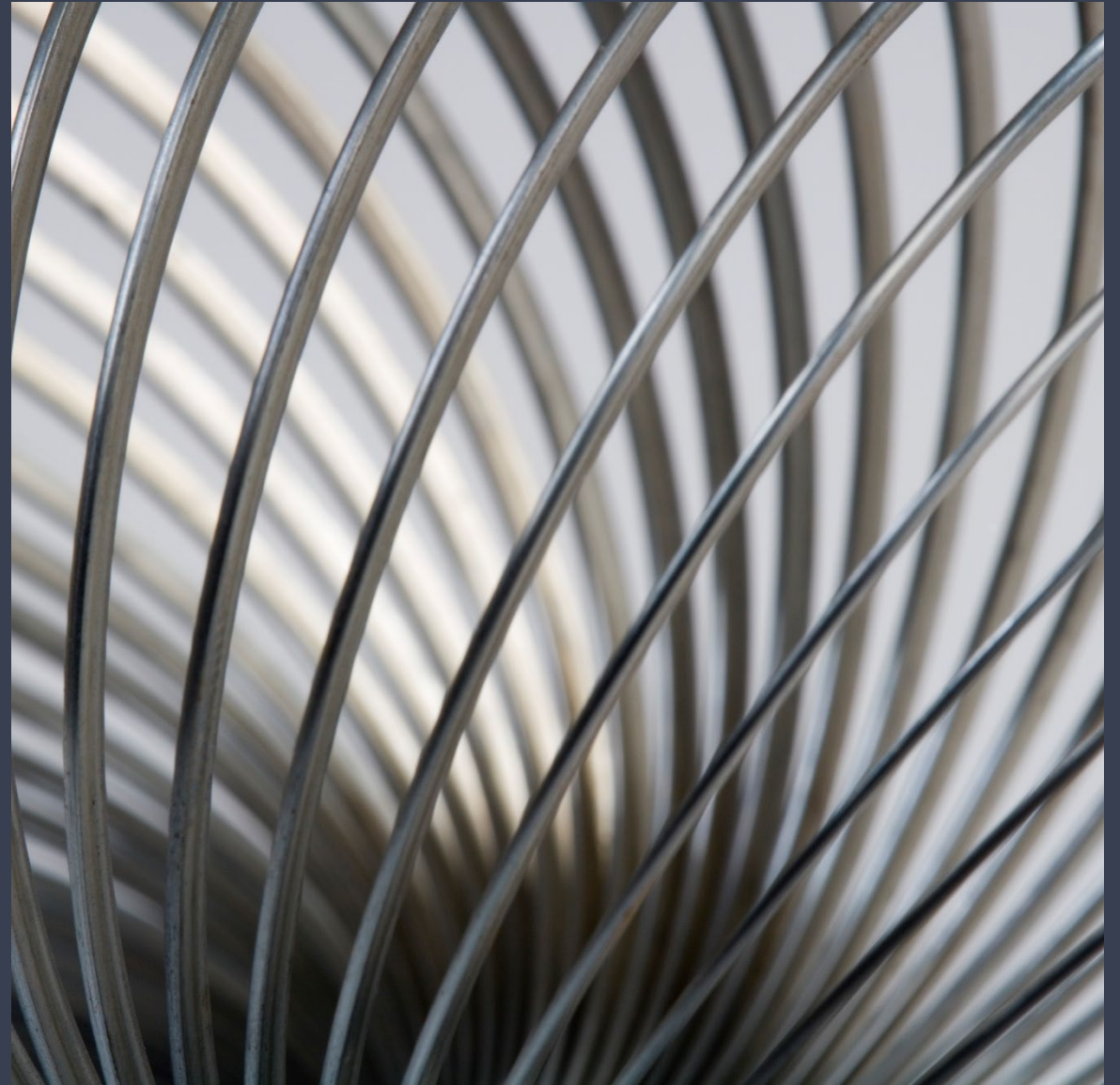


NUGM 2024

MANAGE 2000  
APPLICATION  
SECURITY

Bud Brown, Epicor Software



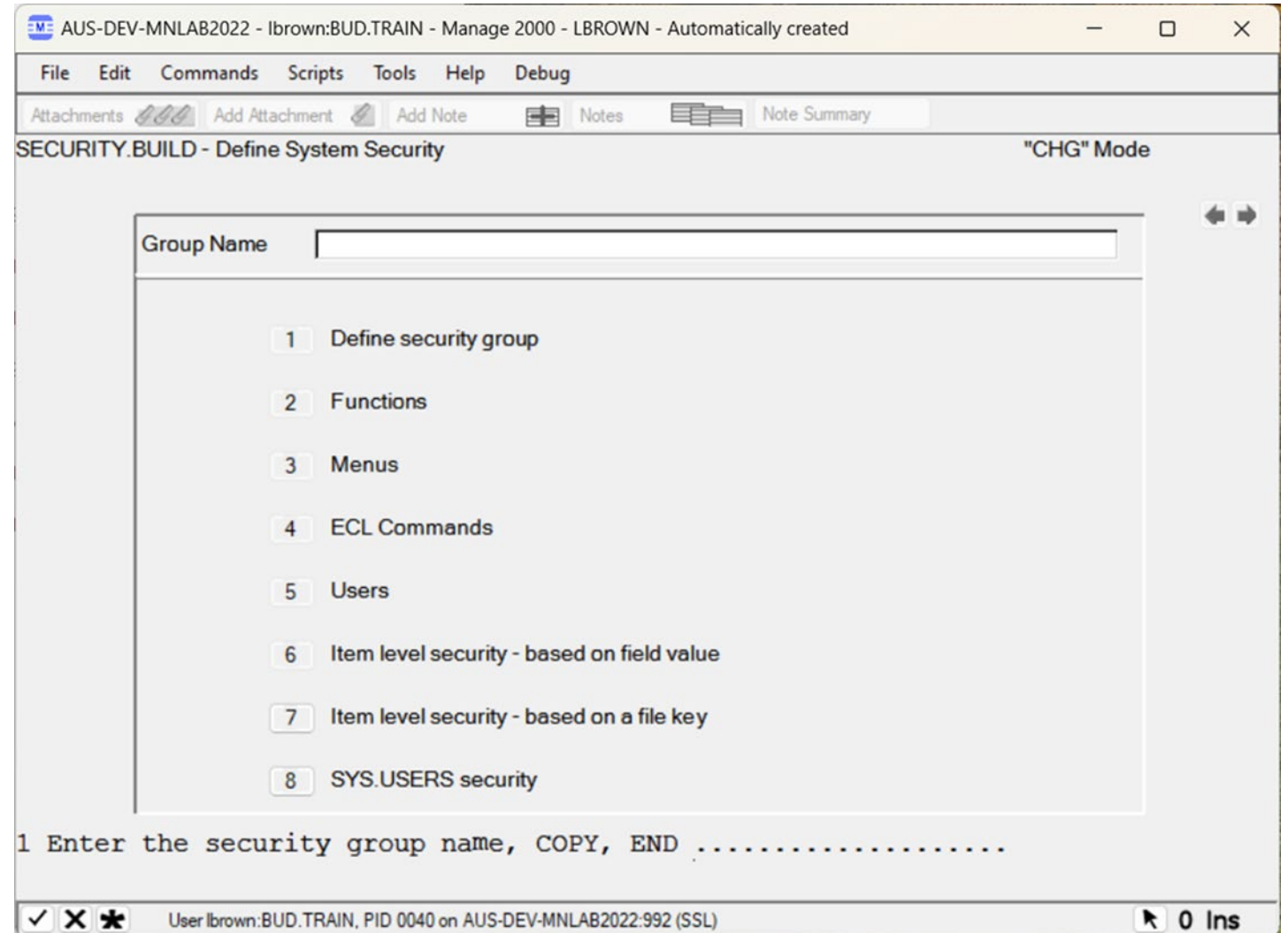
# AGENDA

- 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

AUS-DEV-MNLAB2022 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created

File Edit Commands Scripts Tools ProcessOpts Help Debug

Attachments Add Attachment Add Note Notes Note Summary

General Company Information and Controls (Part 2) "CHG" Mode

01 Product Name	Manage 2000		
02 Main Login Account	MANAGE-2000.8.0	19 *Cost Decimals	3
03 Default Menu Name		20 *Price Decimals	3
04 Menu Security	Y	21 *Qty Per Assy Decimals	3
05 Function Security	Y	22 *Sales Qty Decimals	0
06 ECL Security	Y	23 QPA Display Decimals	3
07 Menu Logo Graphic	M2KLogo.gif	24 ACTION.1 Hold Days	
08 Default Co Number	01	25 Cross Reference Logic	N
09 Multiple Co's on GL	Y	26 Global Trans Def Save	
10 Default Module Code		27 Default Fax Logo	
11 *User Control File		28 Fax Cover Sheet	STANDARD
12 *Input Sub Name		29 Company Name on Forms	Y
13 Input Sub Interval		30 Name Control Codes	U14
14 Run Address Lookup	Y	31 Address Control Codes	U14
15 Addr Case Convert	M	32 Extra Address Spacing	20
16 *International Chars		33 Save Trans Def Records	
17 FTS File Name	HOLD_		
18 FTS Overwrite	N		

Change Which Field, END, TOP, \P .....

User lbrown:BUD.TRAIN, PID 0040 on AUS-DEV-MNLAB2022:992 (SSL) 0 Ins



# 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



The screenshot shows a web browser window titled "MANAGE 2000 Menu". The browser's address bar is empty, and the page content is as follows:

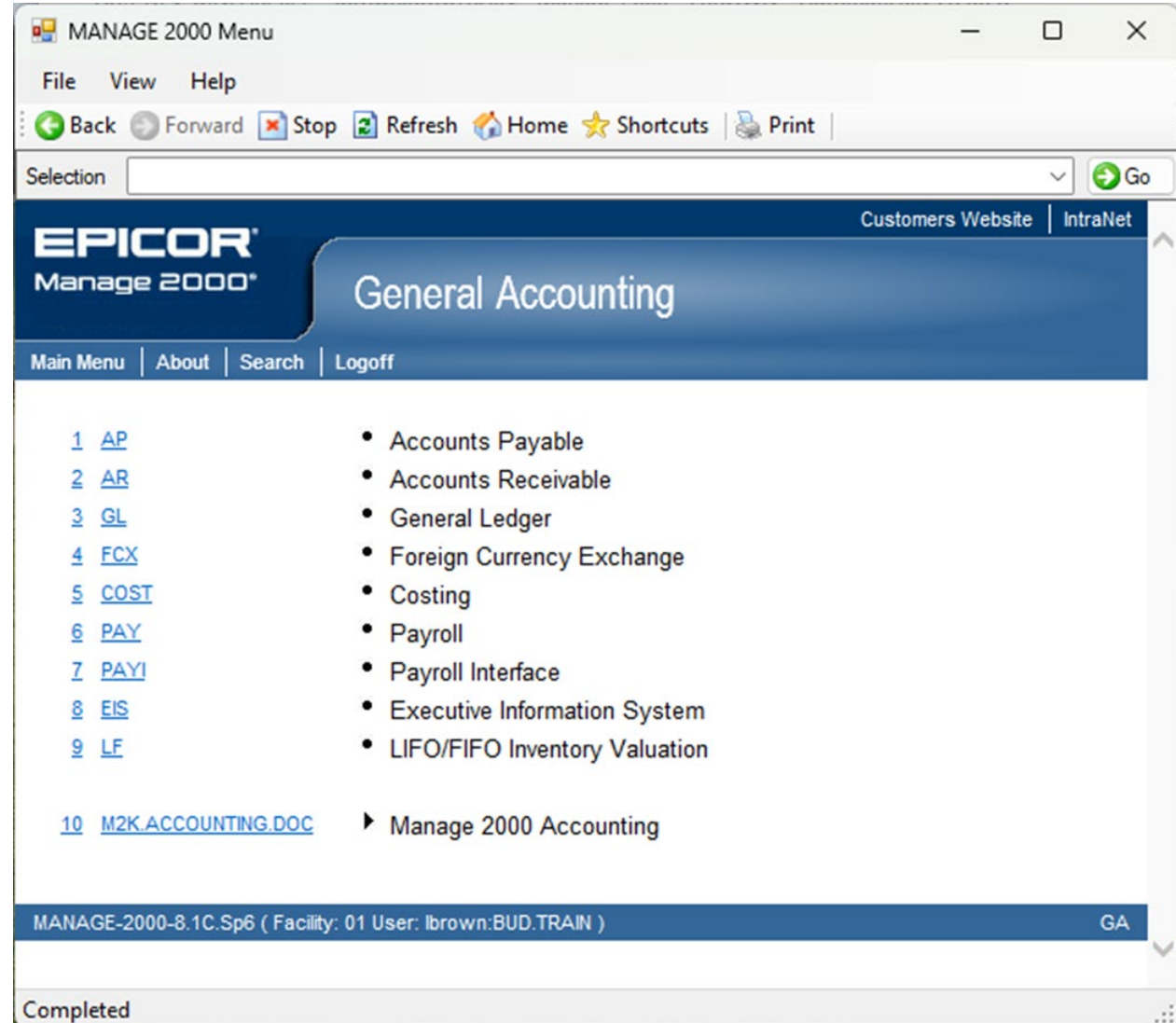
- Header: "EPICOR Manage 2000" logo on the left, "Customers Website | IntraNet" on the right.
- Sub-header: "Manage 2000" in a large blue box.
- Navigation: "Main Menu | About | Search | Logoff" in a blue bar.
- Main Content: A list of menu items on the left and a corresponding list of sub-items on the right.

<a href="#">1 PDM</a>	• Product Data Management
<a href="#">2 MFG</a>	• Manufacturing
<a href="#">3 SAM</a>	• Sales and Marketing
<a href="#">4 CRM</a>	• Customer Relationship Management
<a href="#">5 GA</a>	• General Accounting
<a href="#">6 SYS</a>	• System Tools
<a href="#">7 INTERFACE</a>	• Interface
<a href="#">8 TOOLS</a>	• Tools System Management
<a href="#">9 MARKETING.OVWS</a>	• Marketing Overviews
<a href="#">10 DOC.TRAIN</a>	• Release Documentation and Courses
- Footer: "MANAGE-2000-8.1C.Sp6 ( Facility: 01 User: lbrown:BUD.TRAIN )"
- Status Bar: "Completed"



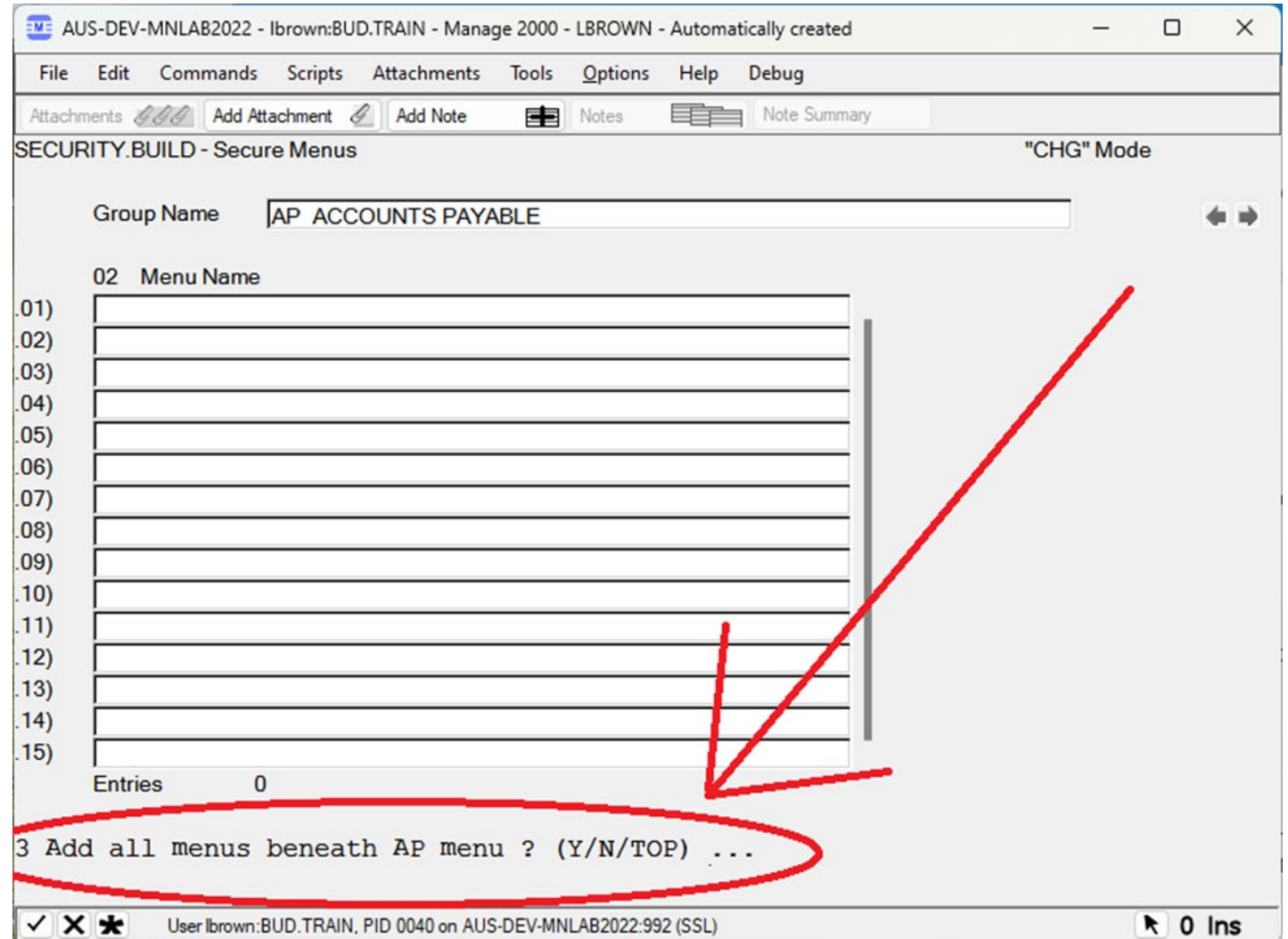
# MENU SECURITY

- 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



# MENU SECURITY

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

The screenshot shows a web application window titled "AUS-DEV-MNLAB2022 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created". The interface includes a menu bar with "File", "Edit", "Commands", "Scripts", "Attachments", "Tools", "ProcessOpts", "Help", and "Debug". Below the menu bar is a toolbar with "Attachments", "Add Attachment", "Add Note", "Notes", and "Note Summary". The main content area is titled "SECURITY.BUILD - Secure Menus" and "CHG" Mode. A "Group Name" field contains "AP ACCOUNTS PAYABLE". Below this is a table with 15 rows, each representing a menu entry. The table has two columns: "02 Menu Name" and an empty column. The entries are:

02 Menu Name	
.01) AP Accounts Payable	
.02) AP.1099.PROCESS AP 1099 Process	
.03) AP.CHECKS AP Checks	
.04) AP.CHK.RPTS AP Reports - Checks	
.05) AP.CODES AP Codes	
.06) AP.DOC AP Documentation	
.07) AP.HOWTOS AP Application How-to's	
.08) AP.INQS AP Inquiries	
.09) AP.PROCESS AP Process	
.10) AP.RPTS AP Reports	
.11) AP.TOOLS AP Tools	
.12) AP.TOPIC.OVERVIEWS AP Topic Overviews	
.13) AP.VENDOR.RPTS AP Reports - Vendor	
.14) AP.VOUCHER.INV.RPTS AP Reports - Voucher & Invoi	
.15)	

Below the table, it says "Entries 14". At the bottom of the main content area, there is a prompt: "Change Which Field, END, TOP, \P |.....". The status bar at the bottom shows "User lbrown:BUD.TRAIN, PID 0040 on AUS-DEV-MNLAB2022:992 (SSL)" and "0 Ins".





# 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

Screenshot of a web-based configuration interface for user management. The window title is "AUS-DEV-MNLAB2022 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created". The interface shows a form for "SysUsers.2 Info By Account Used" in "CHG" Mode. The form has fields for User ID (LBROWN), User Name (LBROWN - Automatically created), and various configuration options. Red circles and arrows highlight the "Initial Menu" field (set to "MANAGE-2000 Manage 2000") and the "TCL Level" field (set to "Y").

Field ID	Field Name	Value
03	Restrict Logto	[ ] .01)
04	Logto Account	BUD.TRAIN
05	Logon File Name	[ ]
06	Logon Item Name	[ ]
07	Home Facility	01
08	Home Phone Loc	[ ]
09	Base Time Zone	[ ]
10	Prompt for TZ	[ ]
11	Web Sitemap	[ ]
12	Web Shortcuts	[ ]
13	Initial Menu	MANAGE-2000 Manage 2000
14	Invoke	[ ]
15	TCL Level	Y
16	PMI Access	Y
17	Add Login Cmnds	[ ]
18	Check Mail	N
19	Web Site Code	[ ]
20	Mits Server	[ ]

Change Which Field, END, TOP, \P .....

# FUNCTION SECURITY

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

SECURITY.BUILD - Secure Functions "ADD" Mode

Group Name

	02 Function Name	03 Tasks	04 Pmts	05 Password
.01)	COMPANY.NAME Set System-Wide Controls o	N	N	
.02)	FN.BUILD Define Software Functions	N	N	
.03)	MENU.BUILD Build Menus	N	N	
.04)	SECURITY.BUILD Define Security Paramete	N	N	
.05)	SYS.USERS Maintain Manage 2000 User Inf	N	N	
.06)				
.07)				
.08)				
.09)				
.10)				
.11)				
.12)				
.13)				
.14)				
.15)				

Entries 5

Change Which Field, END, TOP, \P |.....

User lbrown:BUD.TRAIN, PID 0040 on AUS-DEV-MNLAB2022:992 (SSL) 0 Ins



# 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

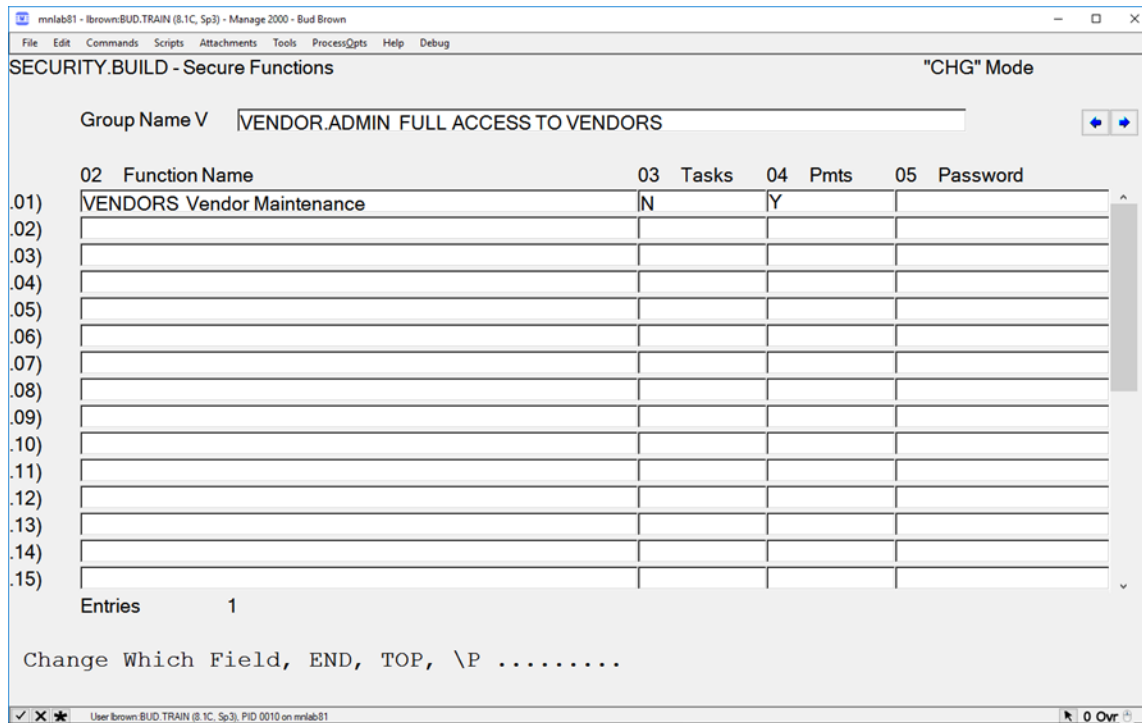
---

- 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



Window title: mnlab81 - lbrown:BU.D.TRAIN (8.1C, Sp3) - Manage 2000 - Bud Brown

SECURITY.BUILD - Secure Functions "CHG" Mode

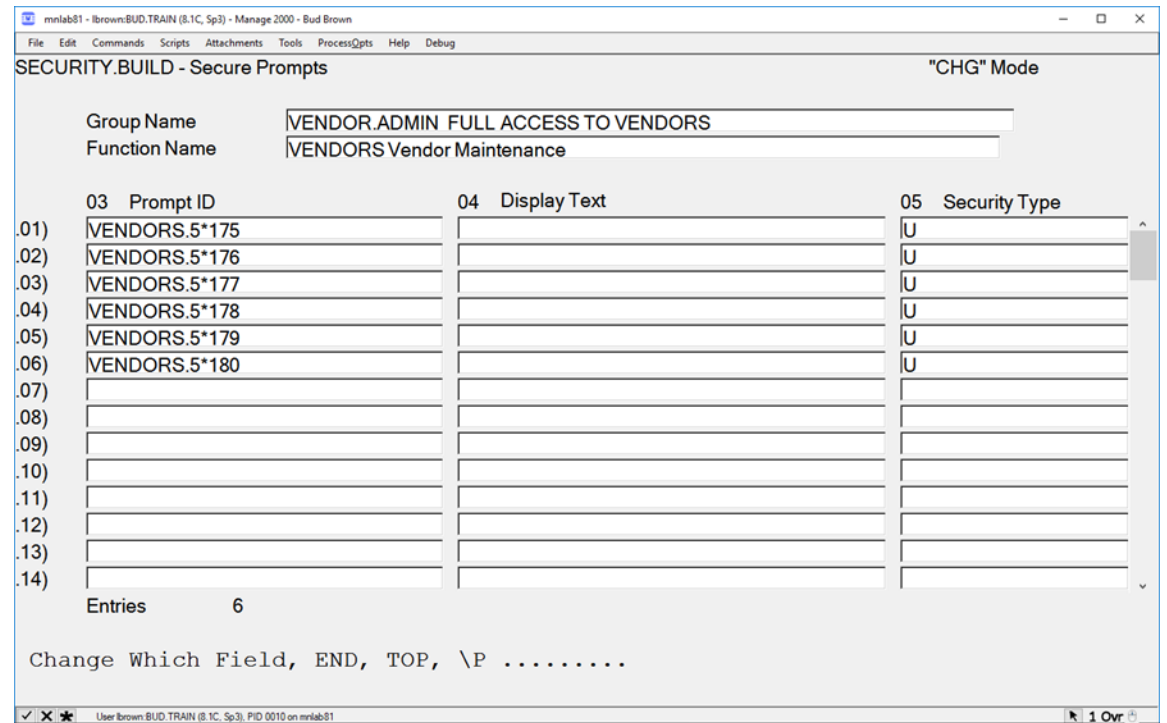
Group Name V |VENDOR.ADMIN FULL ACCESS TO VENDORS

02	Function Name	03	Tasks	04	Pmts	05	Password
.01)	VENDORS Vendor Maintenance		N		Y		
.02)							
.03)							
.04)							
.05)							
.06)							
.07)							
.08)							
.09)							
.10)							
.11)							
.12)							
.13)							
.14)							
.15)							

Entries 1

Change Which Field, END, TOP, \P .....

User lbrown:BU.D.TRAIN (8.1C, Sp3), PID 0010 on mnlab81



Window title: mnlab81 - lbrown:BU.D.TRAIN (8.1C, Sp3) - Manage 2000 - Bud Brown

SECURITY.BUILD - Secure Prompts "CHG" Mode

Group Name |VENDOR.ADMIN FULL ACCESS TO VENDORS

Function Name |VENDORS Vendor Maintenance

03	Prompt ID	04	Display Text	05	Security Type
.01)	VENDORS.5*175				U
.02)	VENDORS.5*176				U
.03)	VENDORS.5*177				U
.04)	VENDORS.5*178				U
.05)	VENDORS.5*179				U
.06)	VENDORS.5*180				U
.07)					
.08)					
.09)					
.10)					
.11)					
.12)					
.13)					
.14)					

Entries 6

Change Which Field, END, TOP, \P .....

User lbrown:BU.D.TRAIN (8.1C, Sp3), PID 0010 on mnlab81



# FIELD LEVEL SECURITY

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

mnlab81 - lbrown:BUD.TRAIN (8.1C, Sp3) - Manage 2000 - Bud Brown

File Edit Commands Scripts Attachments Tools ProcessOpts M\$O Help Debug

VENDORS.5 - Remit-To Address and General Information "CHG" Mode

Vendor Number	****	Phone Numbers	
02 Remit to		12 Business	
03 Pay Name	*****	13 800	
Remit-To Address (if different from Buy)		14 Fax	
04	*****	15 Alpha Sort	
05		16 Audit Limit	3000.00
06 ZIP/Post	*****	17 Default Pay	
07 City	Denver	18 Auto-Invoice	
08 State	CO Colorado		
09 Country	USA United States of America		
10 Time Zn			
11 Contact	2022 Rita Jones		

19 Accounts Payable Comments	Entries	0
.01)		
.02)		
20 PO Payable Notes	Entries	0
.01)		
.02)		

Change Which Field, END, TOP, \P . . . . .

User lbrown: BUD.TRAIN (8.1C, Sp3), PID 0010 on mnlab81 0 Ovr



# FIELD LEVEL SECURITY

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

mnlab81 - lbrown:BUD.TRAIN (8.1C, Sp3) - Manage 2000 - Bud Brown

File Edit Commands Scripts Attachments Tools ProcessOpts Help Debug

SECURITY.BUILD - Secure Functions "CHG" Mode

Group Name

	02 Function Name	03 Tasks	04 Pmts	05 Password
.01)	VENDORS Vendor Maintenance	N	N	
.02)				
.03)				
.04)				
.05)				
.06)				
.07)				
.08)				
.09)				
.10)				
.11)				
.12)				
.13)				
.14)				
.15)				

Entries 1

Change Which Field, END, TOP, \P .....

User lbrown:BUD.TRAIN (8.1C, Sp3), PID 0010 on mnlab81 0 Ovr





# FIELD LEVEL SECURITY

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

AUS-DEV-MNLAB2022 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created

File Edit Commands Scripts Attachments Tools Process\_Opts Help Debug

Attachments Add Attachment Add Note Notes Note Summary

SECURITY.BUILD - Secure Prompts "CHG" Mode

Group Name: VENDOR.DISPLAY Some Vendor fields locked down  
Function Name: VENDORS Vendor Maintenance

03 Prompt ID	04 Display Text	05 Security Type
01) VENDORS.5*175		D
02) VENDORS.5*176		D
03) VENDORS.5*177		D
04) VENDORS.5*178		D
05) VENDORS.5*179		D
06) VENDORS.5*180		D
07)		
08)		
09)		
10)		
11)		
12)		
13)		
14)		

Entries 6

Change Which Field, END, TOP, \P .....

User lbrown:BUD.TRAIN, PID 0040 on AUS-DEV-MNLAB2022:992 (SSL) 1 Ins

AUS-DEV-MNLAB2022 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created

File Edit Commands Scripts Attachments Tools Process\_Opts Help Debug

Attachments Add Attachment Add Note Notes Note Summary

SECURITY.BUILD - Secure Prompts "CHG" Mode

Group Name: VENDOR.ADMIN Full Access to Vendors  
Function Name: VENDORS Vendor Maintenance

03 Prompt ID	04 Display Text	05 Security Type
01) VENDORS.5*175		U
02) VENDORS.5*176		U
03) VENDORS.5*177		U
04) VENDORS.5*178		U
05) VENDORS.5*179		U
06) VENDORS.5*180		U
07)		
08)		
09)		
10)		
11)		
12)		
13)		
14)		

Entries 6

Change Which Field, END, TOP, \P .....

User lbrown:BUD.TRAIN, PID 0040 on AUS-DEV-MNLAB2022:992 (SSL) 1 Ins



# 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

AUS-DEV-MNLAB2022 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created

File Edit Commands Scripts Attachments Tools ProcessOpts Help Debug

Attachments Add Attachment Add Note Notes Note Summary

SECURITY.BUILD - Define System Security "ADD" Mode

Group Name

- 1 Define security group
- 2 Functions
- 3 Menus
- 4 ECL Commands**
- 5 Users
- 6 Item level security - based on field value
- 7 Item level security - based on a file key
- 8 SYS.USERS security

Enter Sub Section to Process, TOP, END |...

User lbrown:BUD.TRAIN, PID 0040 on AUS-DEV-MNLAB2022:992 (SSL) 0 Ins

AUS-DEV-MNLAB2022 - lbrown:BUD.TRAIN - Manage 2000 - LBROWN - Automatically created

File Edit Commands Scripts Attachments Tools ProcessOpts Help Debug

Attachments Add Attachment Add Note Notes Note Summary

SECURITY.BUILD - Allowed ECL commands "ADD" Mode

Group Name

	02 Allowed ECL command	Type	Description
01)		V	Unidata verb
02)	CLEAR.FILE	V	Unidata verb
03)	CNAME	V	Unidata verb
04)	COPY	V	Unidata verb
05)	DELETE	V	Unidata verb
06)	DELETE.FILE	V	Unidata verb
07)	DELETE.INDEX	V	Unidata verb
08)	ED	P	Extended editor (Automatic finds xxx.
09)	EDP	F	Editor using the PC editing screen
10)	MODIFY	V	Unidata verb
11)	epiEdit	P	Pseudo Function for EDX
12)			
13)			
14)			
15)			

Entries 11

Change Which Field, END, TOP, \P .....

User lbrown:BUD.TRAIN, PID 0040 on AUS-DEV-MNLAB2022:992 (SSL) 0 Ins

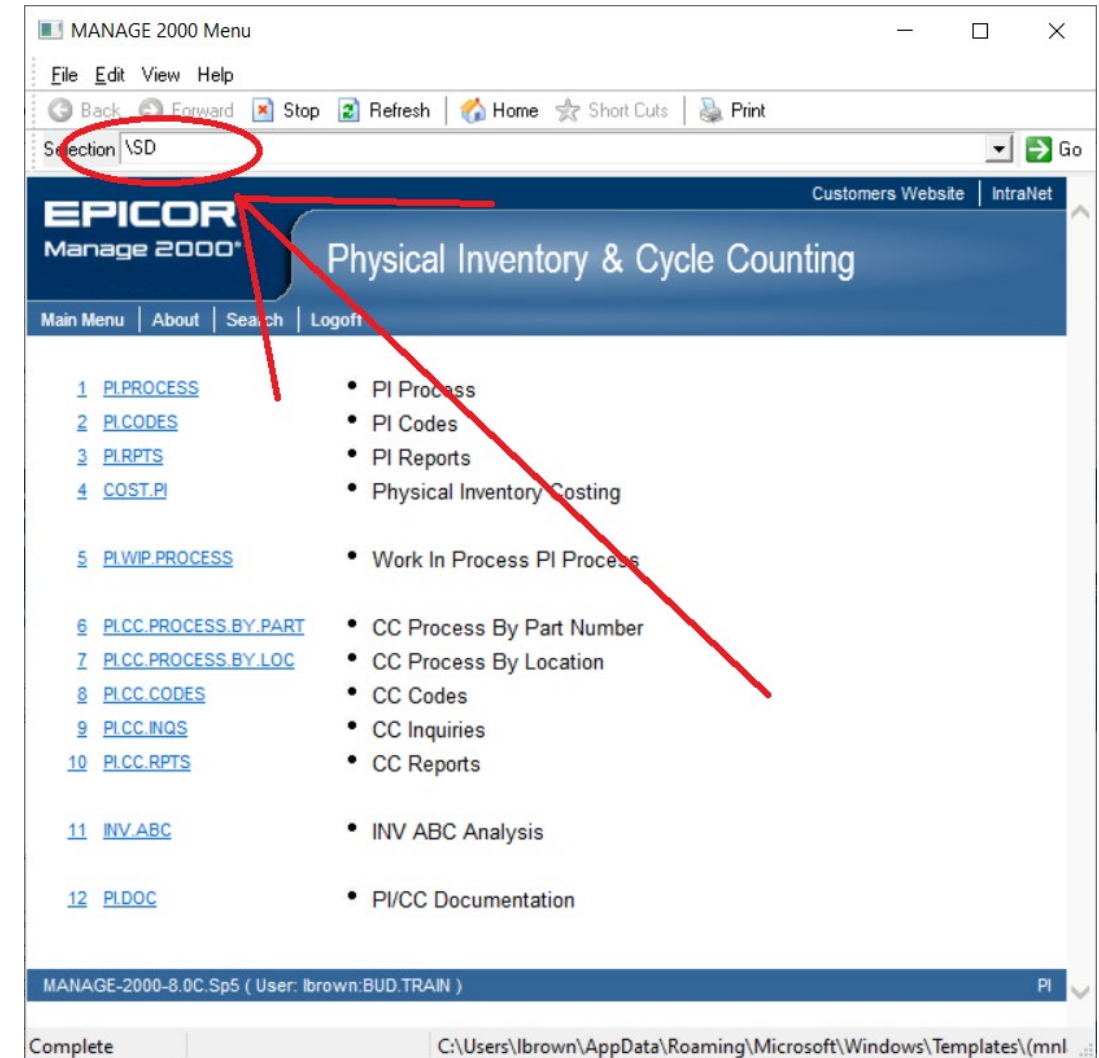
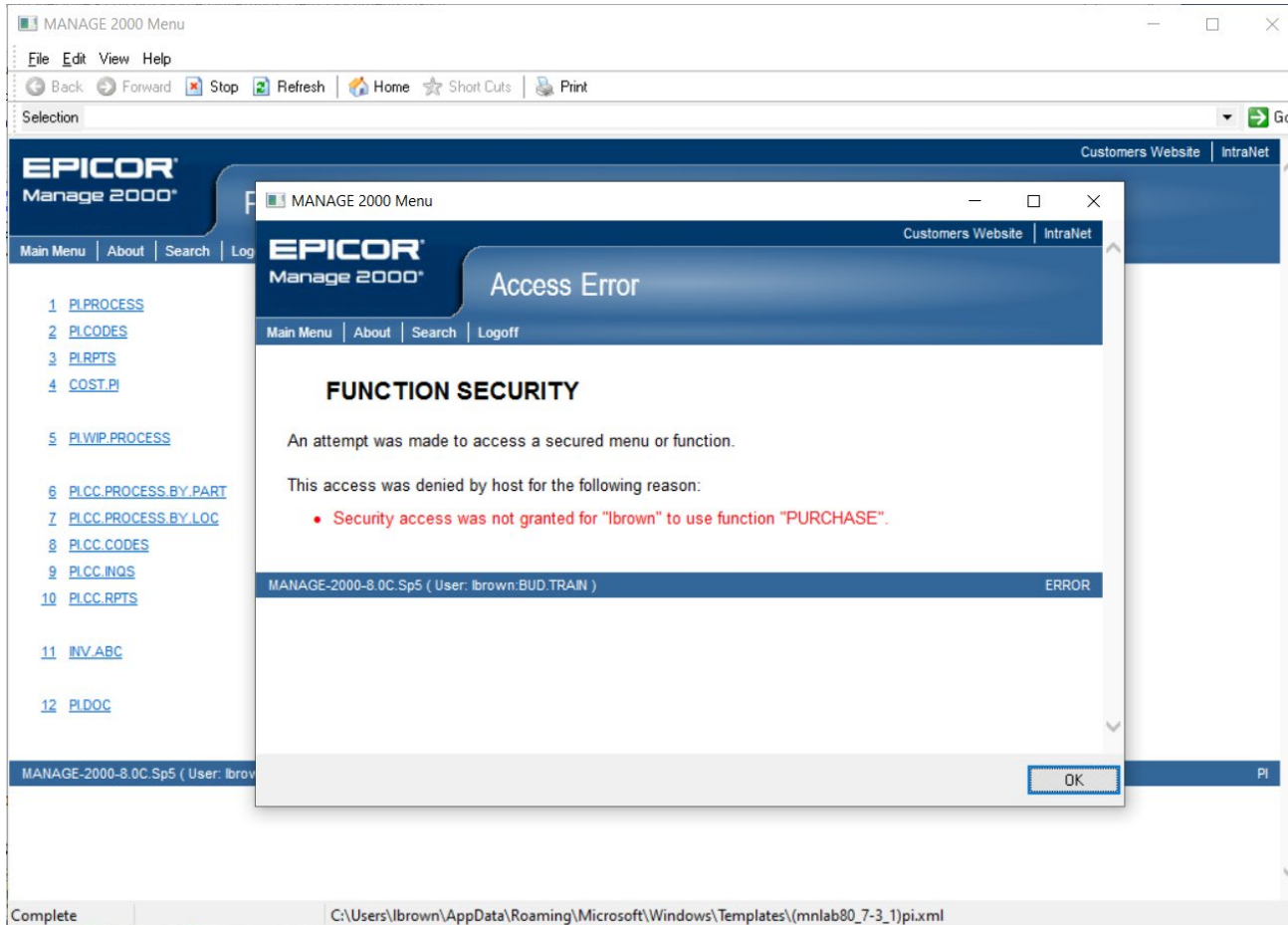


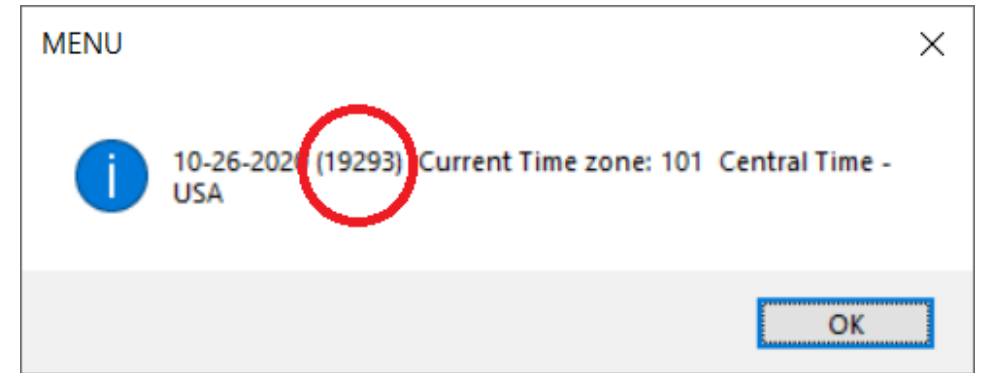
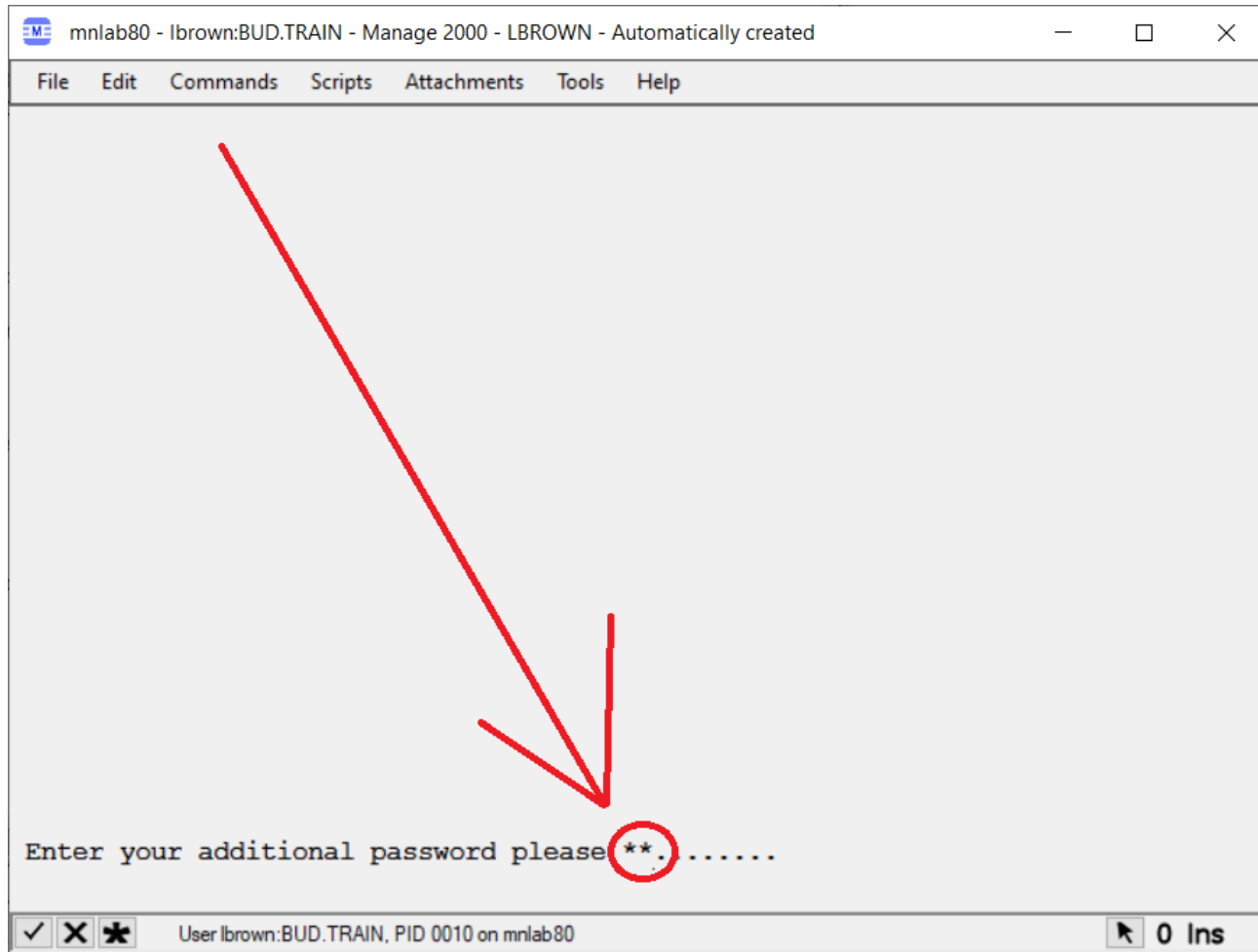
# \SD TO SHOW WHY SECURITY FAILED

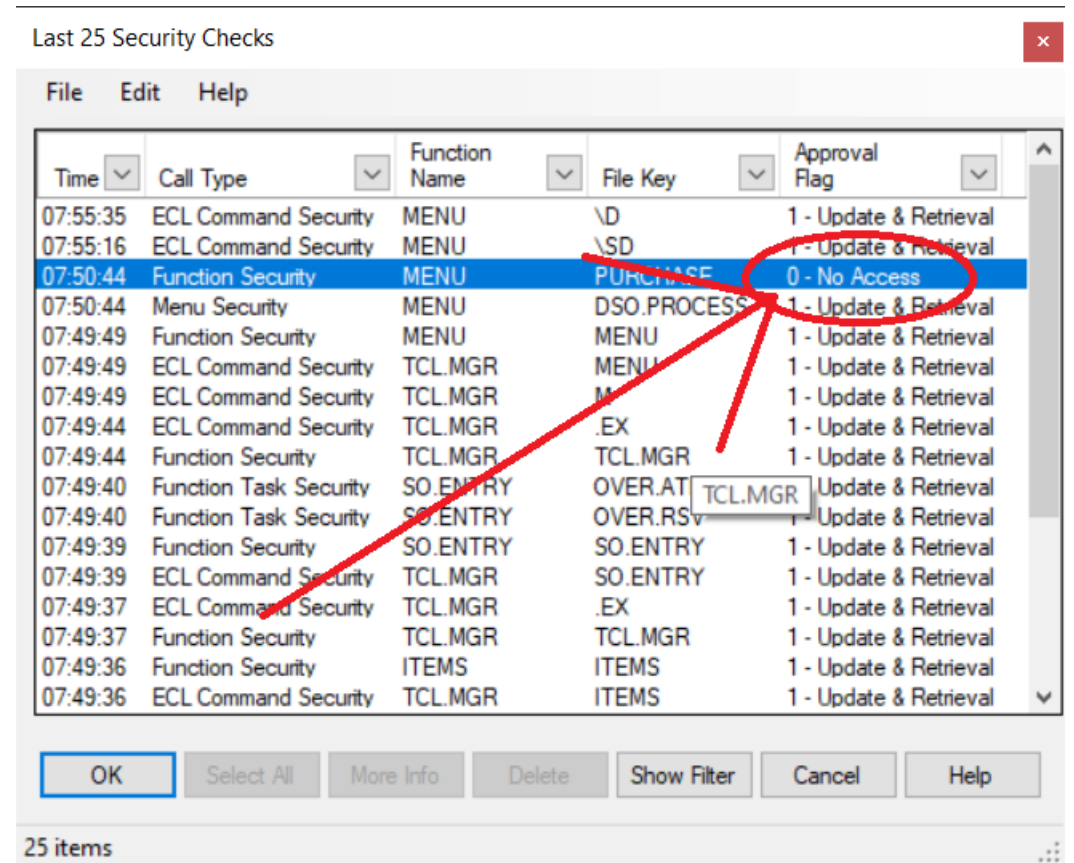
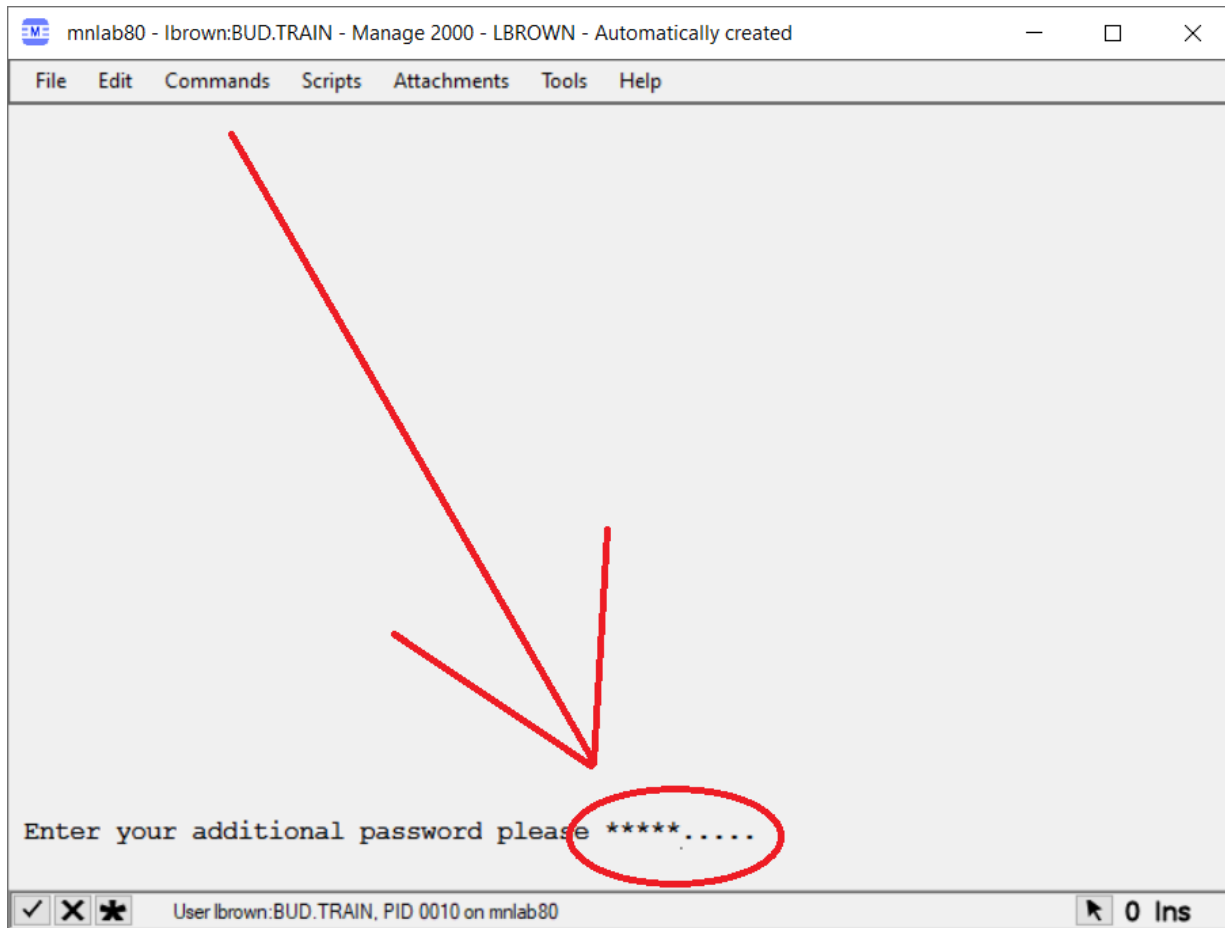
---

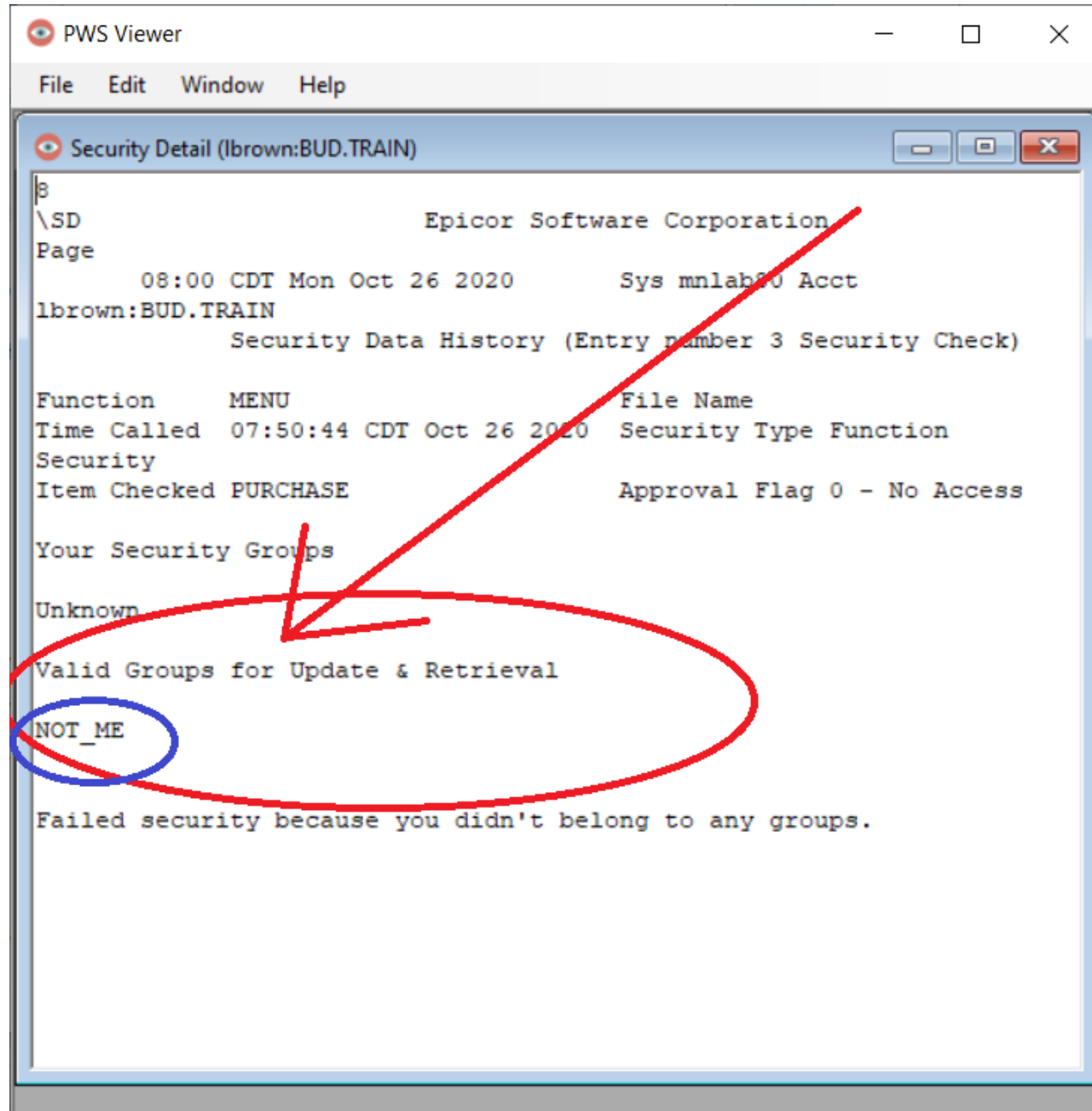
- After a user fails security, type in \SD at the menu
- User will be prompted for a password that is today's Internal Date
- Type in \D to find out current Internal Date
- A List-box will popup showing all security checks
- Select the one that says No Access and click OK
- The PWS Viewer will open and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













# 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

