Bypassing Password Security on the IBM System/34

2024-Feb-17 Joe G. and David "Grizzly" K.

1. Obtain physical access to the S/34 and the console.
2. IPL the system to an IPL Signon screen.
3. On the CE Panel, press the MSP STOP button. An Alter/Display menu will appear on the console.
4. Press "1" (Alter/Display Main Storage) and press the Field Exit key (not ENTER).
5. The cursor will be sitting on an address field in the first row. Type "0000M" and press Enter.
6. A page from memory will appear. Write down the value in bytes 1D-1E. In our example below, it's "09A1"

   ```
   0000M F40022F4 00114006 90130005 402C00C1
   0010  A504BOFD 08026900 000D8115 4009A101
   ```

7. Press the ATTN key. Press "2" (Alter/Display Disk Storage) and press Field Exit (not ENTER).
8. Enter "F 00" and the 4 characters from Step 7 then press Enter.

   ```
   F 0009A1
   ```

9. Use the Roll Up key to page forward a couple of pages from that point. You will start to see entries in the disk VTOC like #LIBRARY, #SPOOL1, #SYSWORK, etc at addresses 0000, 0040, 0080, and 00C0. Scroll until you see the name SECPROF in the right side of the screen. Write down the three bytes at offset 16-18 from the start of the line containing the word SECPROF. In this example, the address is 0080 so we want bytes 0096-0098:

   ```
   0080 5C01E205 C3D709D6 C6821130 48000100 *. SECPROF......
   0090 80000F00 0096071F 8507201B 30010000 ................
   ```

10. At the top of the screen, next to SSS= enter those three bytes and press Enter:

    ```
    SSS= 071F85
    ```

11. The password file will be displayed. There are 4 entries per page. Find the Master Security Officer entry. It's likely the first entry on the screen, but it's the entry with Hex "80" in offset 0C of the entry (could be 000C, 004C, 008C, or 00CC):

    0000 2E29A3BF BFBFBFBF 0E0D0C0B 80404040
    0010 40404040 40404040 40404040 40404040

12. The 8 bytes at offset 00-07 are the username masked with a simple XOR 255. The username is in EBCDIC. See the table below. The name is padded with spaces (Hex BF = EBCDIC 40 = space). The spaces can be skipped in the username.

    2E293ABF BFBFBFBF = "JOE   "

13. The 4 bytes at offset 08-0B are the password. Passwords are only 4 characters. They are also masked with a simple XOR 255. The password is in EBCDIC. See the table below.

    0E0D0C0B = "1234"

14. Press the ATTN key to return to the Alter/Display menu, then press "0" and press Field Exit to return to the IPL Signon screen. Enter the username and password from steps 13 and 14 above, set the date and time, and press Enter to IPL and sign on.

15. Once logged on, to disable password security:
    - Run the PRSRC procedure (if it exists), Define Resource Security, and disable it.
    - Run the PROF procedure, Define Password Security, and disable it.

16. XOR CHART

Hex	Char		Hex	Char		Hex	Char		Hex	Char
3E	A		2A	N		0F	0		A5	!
3D	B		29	O		0E	1		83	@
3C	C		28	P		0D	2		84	#
3B	D		27	Q		0C	3		A4	$
3A	E		26	R		0B	4		93	%
39	F		1D	S		0A	5		4F	&
38	G		1C	T		09	6		A3	*
37	H		1B	U		08	7		B1	+
36	I		1A	V		07	8		9F	-
2E	J		19	W		06	9		92	_
2D	K		18	X					81	=
2C	L		17	Y		BF	SPACE		B4	.
2B	M		16	Z						