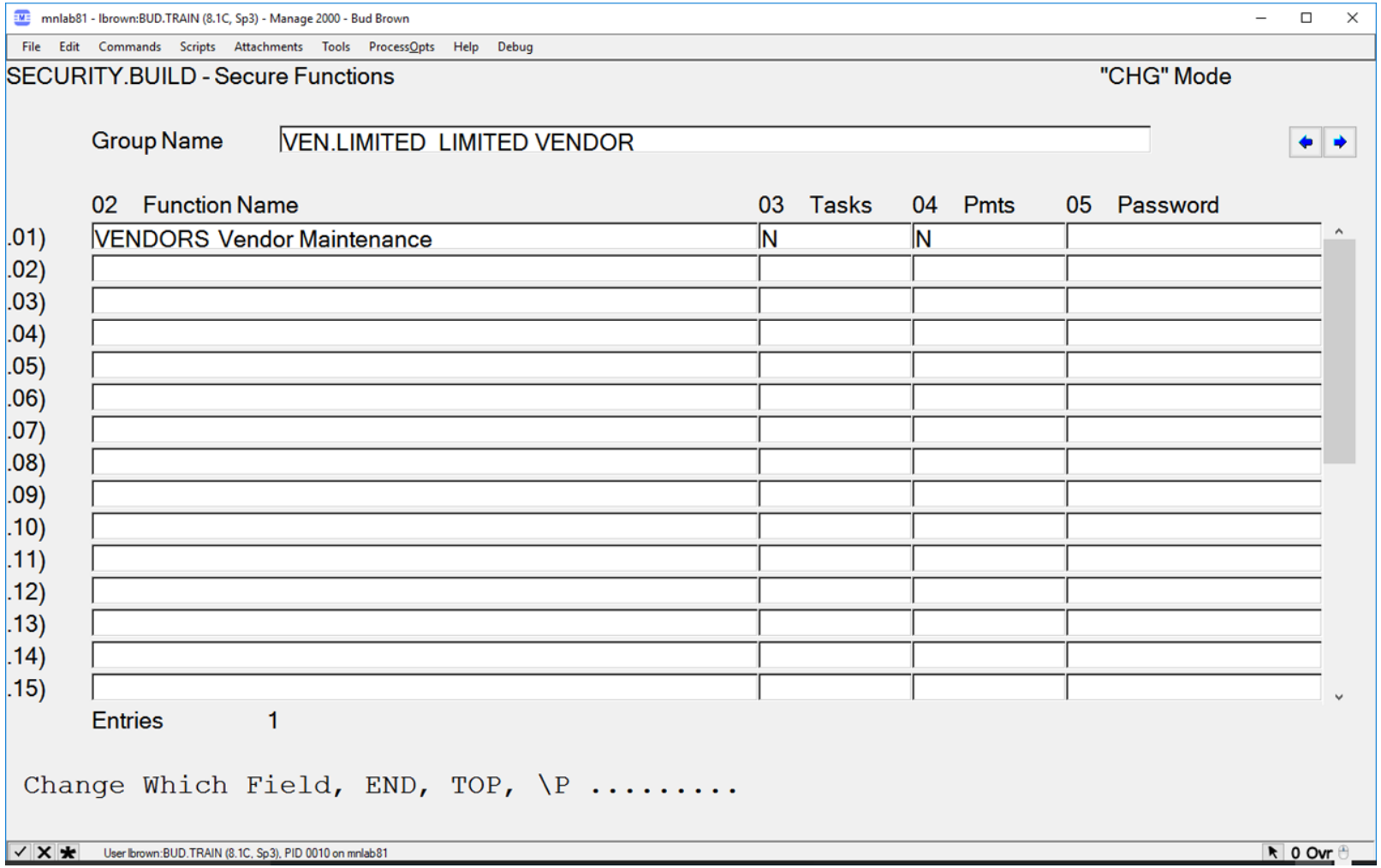
- Users who are not part of the security group can't see fields



NovoRoi Systems, LLC

FIELD LEVEL SECURITY

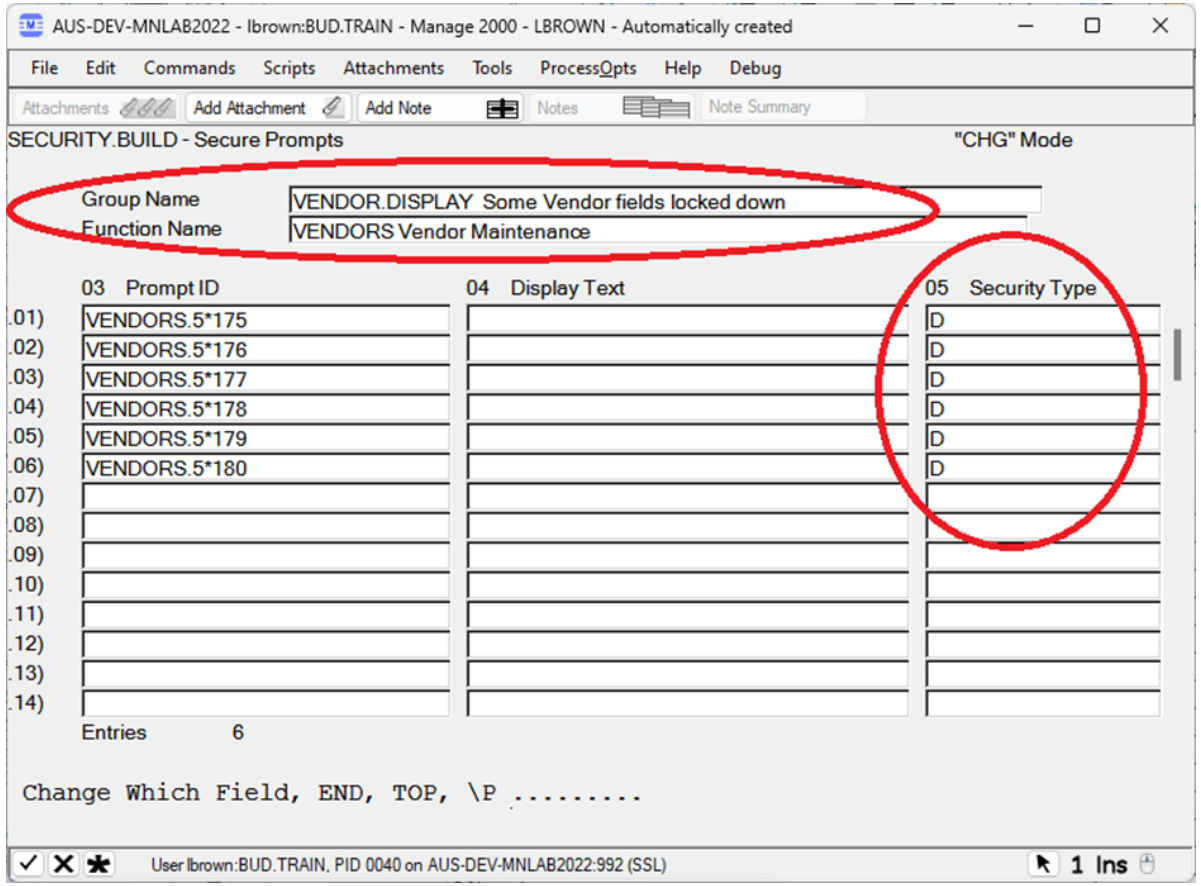
- A second security group will be needed to get the user into the function

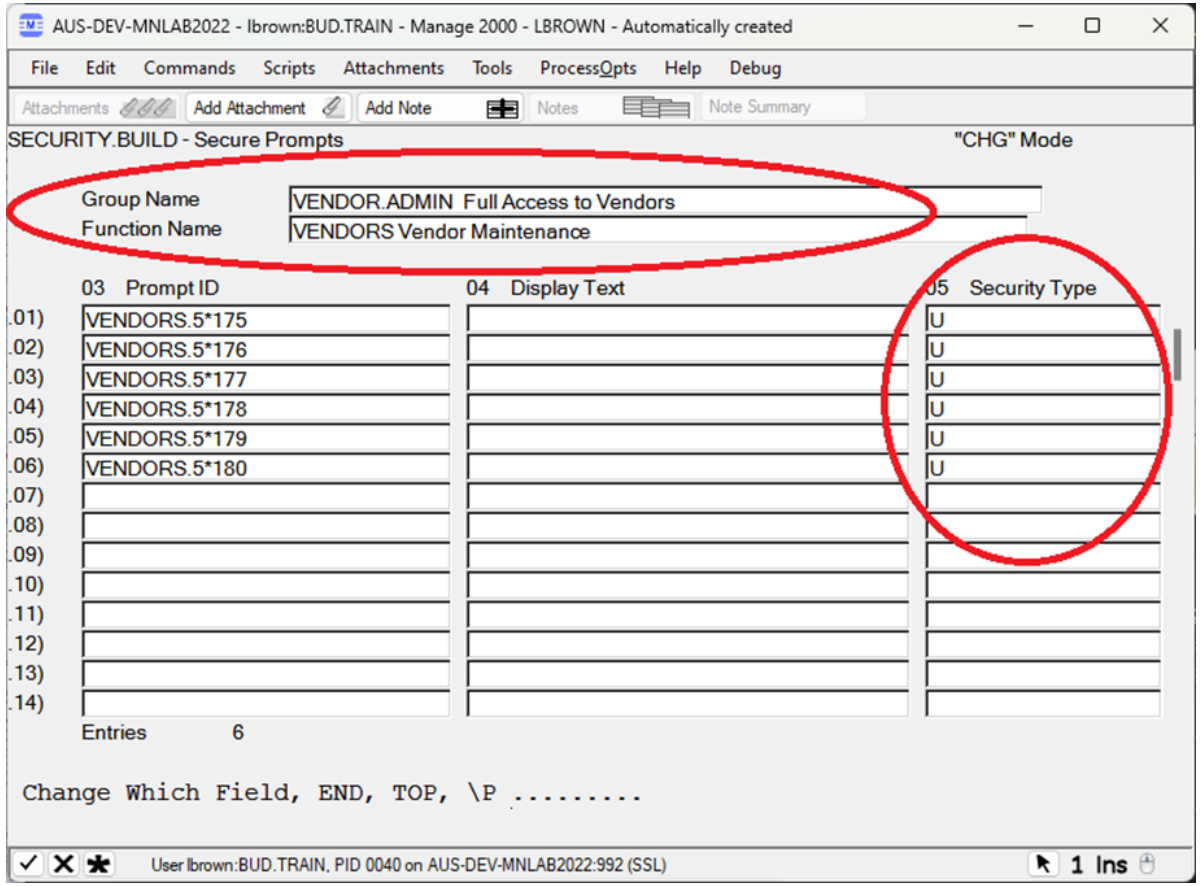


NovoRoi Systems, LLC

FIELD LEVEL SECURITY

- A third Security group can be created if some users need to see those fields but not update them



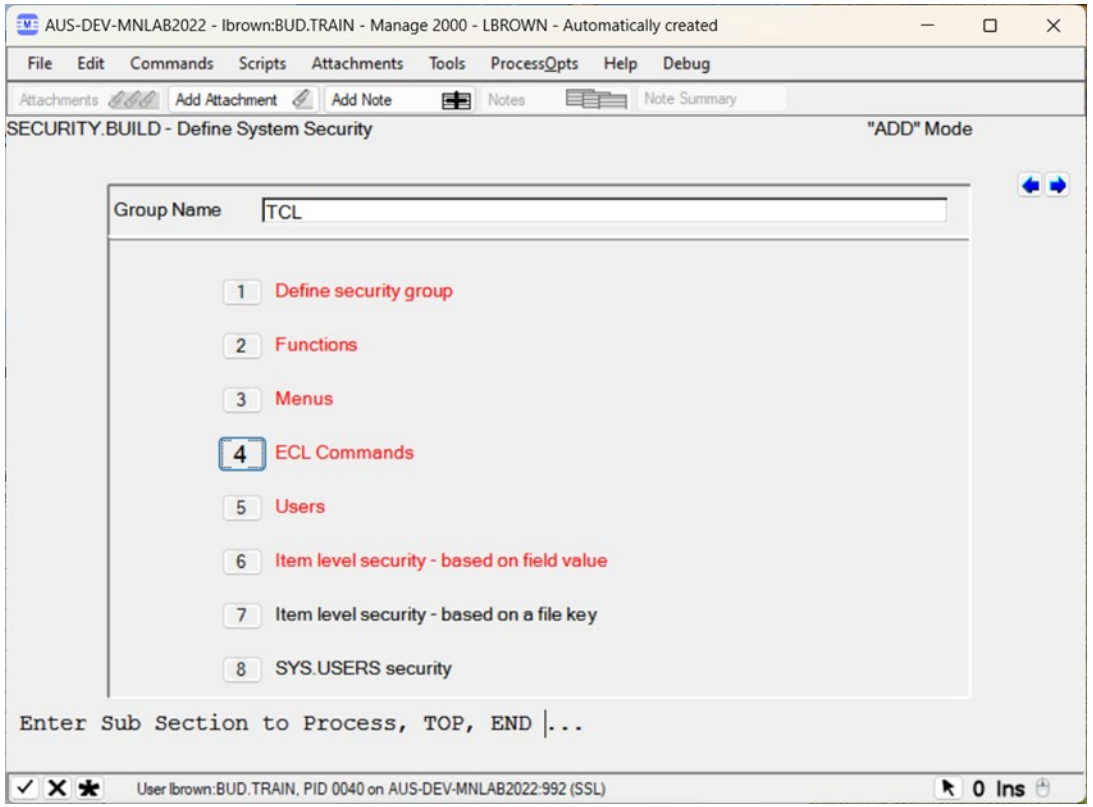


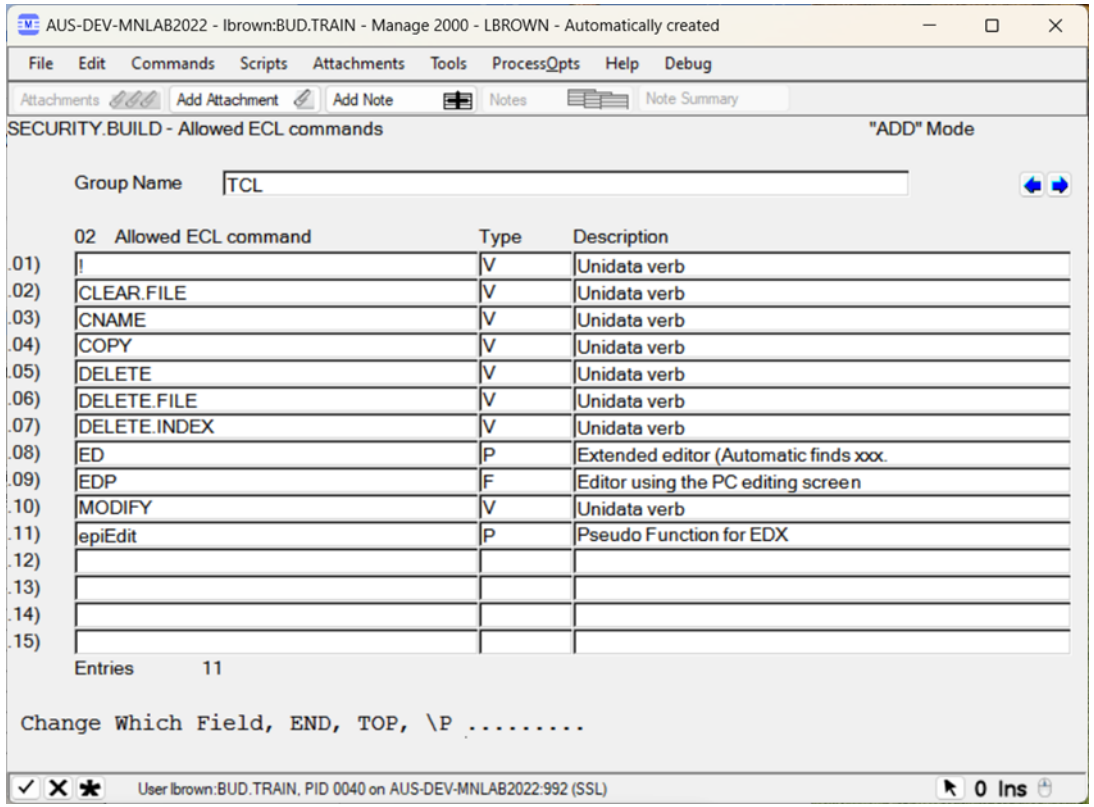
TCL SECURITY (AKA ECL SECURITY)

- Prevents users from using certain TCL commands at the TCL prompt
- Lock down the following at a minimum
- DELETE
- DELETE.FILE
- DELETE.INDEX
- CLEAR.FILE
- EDP
- ED
- MODIFY
- !
- COPY
- CNAME
- epiEdit
- See handout 3

TCL SECURITY

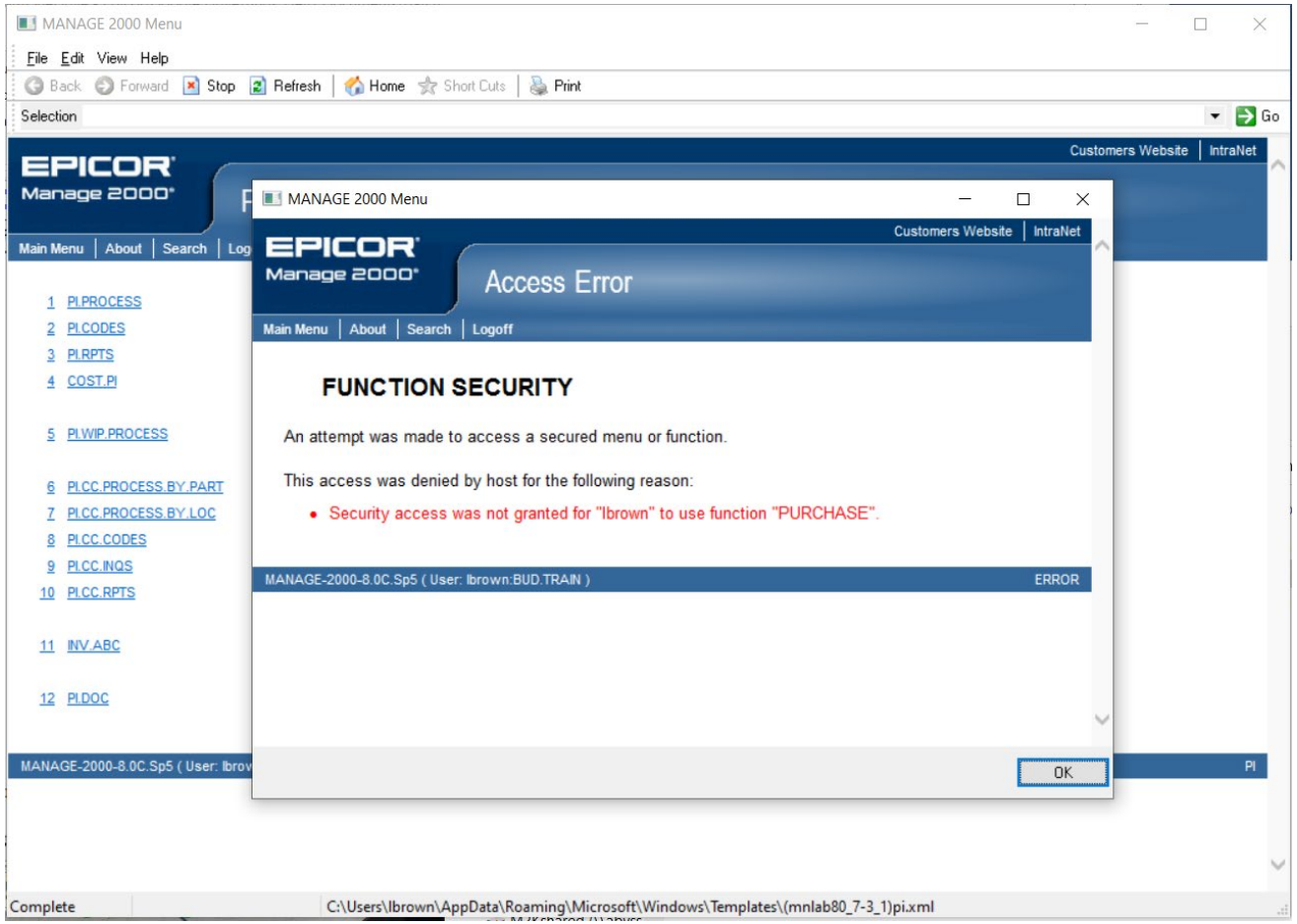
- TCL Security can be set in screen 4 of SECURITY.BUILD

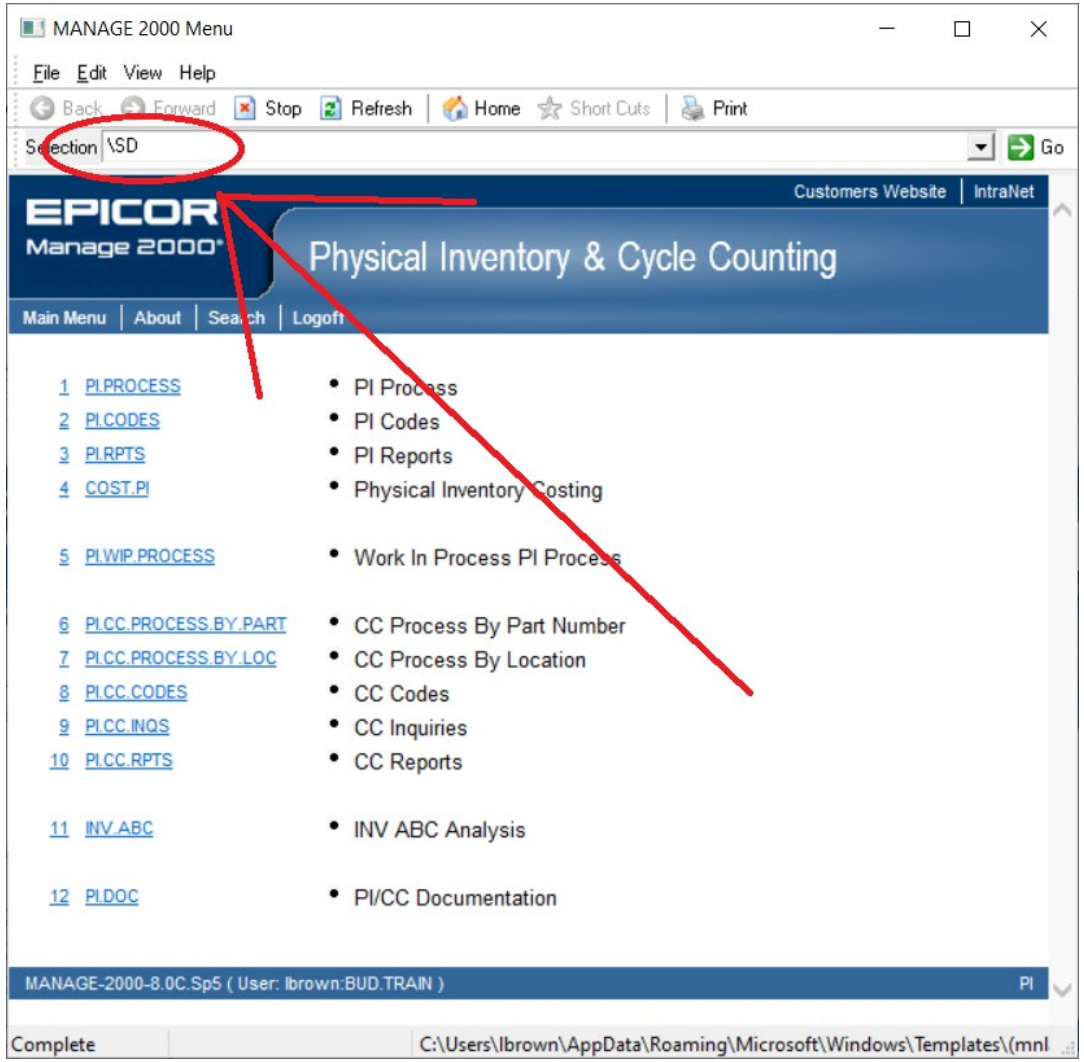


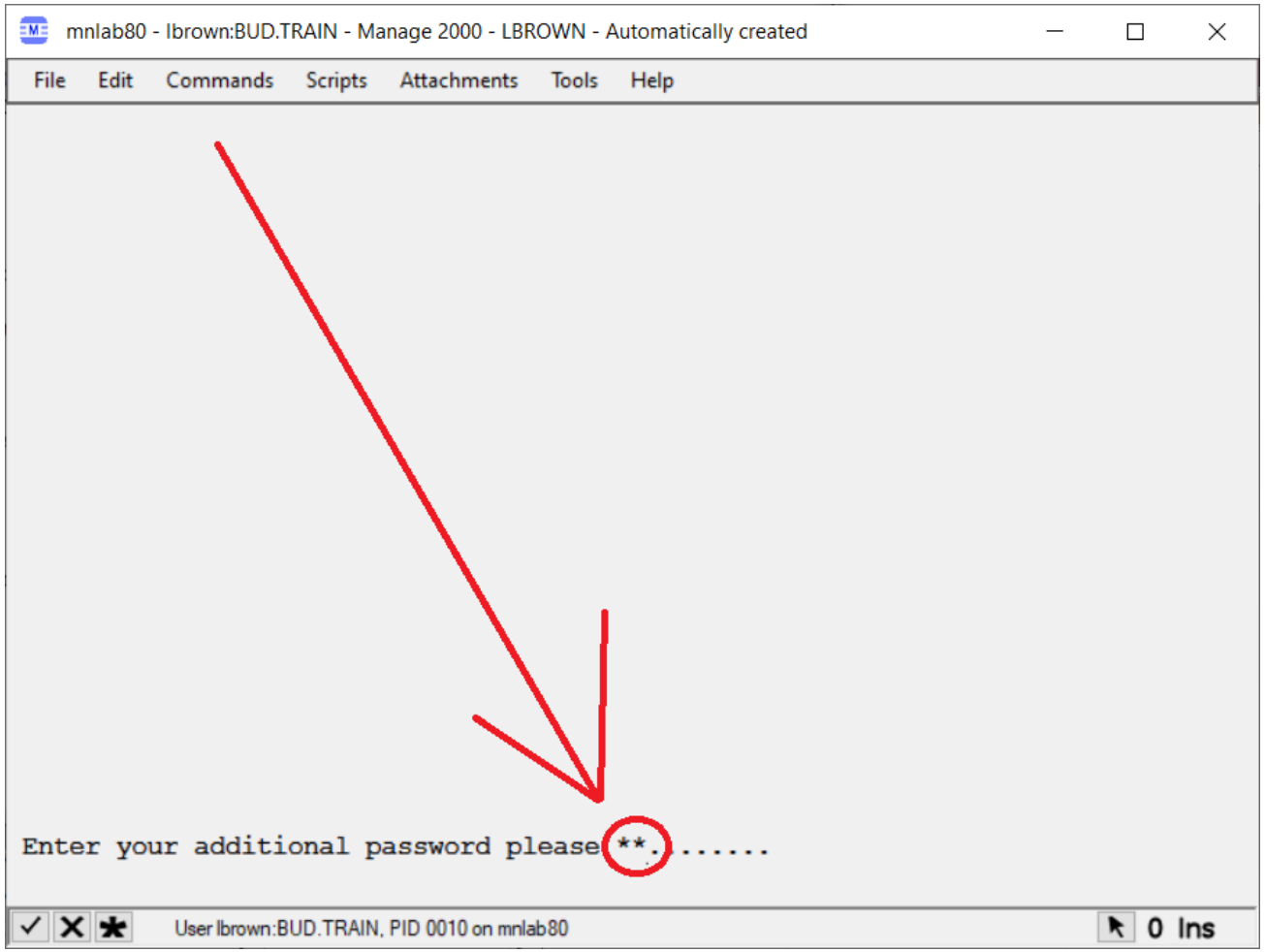


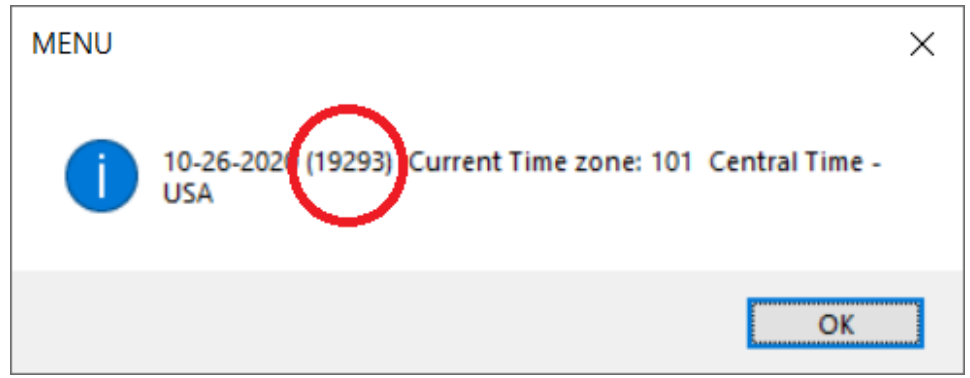
\SD TO SHOW WHY SECURITY FAILED

- After a user fails security, type in \SD at the menu
- User will be prompted for a password that is today's Internal Date
- Type in \D to find out current Internal Date
- A List-box will popup showing all security checks
- Select the one that says No Access and click OK
- The PWS Viewer will open and show why the user failed security
- See Handout 4

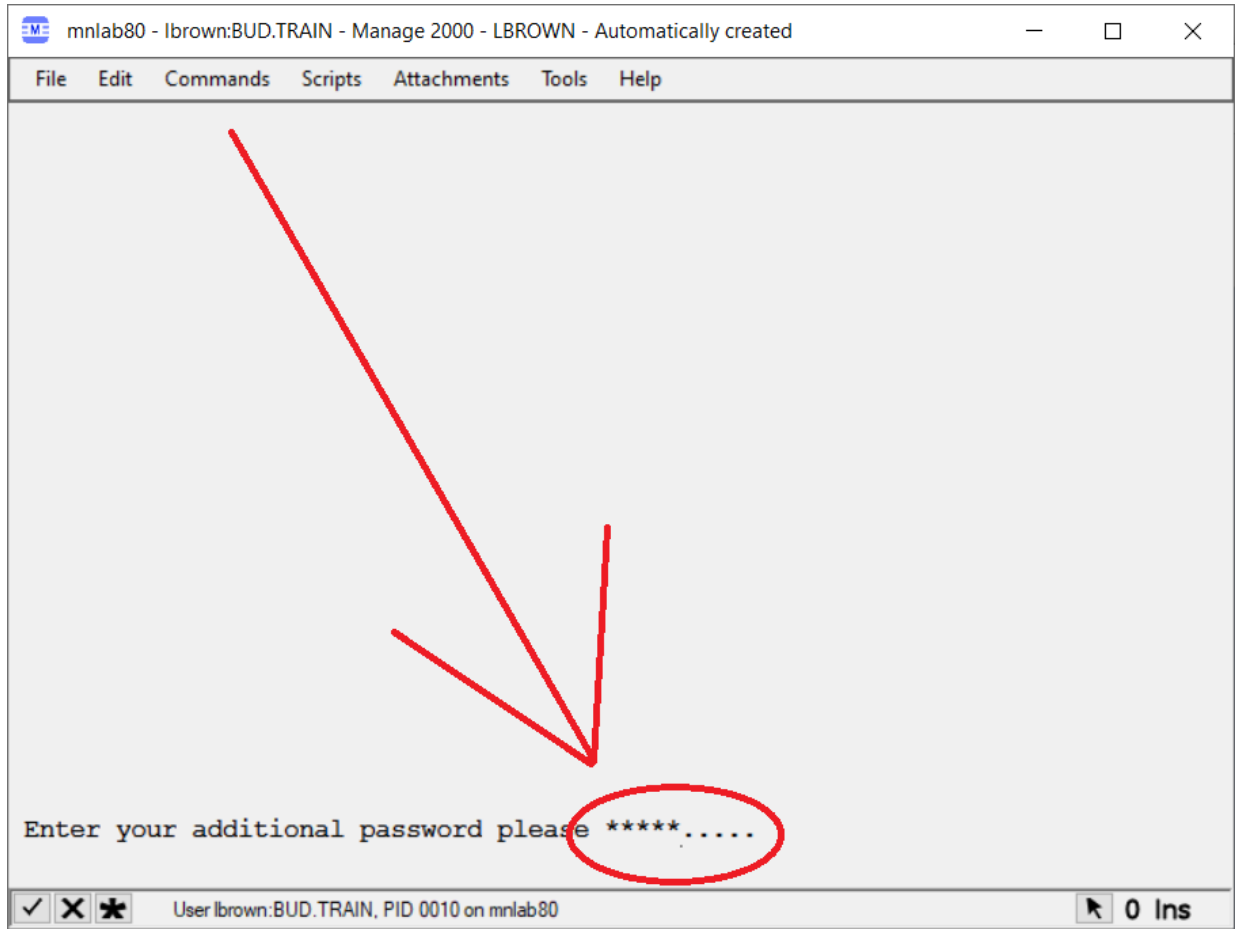

MANAGE 2000 Menu
File Edit View Help
Back Forward Stop Refresh Home Short Cuts Print
Selection
Go
EPICOR Manage 2000
Customers Website | IntraNet
Main Menu | About | Search | Log
1 PI.PROCESS
2 PI.CODES
3 PI.RPTS
4 COST.PI
5 PI.WIP.PROCESS
6 PI.CC.PROCESS.BY.PART
7 PI.CC.PROCESS.BY.LOC
8 PI.CC.CODES
9 PI.CC.INQS
10 PI.CC.RPTS
11 INV.ABC
12 PI.DOC
MANAGE-2000-8.0C.Sp5 (User: lbrov
PI
Complete
C:\Users\lbrown\AppData\Roaming\Microsoft\Windows\Templates\(mnlab80_7-3_1)pi.xml
MANAGE 2000 Menu
Customers Website | IntraNet
EPICOR Manage 2000
Access Error
Main Menu | About | Search | Logoff
FUNCTION SECURITY
An attempt was made to access a secured menu or function.
This access was denied by host for the following reason:
Security access was not granted for "lbrown" to use function "PURCHASE".
MANAGE-2000-8.0C.Sp5 (User: lbrown:BUD.TRAIN)
ERROR
OK

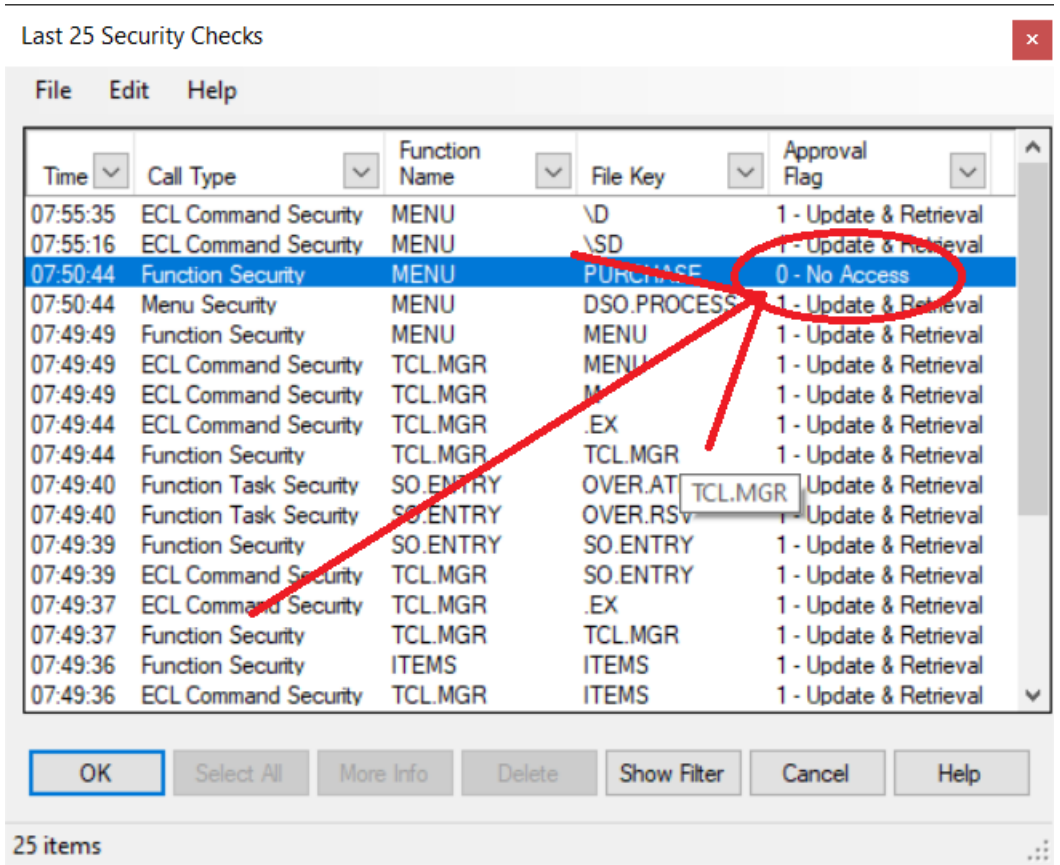

MANAGE 2000 Menu
File Edit View Help
Back Forward Stop Refresh Home Short Cuts Print
Selection \SD
Go
EPICOR Manage 2000
Customers Website | IntraNet
Physical Inventory & Cycle Counting
Main Menu | About | Search | Logoff
1 PI.PROCESS • PI Process
2 PI.CODES • PI Codes
3 PI.RPTS • PI Reports
4 COST.PI • Physical Inventory Costing
5 PI.WIP.PROCESS • Work In Process PI Process
6 PI.CC.PROCESS.BY.PART • CC Process By Part Number
7 PI.CC.PROCESS.BY.LOC • CC Process By Location
8 PI.CC.CODES • CC Codes
9 PI.CC.INQS • CC Inquiries
10 PI.CC.RPTS • CC Reports
11 INV.ABC • INV ABC Analysis
12 PI.DOC • PI/CC Documentation
MANAGE-2000-8.0C.Sp5 (User: lbrown:BUD.TRAIN)
PI
Complete
C:\Users\lbrown\AppData\Roaming\Microsoft\Windows\Templates\(mnl

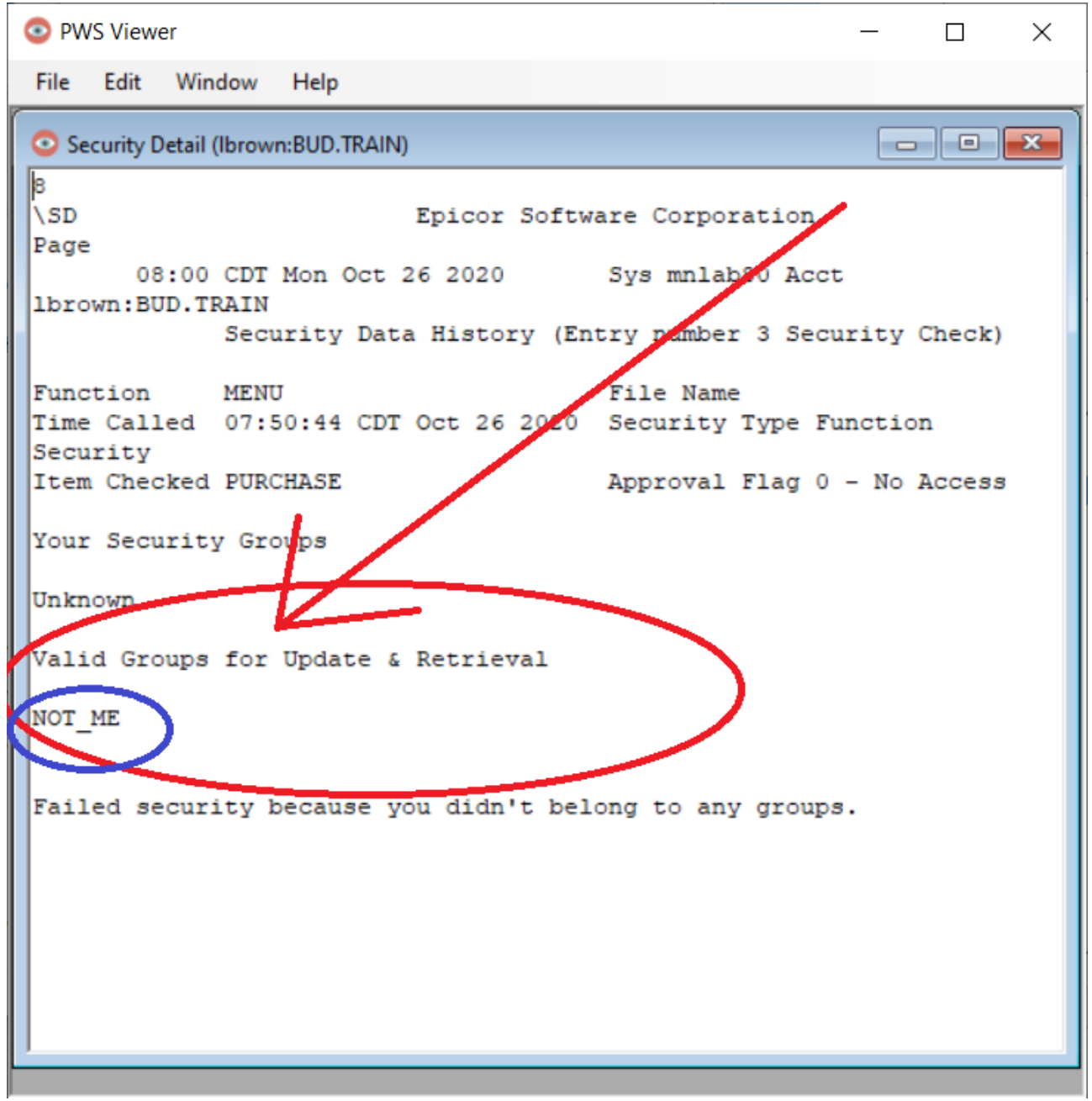




NovoRoi Systems, LLC


mnlab80 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created
File Edit Commands Scripts Attachments Tools Help
Enter your additional password please *****.....
User lbrown:BUD.TRAIN, PID 0010 on mnlab80
0 Ins


Last 25 Security Checks
File Edit Help
Time
Call Type
Function Name
File Key
Approval Flag
07:55:35 ECL Command Security MENU \D 1 - Update & Retrieval
07:55:16 ECL Command Security MENU \SD 1 - Update & Retrieval
07:50:44 Function Security MENU PURCHASE 0 - No Access
07:50:44 Menu Security MENU DSO.PROCESS 1 - Update & Retrieval
07:49:49 Function Security MENU MENU 1 - Update & Retrieval
07:49:49 ECL Command Security TCL.MGR MENU 1 - Update & Retrieval
07:49:49 ECL Command Security TCL.MGR M 1 - Update & Retrieval
07:49:44 ECL Command Security TCL.MGR .EX 1 - Update & Retrieval
07:49:44 Function Security TCL.MGR TCL.MGR 1 - Update & Retrieval
07:49:40 Function Task Security SO.ENTRY OVER.AT 1 - Update & Retrieval
07:49:40 Function Task Security SO.ENTRY OVER.RSV 1 - Update & Retrieval
07:49:39 Function Security SO.ENTRY SO.ENTRY 1 - Update & Retrieval
07:49:39 ECL Command Security TCL.MGR SO.ENTRY 1 - Update & Retrieval
07:49:37 ECL Command Security TCL.MGR .EX 1 - Update & Retrieval
07:49:37 Function Security TCL.MGR TCL.MGR 1 - Update & Retrieval
07:49:36 Function Security ITEMS ITEMS 1 - Update & Retrieval
07:49:36 ECL Command Security TCL.MGR ITEMS 1 - Update & Retrieval
TCL.MGR
OK Select All More Info Delete Show Filter Cancel Help
25 items



NovoRoi Systems, LLC

DON'T USE **ALL** WITH MENU OR FUNCTION SECURITY

- As mentioned in slide 3, a security group locks down every function or menu listed in the security group to the users listed in the security group
- Most people don't set up a security group to granting access to Printing and logging in
- If ALL is used in a security, every function or menu gets locked down and it usually causes a Down System because users can't get logged in

BEST PRACTICES

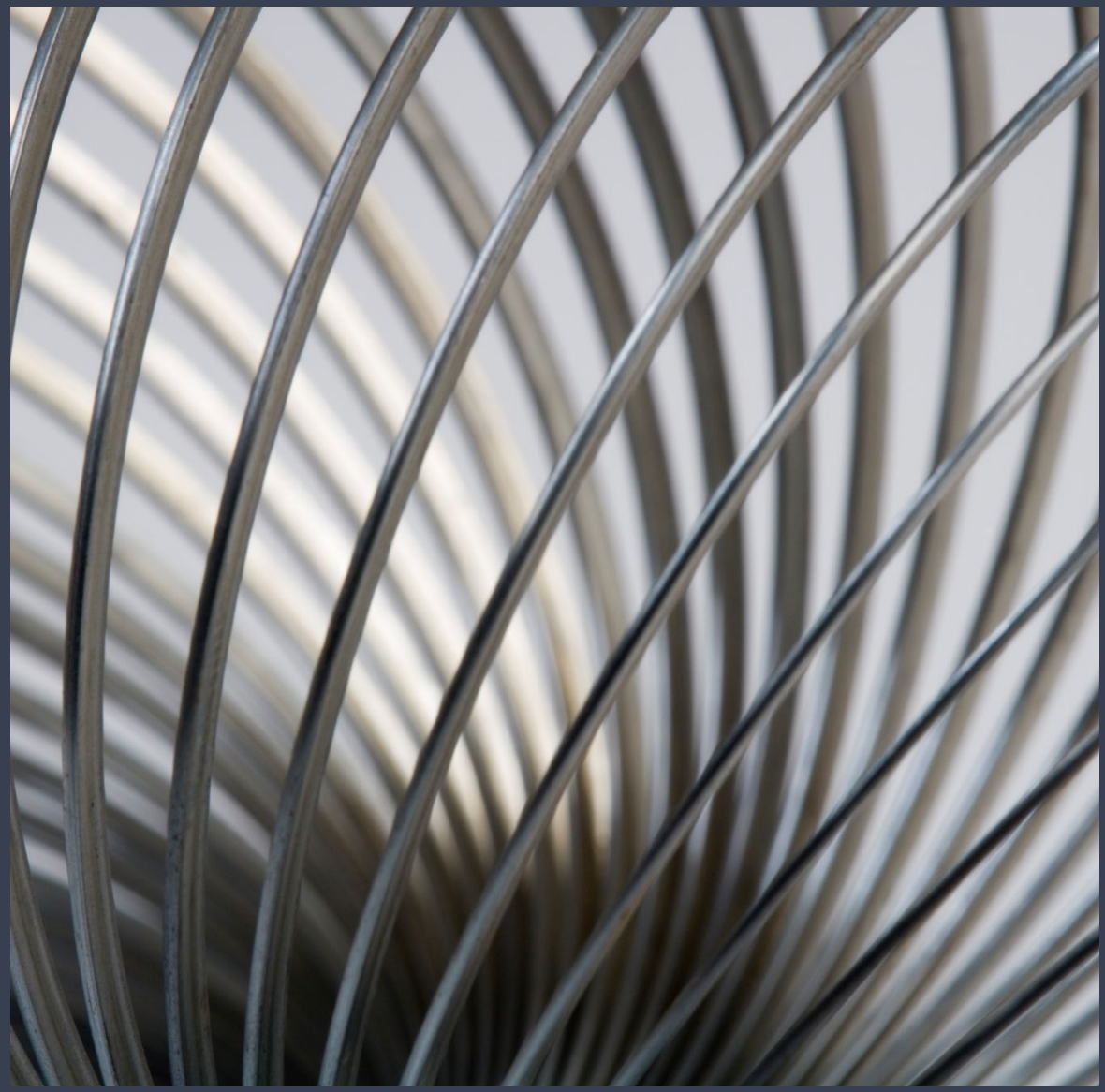
- See Handout 5 – Good guidelines for implementing security
- Suggests Mostly Menu security
- And a tiny bit of Function Security for locking down backdoors
- See Handout 6 – Granting a user access to a function

QUESTIONS?

- It’s their crib, what should I discard?

NUGM 2024

THANK YOU



Bud Brown – Epicor Software - 952-417-5196