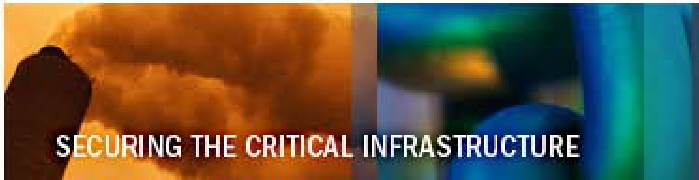
News from Camp 4

Reid Wightman

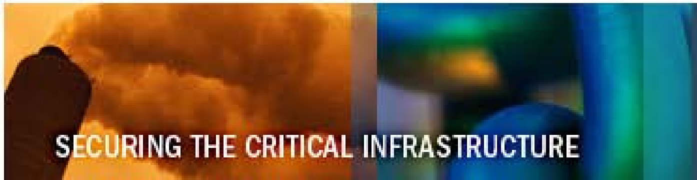
wightman@digitalbond.com

AppSecDC, 2012



Today

- Quick Recap
- New ‘sploits
- Dear Vendor



What’s a PLC

- Programmable Logic Controller
- Inputs and Outputs
  - Input example: thermometer in a mash tun
  - Output example: heater element and pump motor on a mash tun
- Program sez:
  - Keep the temperature @ 153-156F for one hour
  - After the timer expires, turn on the pump on to move the mash to fermentation tank
- PLC reports to HMI: How is the beer coming?

Quick recap

- GE D20
  - Security via one protocol (TELNET) but not another (TFTP, LogicLinx)
  - Bad guys get full access (read/write) to configuration, plus plaintext passwords, ability to write new ladder logic, etc

Quick Recap 2

- Schneider Modicon
  - Security via one protocol (HTTP) but not others (FTP/TELNET/Modbus)
  - Bad guys get full access (read/write) to configuration, plus plaintext passwords

Quick Recap 3

- Koyo ECOM100
  - Security via one protocol (HAP) but not another (HTTP)
  - HAP protocol features small password space, easy to bruteforce

Quick Recap 4

- Rockwell ControlLogix
  - Security via one protocol (EIP) but not another (err…EIP)
  - Bad guys can kill controller remotely

<3 Metasploit

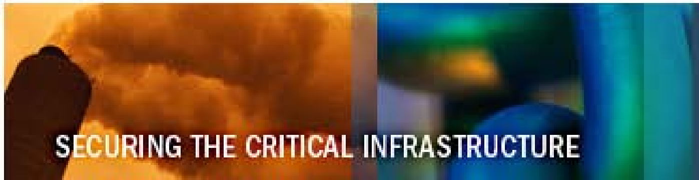
- Building as many vulnerability demonstrations as possible into MSF
- Let everybody see just how easy it is to kill controllers

D20 Modules

- d20tftpbd – provides asyncronous command line via TFTP
- d20pass – retrieves configuration via TFTP, parses config, stores usernames + passwords as loot
- d20_tftp_overflow – triggers buffer overflow in TFTP service. Currently DoS, likely RCE.

Modicon Modules

- modicon_password_recovery – retrieve passwords
  - HTTP, Write Password are plaintext
  - FTP Password uses vxworks loginDefaultEncrypt() – easily reversed
- Two new modules today...wait for it.



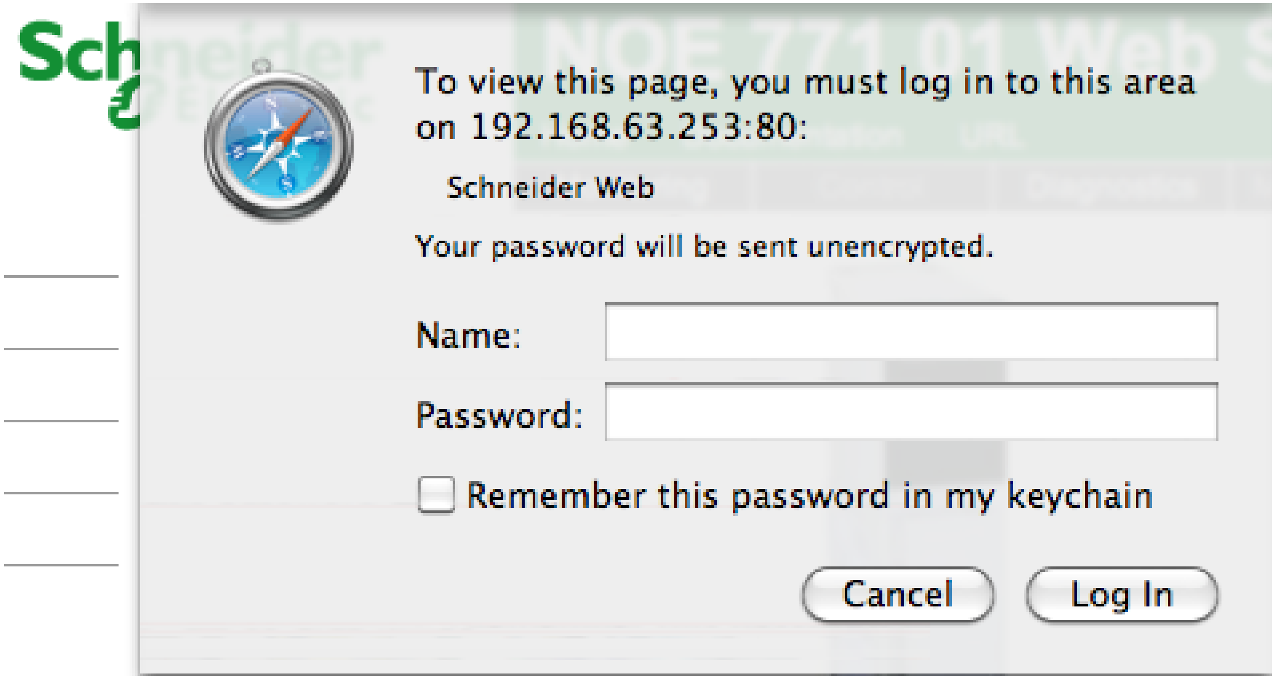
Allen-Bradley ControlLogix

- multi_cip_command – Three payloads derived from Rubén Santamarta’s C code
  - STOP the CPU
  - Crash the CPU
  - Crash the Ethernet card

Koyo

- koyo_login – Brute-force Koyo ECOM passwords

Inconsistent Security



To view this page, you must log in to this area on 192.168.63.253:80:

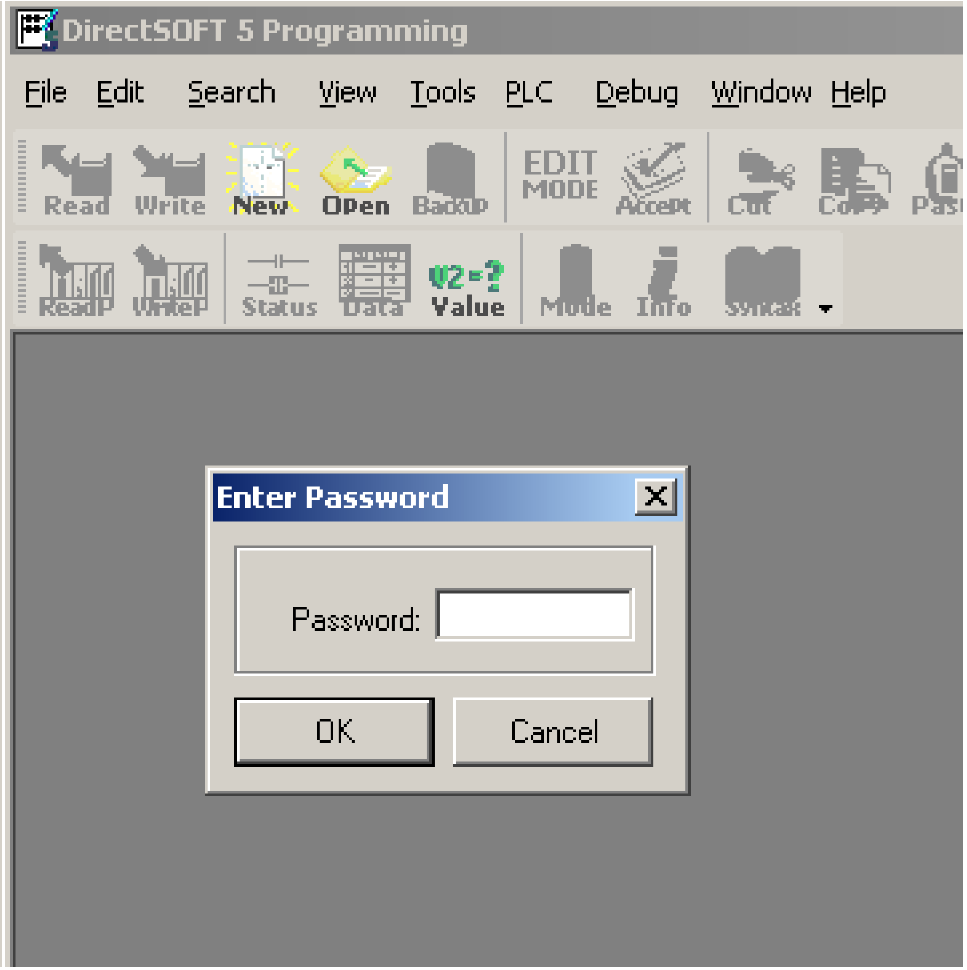
Schneider Web

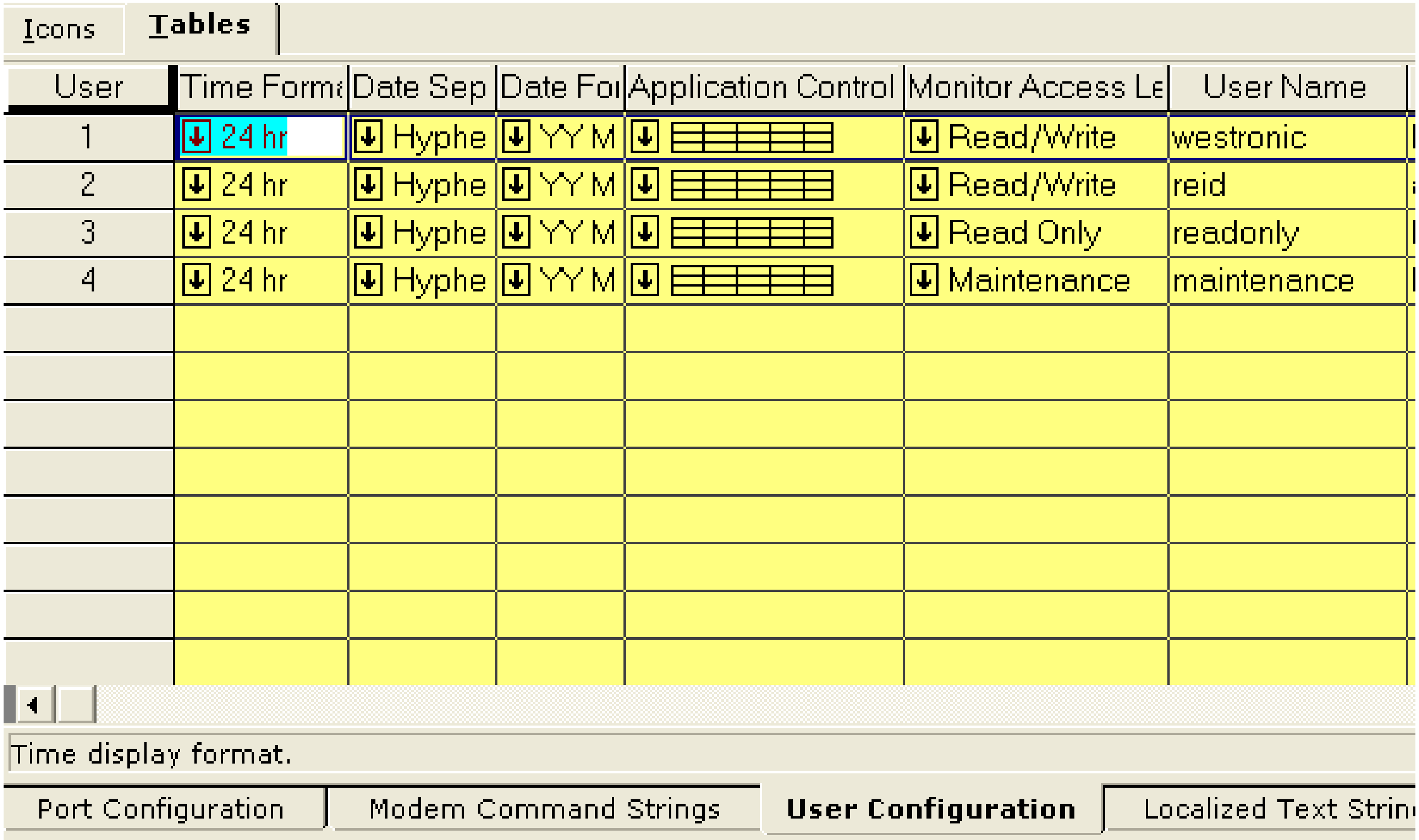
Your password will be sent unencrypted.

Name:

Password:

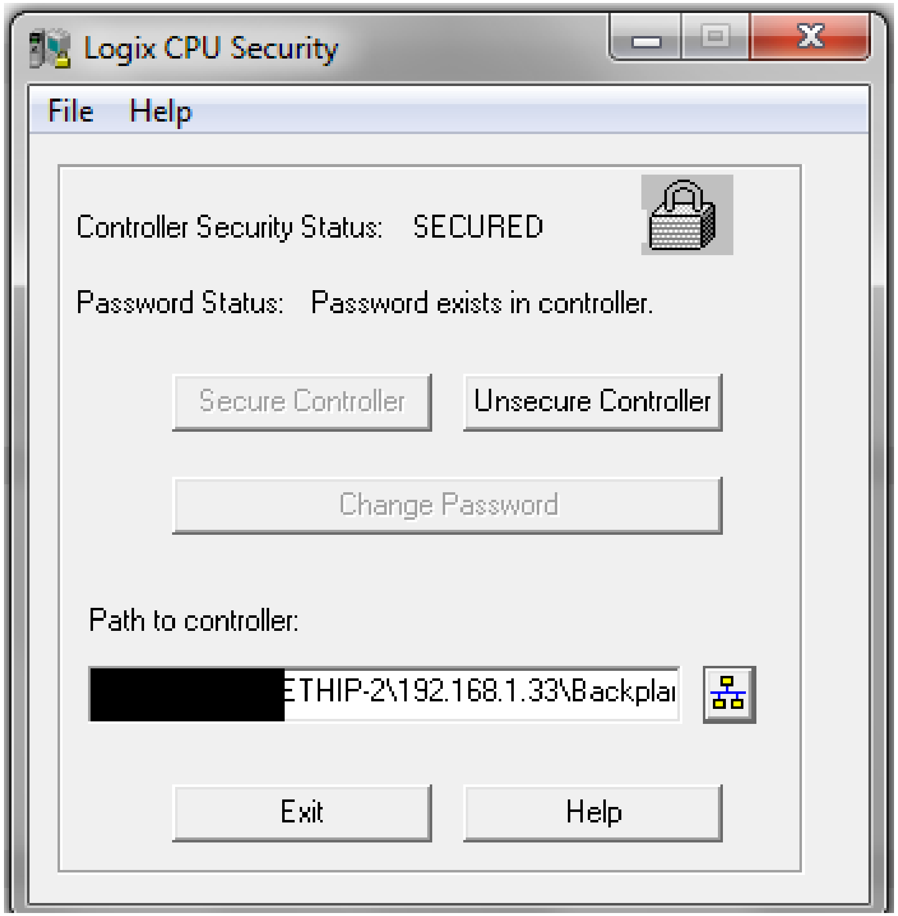
□ Remember this password in my keychain


DirectSOFT 5 Programming
File
Edit
Search
View
Tools
PLC
Debug
Window
Help
Read
Write
New
Open
Backup
EDIT MODE
Accept
Cut
Copy
Pas
ReadP
WriteP
Status
Data
Value
Mode
Info
Syntax
Enter Password
Password:
OK
Cancel



User	Time Forma	Date Sep	Date Foi	Application Control	Monitor Access Le	User Name	
1	↓ 24 hr	↓ Hyphe	↓ YY M	↓ ▤▤▤▤▤▤	↓ Read/Write	westronic	I
2	↓ 24 hr	↓ Hyphe	↓ YY M	↓ ▤▤▤▤▤▤	↓ Read/Write	reid	a
3	↓ 24 hr	↓ Hyphe	↓ YY M	↓ ▤▤▤▤▤▤	↓ Read Only	readonly	I
4	↓ 24 hr	↓ Hyphe	↓ YY M	↓ ▤▤▤▤▤▤	↓ Maintenance	maintenance	I

Time display format.

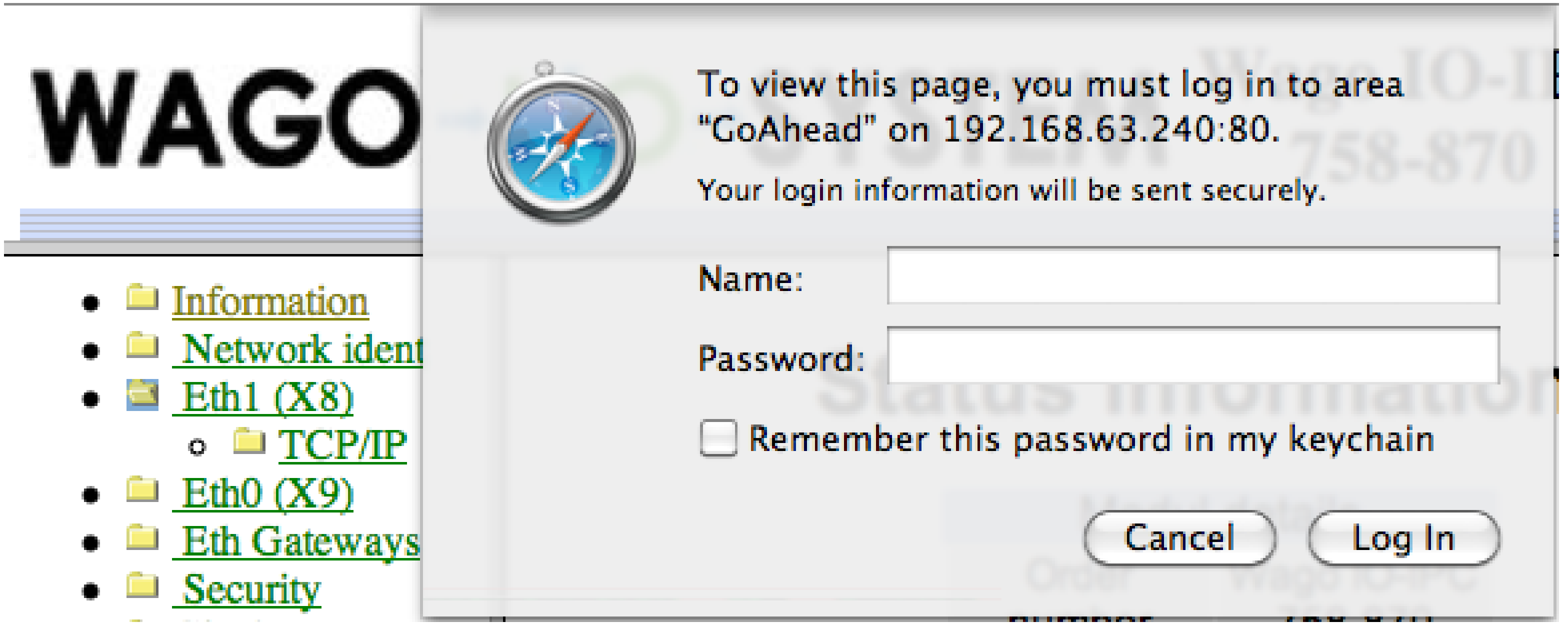


Controller Security Status: SECURED

Password Status: Password exists in controller.

Path to controller:

[redacted] ETHIP-2\192.168.1.33\Backplai



To view this page, you must log in to area "GoAhead" on 192.168.63.240:80.

Your login information will be sent securely.

Name:

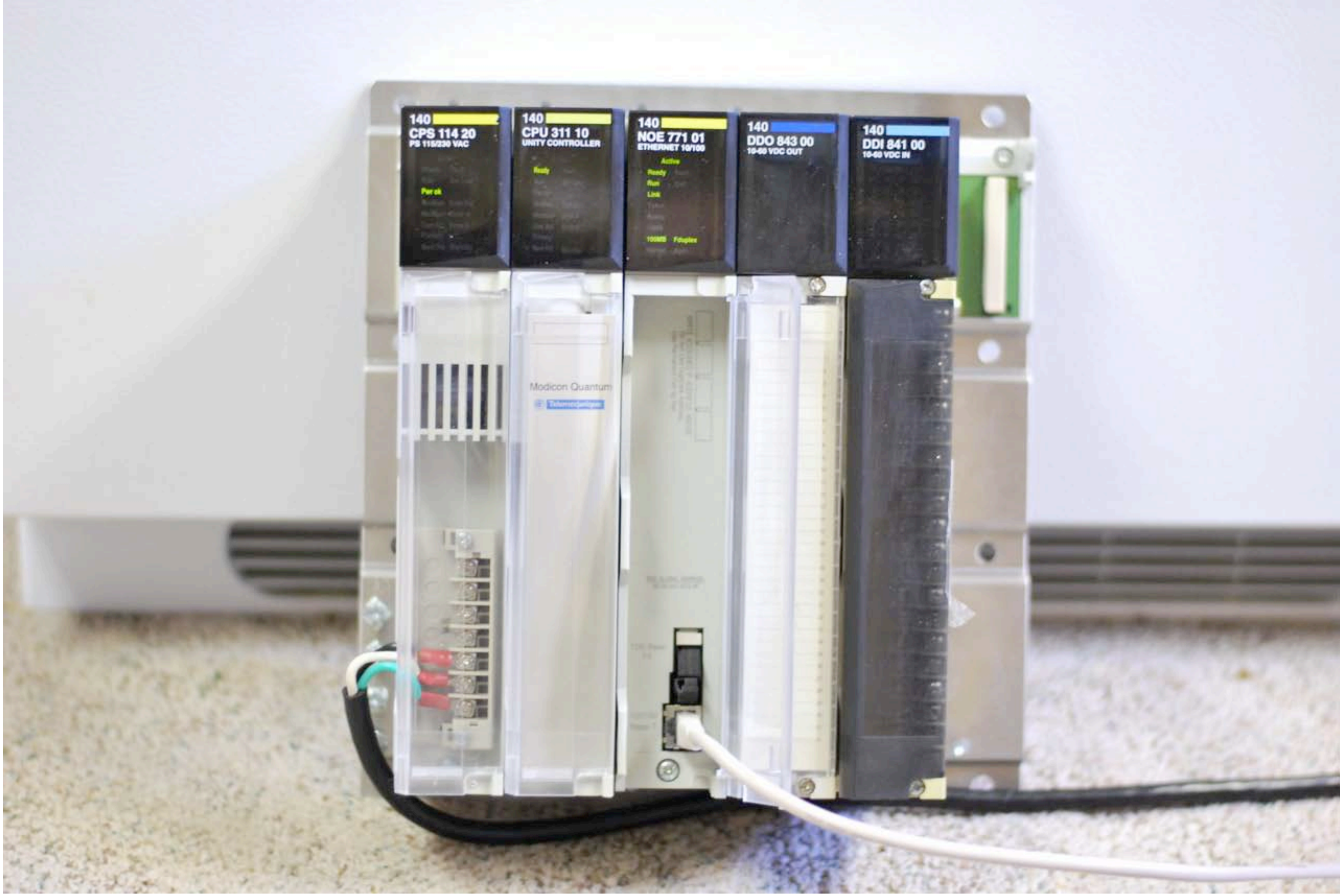
Password:

□ Remember this password in my keychain

The search for more exploits

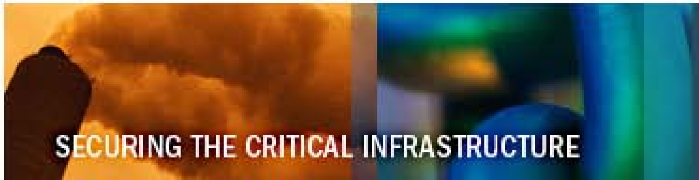
Stuxnet + Beresford Fun

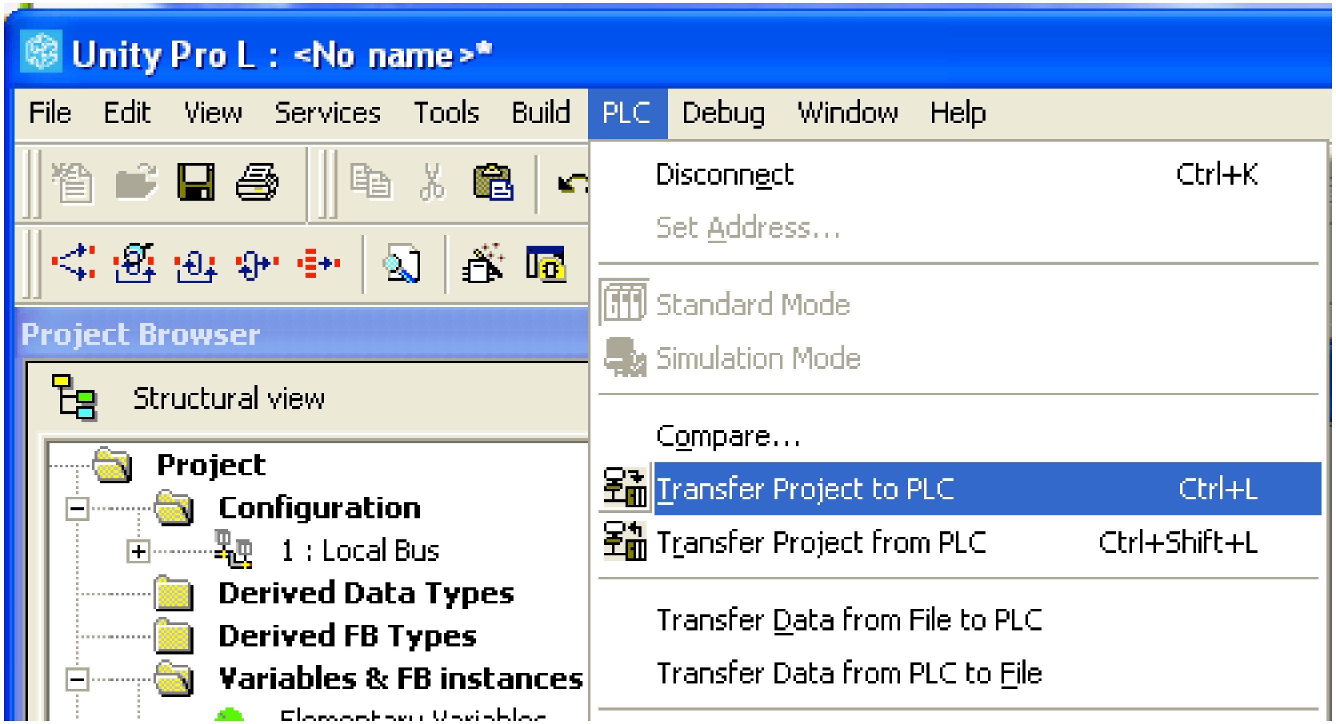
- Stuxnet showed ladder-logic ‘hooking’
- Beresford showed weakness in Siemens controllers that ‘bad guys’ could use
- Most PLCs have the ‘Beresford/Stuxnet’ vuln
  - Download ladder logic without authentication
  - Upload ladder logic without authentication
  - Code-hooking can combine the two with a simple Langner-style ‘logic time bomb’

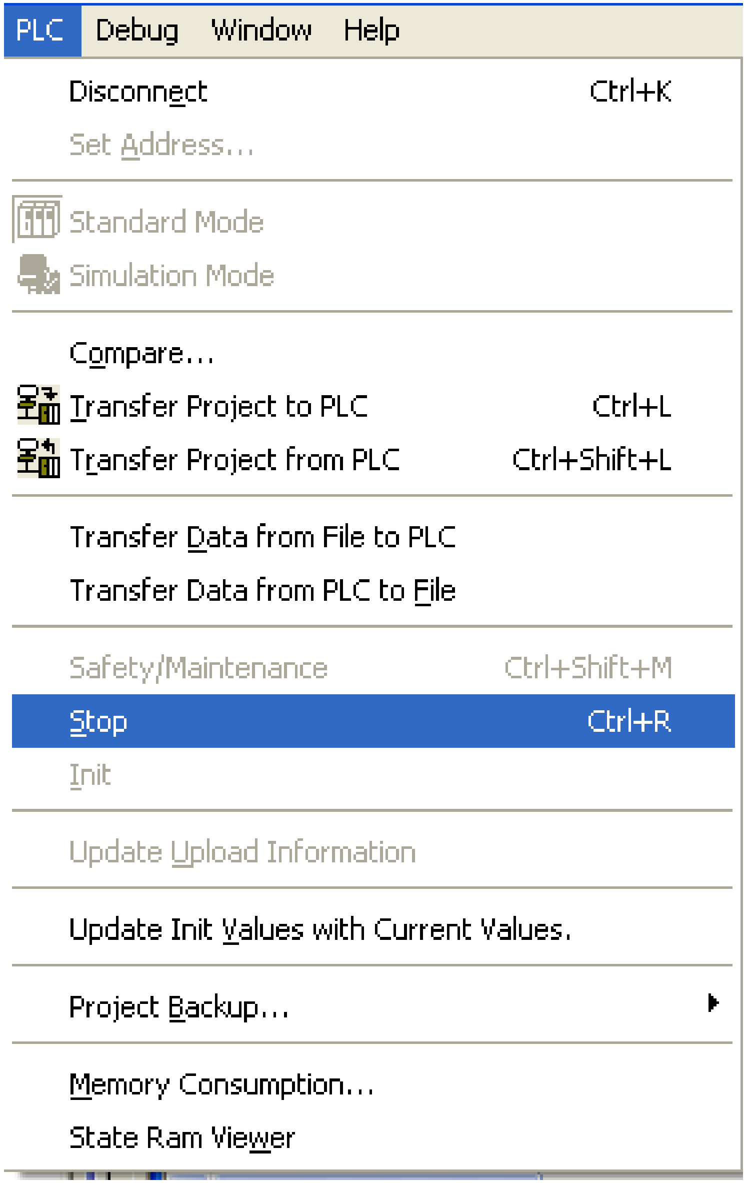

140
CPS 114 20
PS 115/230 VAC
140
CPU 311 10
UNITY CONTROLLER
140
NOE 771 01
ETHERNET 10/100
140
DDO 843 00
10-60 VDC OUT
140
DDI 841 00
10-60 VDC IN
Modicon Quantum
Telemecanique

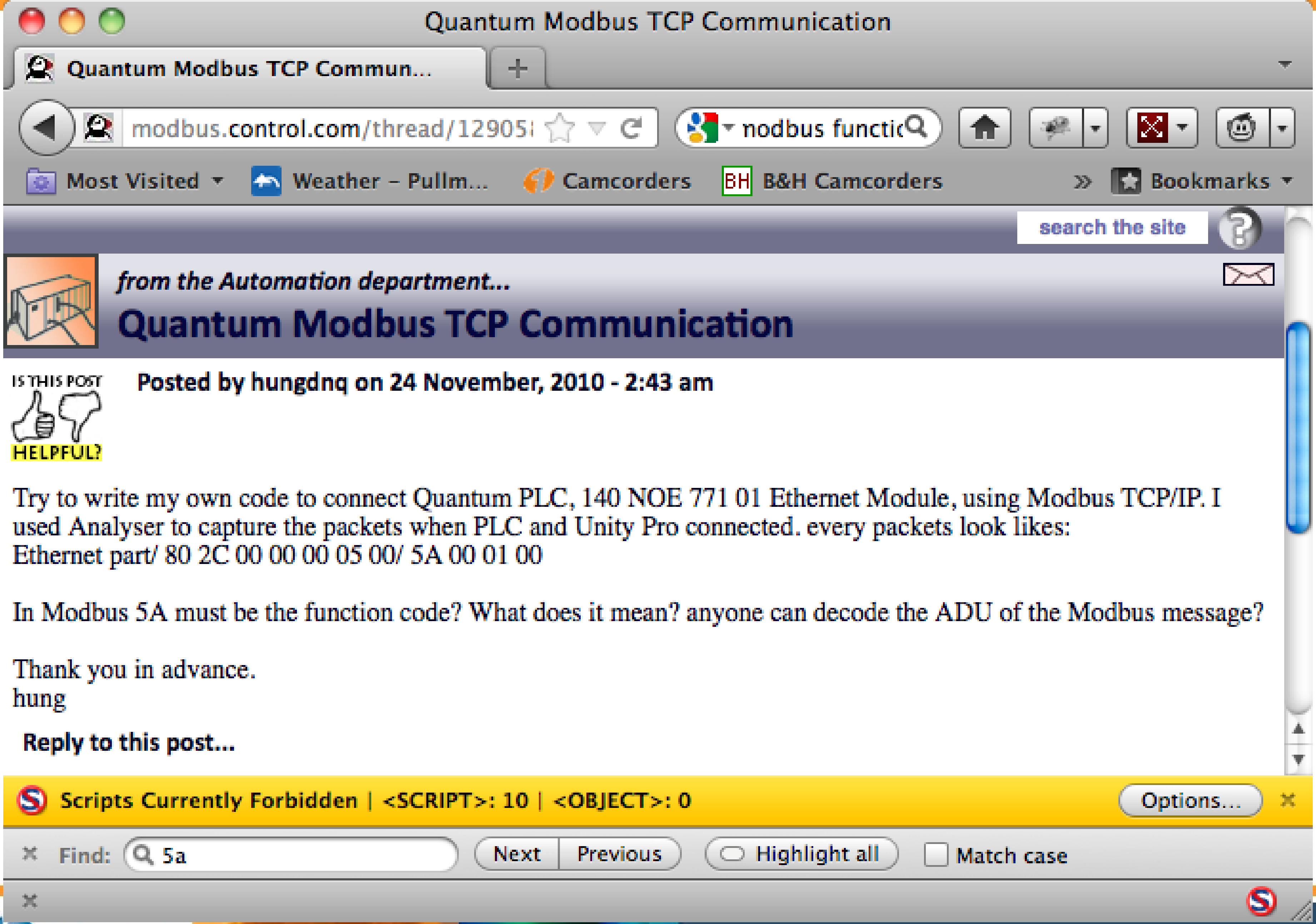
Modicon

- Modbus used for Engineering Access
- Special Function Code 90: “Unity”
  - Lets us STOP the CPU
  - Lets us retrieve/overwrite ladder logic




Unity Pro L : <No name >*
File Edit View Services Tools Build PLC Debug Window Help
Project Browser
Structural view
Project
Configuration
1 : Local Bus
Derived Data Types
Derived FB Types
Variables & FB instances
Elementary Variables
Disconnect Ctrl+K
Set Address...
Standard Mode
Simulation Mode
Compare...
Transfer Project to PLC Ctrl+L
Transfer Project from PLC Ctrl+Shift+L
Transfer Data from File to PLC
Transfer Data from PLC to File


PLC
Debug
Window
Help
Disconnect Ctrl+K
Set Address...
Standard Mode
Simulation Mode
Compare...
Transfer Project to PLC Ctrl+L
Transfer Project from PLC Ctrl+Shift+L
Transfer Data from File to PLC
Transfer Data from PLC to File
Safety/Maintenance Ctrl+Shift+M
Stop Ctrl+R
Init
Update Upload Information
Update Init Values with Current Values.
Project Backup...
Memory Consumption...
State Ram Viewer


Quantum Modbus TCP Communication
Quantum Modbus TCP Commun...
modbus.control.com/thread/12905
nodbus functic
Most Visited
Weather - Pullm...
Camcorders
B&H Camcorders
Bookmarks
search the site
Scripts Currently Forbidden | <SCRIPT>: 10 | <OBJECT>: 0
Options...
Find: 5a
Next
Previous
Highlight all
Match case

from the Automation department...

Quantum Modbus TCP Communication

IS THIS POST HELPFUL?

Posted by hungdnq on 24 November, 2010 - 2:43 am

Try to write my own code to connect Quantum PLC, 140 NOE 771 01 Ethernet Module, using Modbus TCP/IP. I used Analyser to capture the packets when PLC and Unity Pro connected. every packets look likes:
Ethernet part/ 80 2C 00 00 00 05 00/ 5A 00 01 00

In Modbus 5A must be the function code? What does it mean? anyone can decode the ADU of the Modbus message?

Thank you in advance.
hung

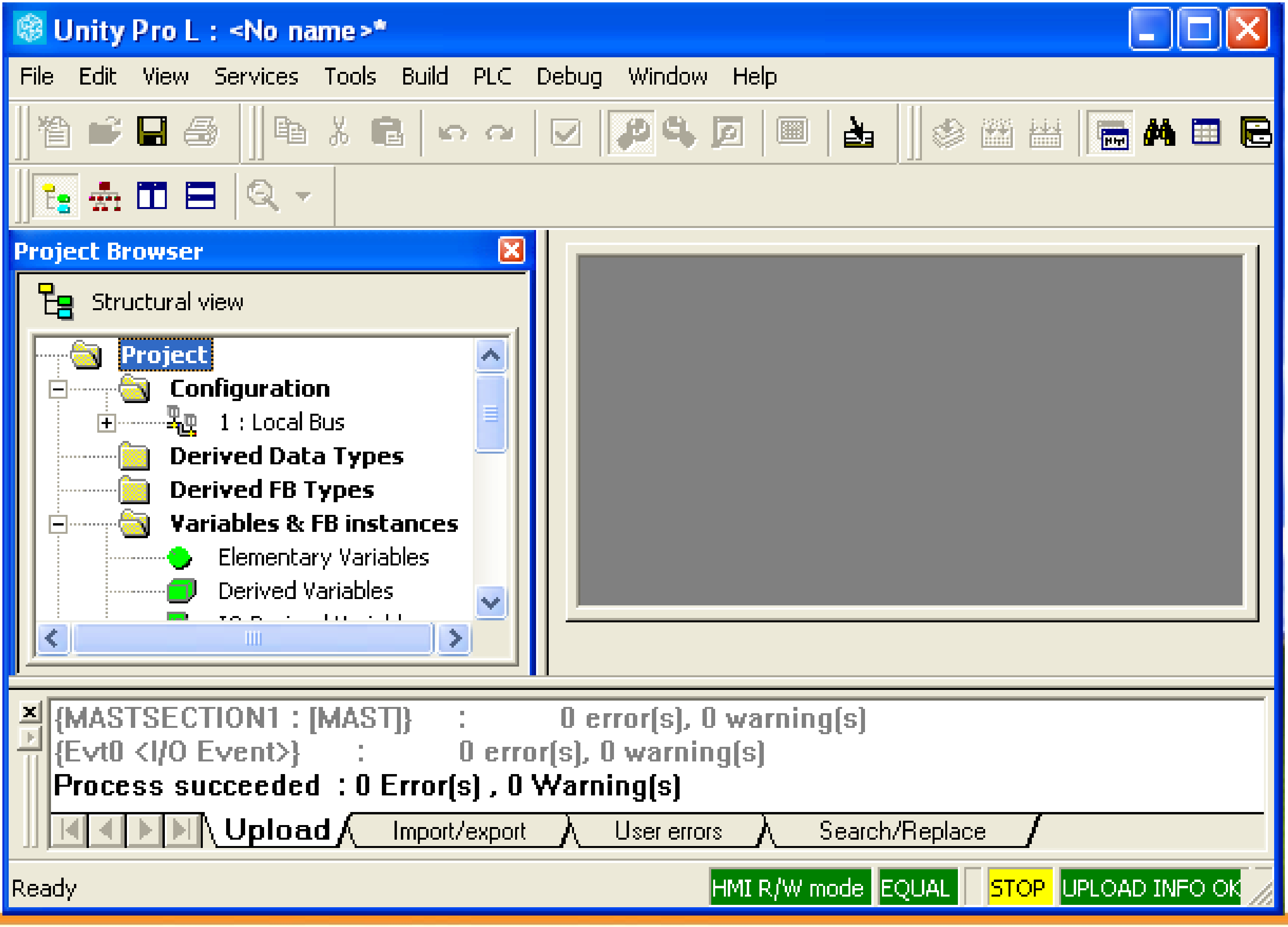
Reply to this post...

Modicon

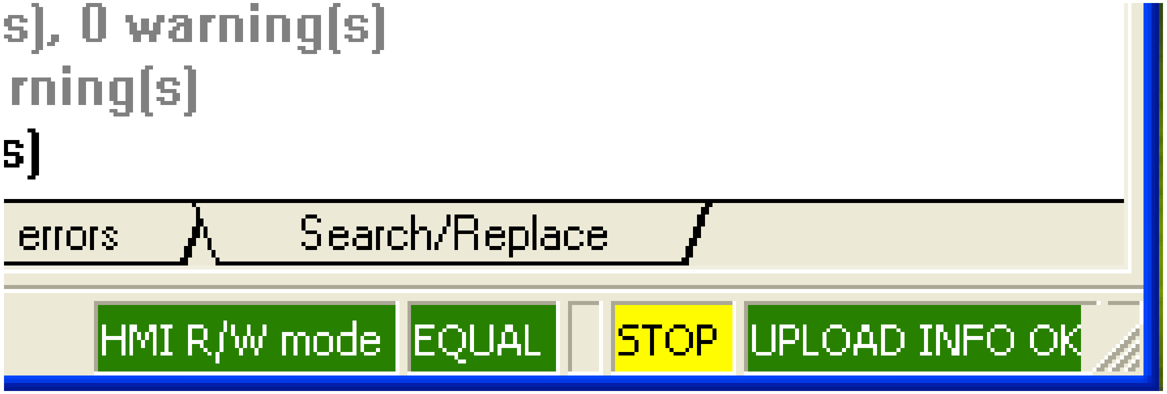
- No authentication for any operation, but…
- …Unity == Chatty
- Quick Python code to isolate packets
  - Walk through .pcap, find unique packets
  - Analyze in Wireshark
  - Find Ladder Logic Upload/Download
  - Find CPU STOP
- Replay commands

Modicon – CPU STOP

- ~100 packets to initialize conversation
- One packet to STOP CPU
  - FC 90
  - Payload 0x01, 0x41, 0xff, 0x00
  - (Start is 0x01, 0x40, 0xff, 0x00)



```
{MASTSECTION1 : [MAST]}      :          0 error(s), 0 warning(s)
{Evt0 <I/O Event>}      :          0 error(s), 0 warning(s)
Process succeeded  : 0 Error(s) , 0 Warning(s)
```



```
s), 0 warning(s)
rning(s)
s)
```

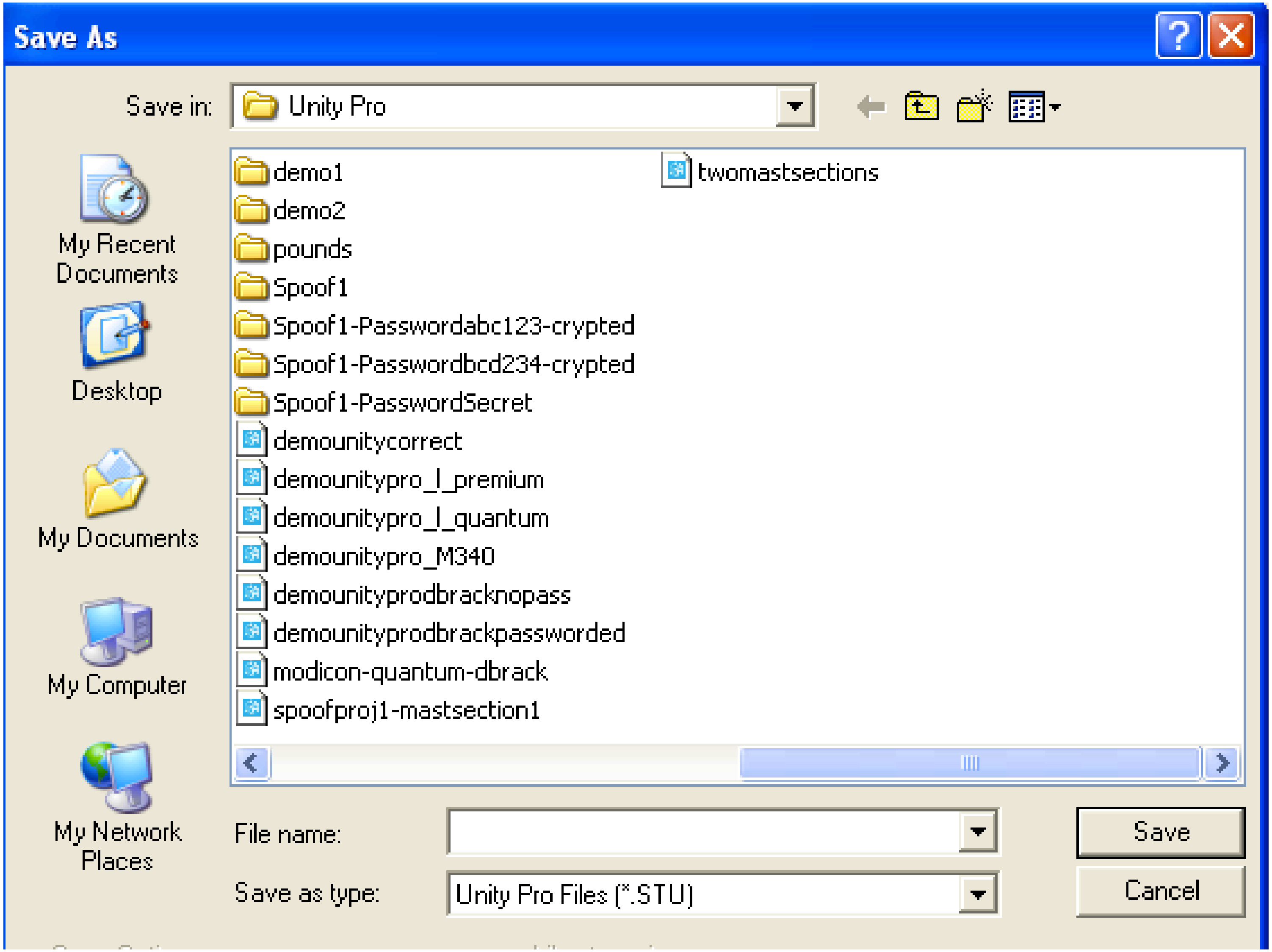
Modicon – Logic Upload

- ~100 packets to initialize (same)
- Split into ~240 byte blocks (max size of Modbus packet + some overhead bytes)
- Second block must be sent twice
  - No idea why
  - Repeated testing

Modicon – Logic Upload

...But...what file do we transfer?

Great question!



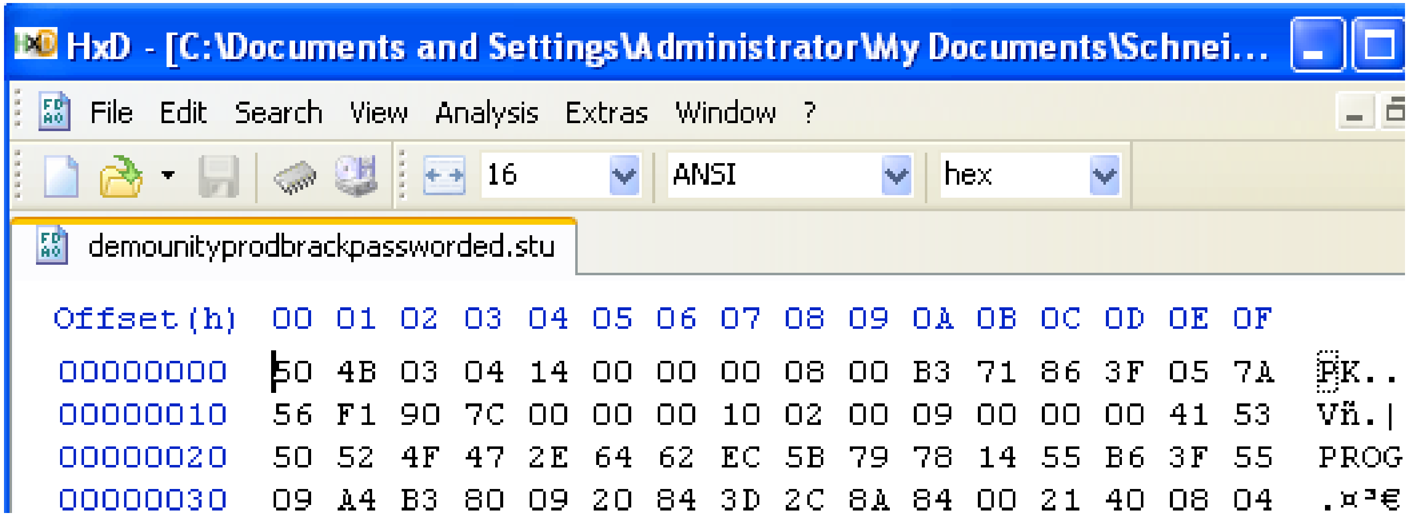
Save As

Save in: Unity Pro

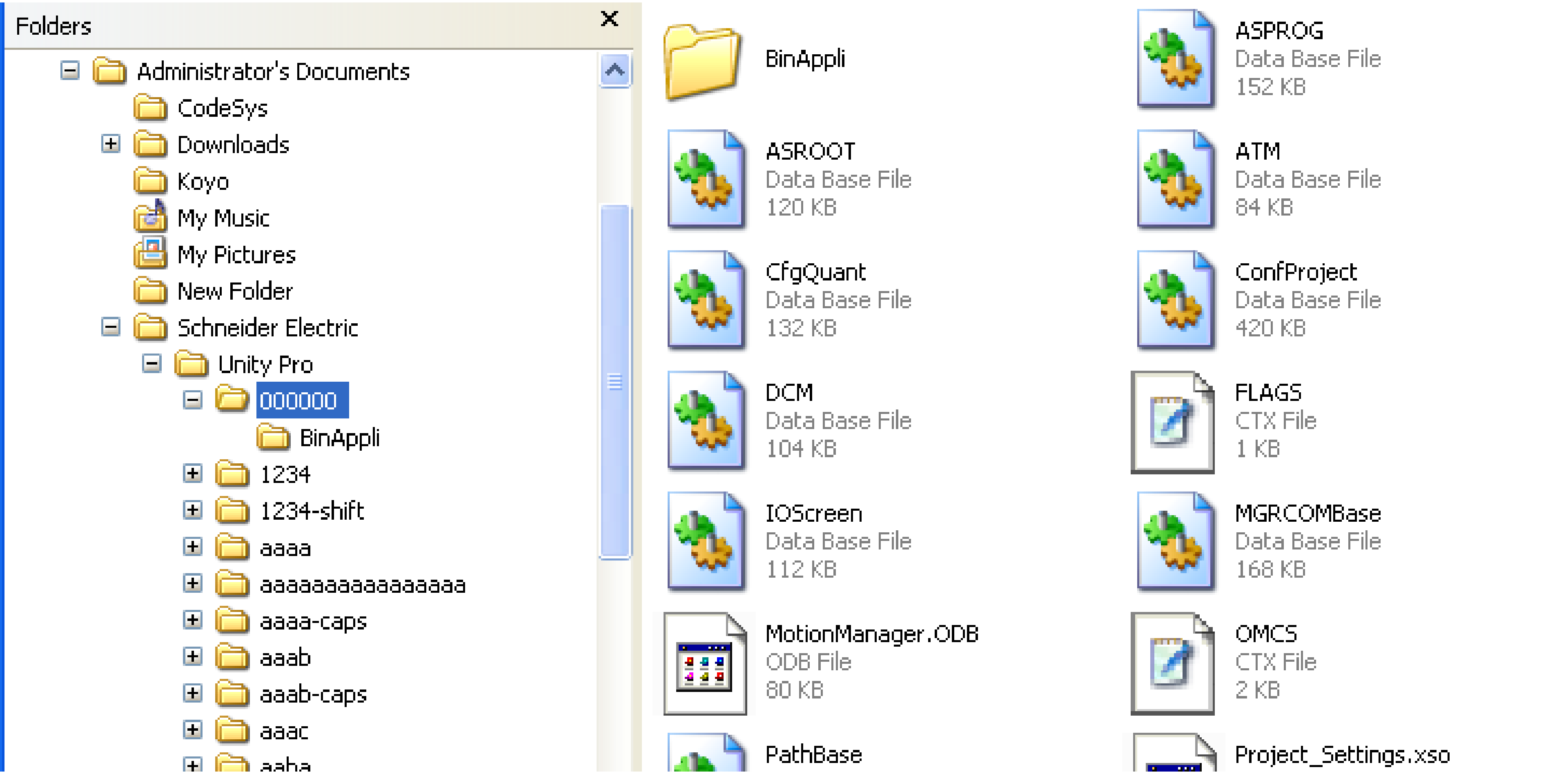
- demo1
- demo2
- pounds
- Spoof1
- Spoof1-Passwordabc123-crypted
- Spoof1-Passwordbcd234-crypted
- Spoof1-PasswordSecret
- demounitycorrect
- demounitypro_l_premium
- demounitypro_l_quantum
- demounitypro_M340
- demounityprodbracknopass
- demounityprodbrackpassworded
- modicon-quantum-dbrack
- spoofproj1-mastsection1
- twomastsections

File name:

Save as type: Unity Pro Files (*.STU)


HxD - [C:\Documents and Settings\Administrator\My Documents\Schnei...
File
Edit
Search
View
Analysis
Extras
Window
?
16
ANSI
hex
demounityprodbrackpassworded.stu

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   50 4B 03 04 14 00 00 00 08 00 B3 71 86 3F 05 7A  PK..
00000010   56 F1 90 7C 00 00 00 10 02 00 09 00 00 00 41 53  Vñ.|
00000020   50 52 4F 47 2E 64 62 EC 5B 79 78 14 55 B6 3F 55  PROG
00000030   09 A4 B3 80 09 20 84 3D 2C 8A 84 00 21 40 08 04  .¤³€
```

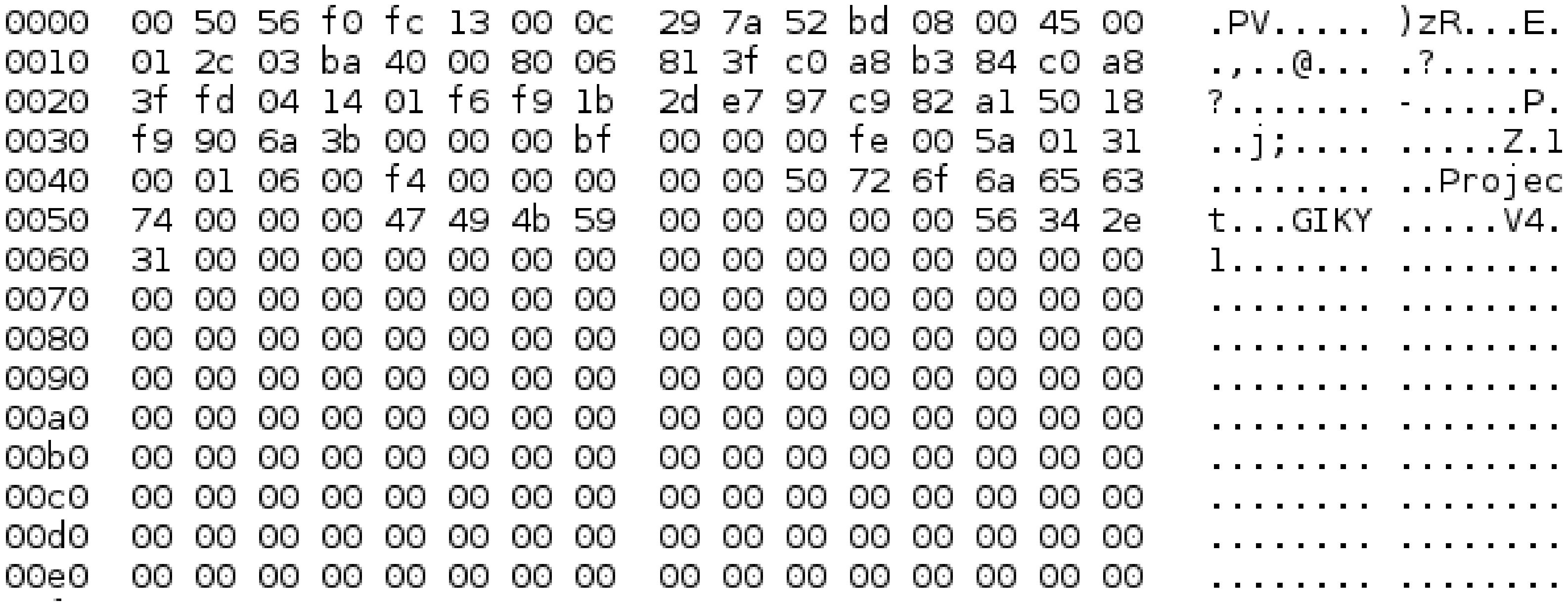


```
Folders                                   ✕
  ⊟ Administrator's Documents
       CodeSys
     ⊞ Downloads
       Koyo
       My Music
       My Pictures
       New Folder
     ⊟ Schneider Electric
        ⊟ Unity Pro
           ⊟ 000000
                BinAppli
           ⊞ 1234
           ⊞ 1234-shift
           ⊞ aaaa
           ⊞ aaaaaaaaaaaaaaaa
           ⊞ aaaa-caps
           ⊞ aaab
           ⊞ aaab-caps
           ⊞ aaac
           ⊞ aaba
```

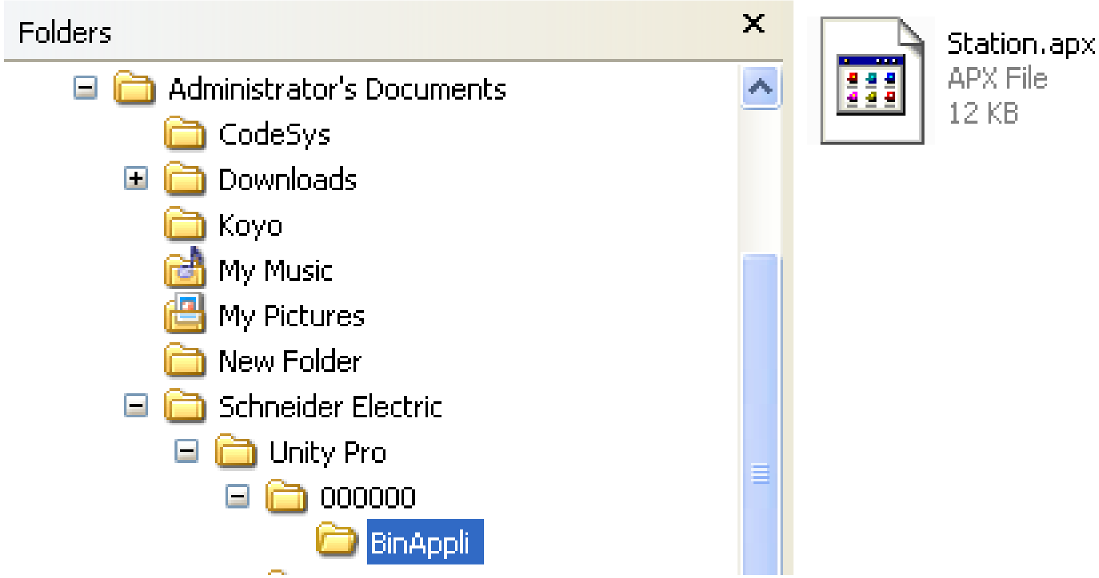
```
BinAppli                        ASPROG
                                Data Base File
                                152 KB

ASROOT                          ATM
Data Base File                  Data Base File
120 KB                          84 KB

CfgQuant                        ConfProject
Data Base File                  Data Base File
132 KB                          420 KB

DCM                             FLAGS
Data Base File                  CTX File
104 KB                          1 KB

IOScreen                        MGRCOMBase
Data Base File                  Data Base File
112 KB                          168 KB

MotionManager.ODB               OMCS
ODB File                        CTX File
80 KB                           2 KB

PathBase                        Project_Settings.xso
```

Back to the PCAP

Block 7 contains strings to search for



```
0000   00 50 56 f0 fc 13 00 0c  29 7a 52 bd 08 00 45 00    .PV..... )zR...E.
0010   01 2c 03 ba 40 00 80 06  81 3f c0 a8 b3 84 c0 a8    .,..@... .?......
0020   3f fd 04 14 01 f6 f9 1b  2d e7 97 c9 82 a1 50 18    ?....... -.....P.
0030   f9 90 6a 3b 00 00 00 bf  00 00 00 fe 00 5a 01 31    ..j;.... .....Z.1
0040   00 01 06 00 f4 00 00 00  00 00 50 72 6f 6a 65 63    ........ ..Projec
0050   74 00 00 00 47 49 4b 59  00 00 00 00 00 56 34 2e    t...GIKY .....V4.
0060   31 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    1....... ........
0070   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
0080   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
0090   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
00a0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
00b0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
00c0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
00d0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
00e0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ........ ........
```


Folders
Administrator's Documents
CodeSys
Downloads
Koyo
My Music
My Pictures
New Folder
Schneider Electric
Unity Pro
000000
BinAppli
Station.apx
APX File
12 KB

Files

- APX == STL (Statement List)
- APB == FBD (Function Block Diagram)
- Multiple blocks become one file
- Both types may be used at once

Simple attack: Overwrite

- Overwrite a remote Modicon to do nothing
- Alt: randomly operate outputs
- Metasploit module shows how it’s done

More complicated: Stuxnet

- Retrieve logic from remote system
- Parse it and wrap it
  - Parsing the output probably the hardest step
  - Alt: Just use Unity to edit the file (it’s what the pros would do)
- Re-upload

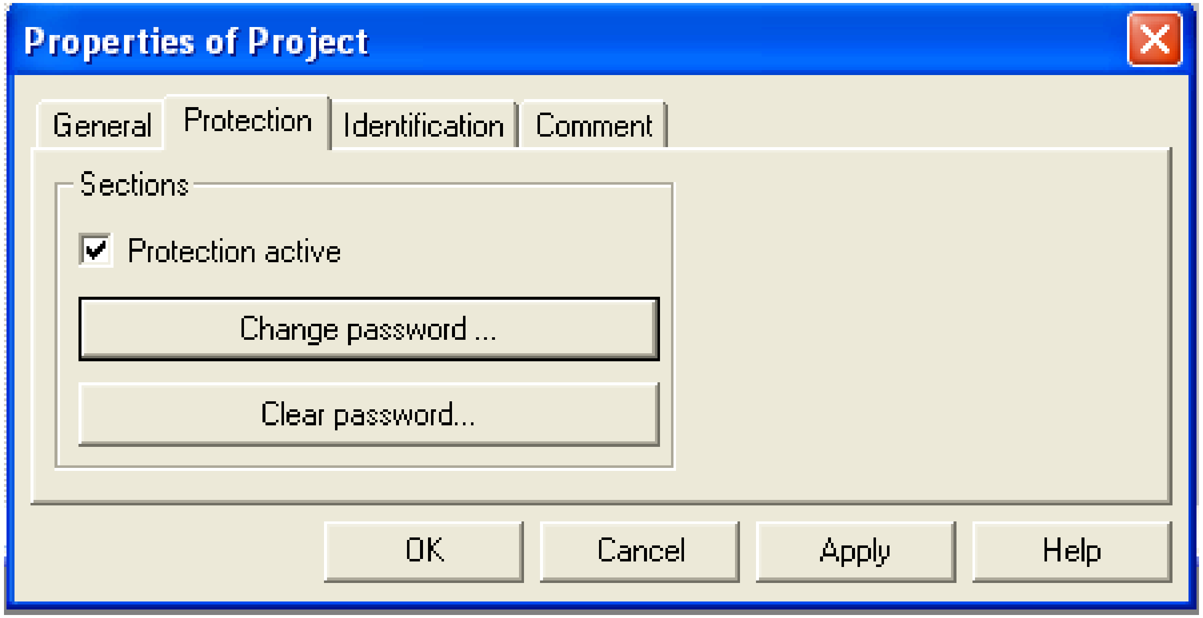
Time spent

- Level of difficulty: miniscule
- < 8 hours from first packet capture to successful file upload/download

Password (Un)protection

- Password protection applies to APX and APB files
- Does not prevent overwrite of existing files
- Does prevent Unity from opening the ‘source code’
- Protection is really crappy

Password (Un)protection

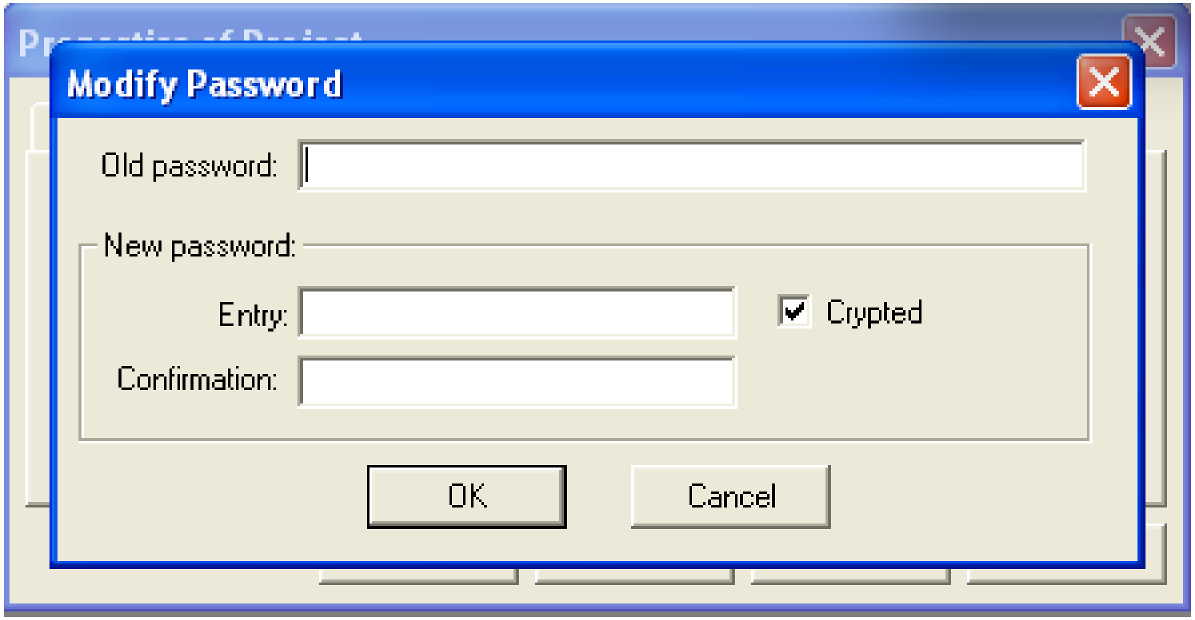


Properties of Project

Sections

☑ Protection active

Password (Un)protection



Modify Password

Old password:

New password:

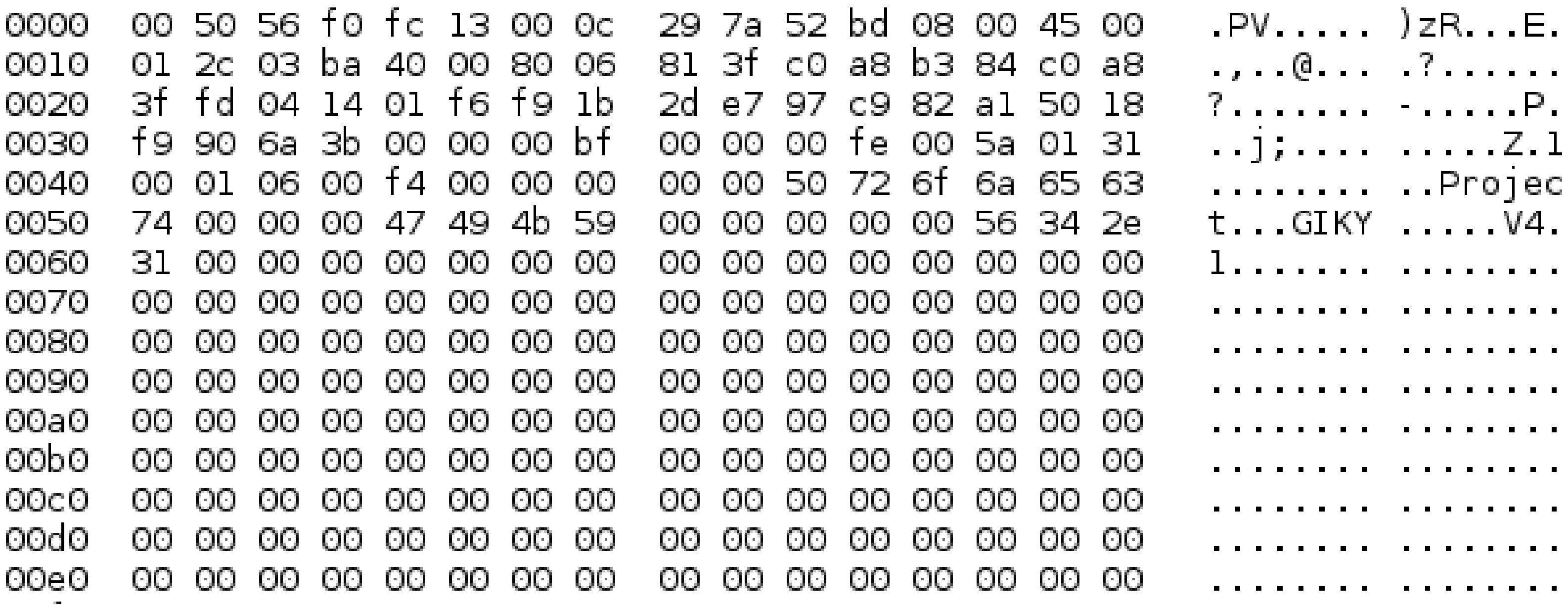
Entry:

☑ Crypted

Confirmation:

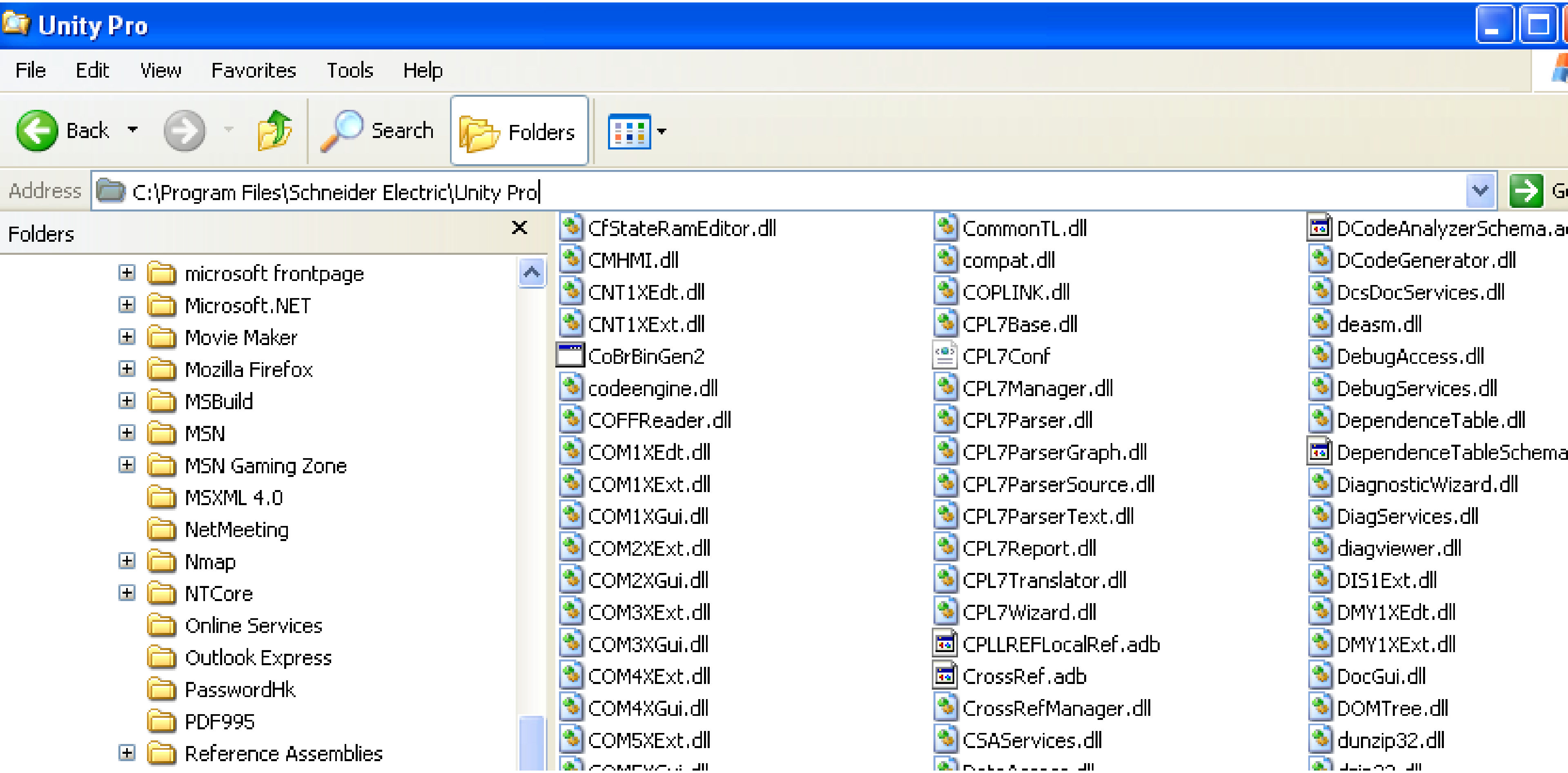
Back to the PCAP

Block 7 contains strings to search for



```
0000  00 50 56 f0 fc 13 00 0c  29 7a 52 bd 08 00 45 00   .PV..... )zR...E.
0010  01 2c 03 ba 40 00 80 06  81 3f c0 a8 b3 84 c0 a8   .,..@... .?......
0020  3f fd 04 14 01 f6 f9 1b  2d e7 97 c9 82 a1 50 18   ?....... -.....P.
0030  f9 90 6a 3b 00 00 00 bf  00 00 00 fe 00 5a 01 31   ..j;.... .....Z.1
0040  00 01 06 00 f4 00 00 00  00 00 50 72 6f 6a 65 63   ........ ..Projec
0050  74 00 00 00 47 49 4b 59  00 00 00 00 00 56 34 2e   t...GIKY .....V4.
0060  31 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   1....... ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

349 DLLs!



C:\Program Files\Schneider Electric\Unity Pro

Folders

microsoft frontpage
Microsoft.NET
Movie Maker
Mozilla Firefox
MSBuild
MSN
MSN Gaming Zone
MSXML 4.0
NetMeeting
Nmap
NTCore
Online Services
Outlook Express
PasswordHk
PDF995
Reference Assemblies

CfStateRamEditor.dll
CMHMI.dll
CNT1XEdt.dll
CNT1XExt.dll
CoBrBinGen2
codeengine.dll
COFFReader.dll
COM1XEdt.dll
COM1XExt.dll
COM1XGui.dll
COM2XExt.dll
COM2XGui.dll
COM3XExt.dll
COM3XGui.dll
COM4XExt.dll
COM4XGui.dll
COM5XExt.dll
COM5XGui.dll

CommonTL.dll
compat.dll
COPLINK.dll
CPL7Base.dll
CPL7Conf
CPL7Manager.dll
CPL7Parser.dll
CPL7ParserGraph.dll
CPL7ParserSource.dll
CPL7ParserText.dll
CPL7Report.dll
CPL7Translator.dll
CPL7Wizard.dll
CPLLREFLocalRef.adb
CrossRef.adb
CrossRefManager.dll
CSAServices.dll
DataAccess.dll

DCodeAnalyzerSchema.a
DCodeGenerator.dll
DcsDocServices.dll
deasm.dll
DebugAccess.dll
DebugServices.dll
DependenceTable.dll
DependenceTableSchema
DiagnosticWizard.dll
DiagServices.dll
diagviewer.dll
DIS1Ext.dll
DMY1XEdt.dll
DMY1XExt.dll
DocGui.dll
DOMTree.dll
dunzip32.dll
dzip32.dll

Password (Un)protection

- Password stored in .APX and .APB files
- Offset ~0x4C8
- Password in plaintext is...plaintext
- Password ‘encrypted’:
  - aaaa => YCOG
  - aaab => 5BB1
  - aaba => 5BDA
  - abaa => 5U1B
  - baaa => 5BBU

Password (Un)protection

- Project is not encrypted, only password is
- Change password to known-value (hexedit)
- Modicon “Password Proxy” could strip password

Password (Un)protection

Modicon password is dumb no matter who you are:

- Hate security? It’s annoying!
- Love security? It doesn’t do anything!

< / Modicon >

- ‘modiconstux’ and ‘modiconstop’ available today
  - Overwrite the ladder logic in that pesky controller
  - STOP or RUN your (least) favorite controller
- Password proxy stripper TBA
- Aside from that, it’s been p0wn3d enough
- What I want:

Schneider -- give me a security roadmap so that I can start recommending your products.

More New Stuff: WAGO

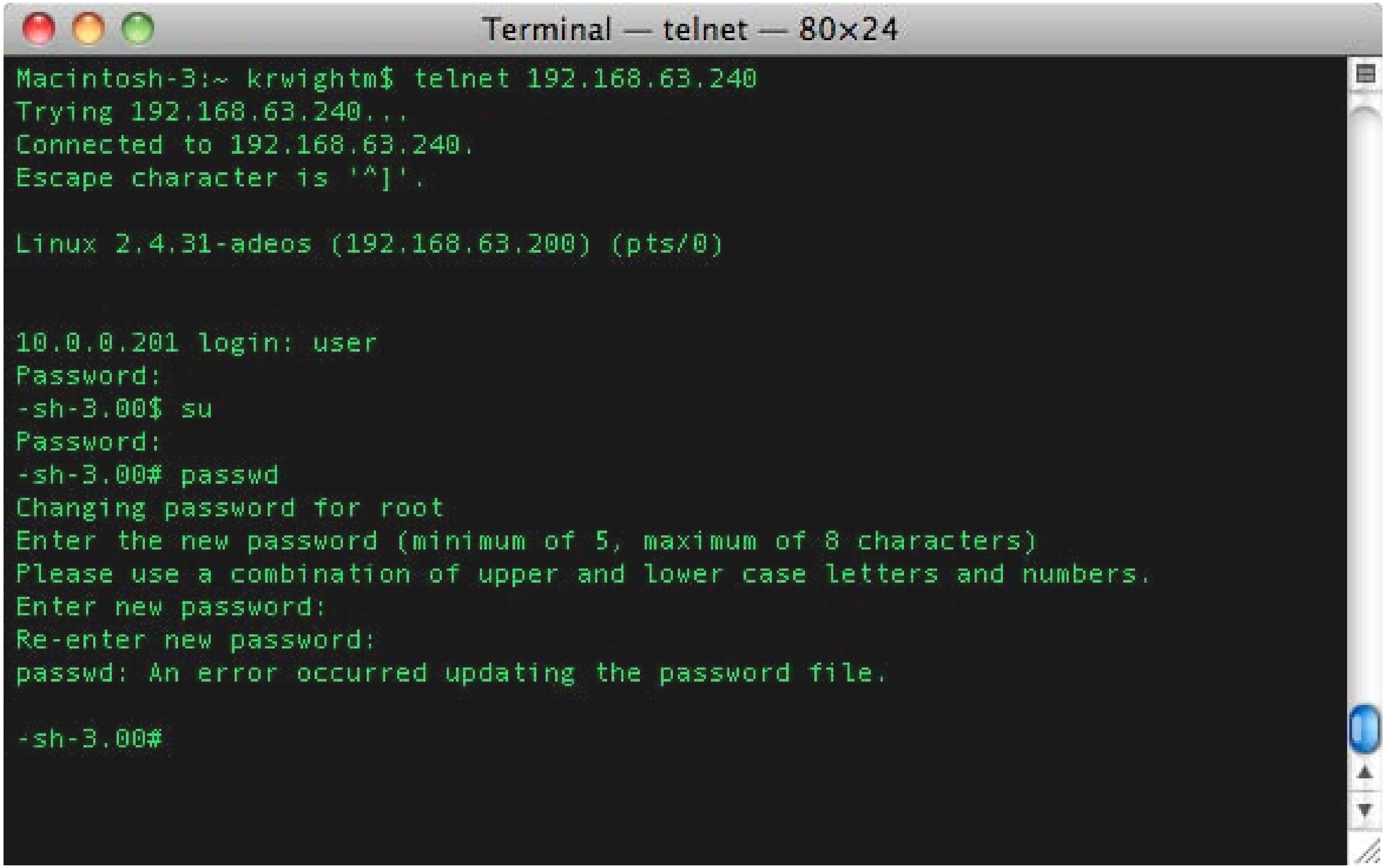
- Russian group DsecRG released vulns with Basecamp
  - CSRF
  - default credentials
- Lots of other vulns + backdoors + FUN!

WAGO

- My model: IPC 758-870
- 266Mhz x86, 32MB flash, 32MB ram
- Linux 2.4.31

WAGO

- Hard-Coded user accounts
  - guest/guest
  - user/user00
  - root/ko2003wa (requires su)
- Open telnet, ftp services
  - Upload files and run them
  - Just like any other Linux box
  - Successfully compiled tinyproxy, tor

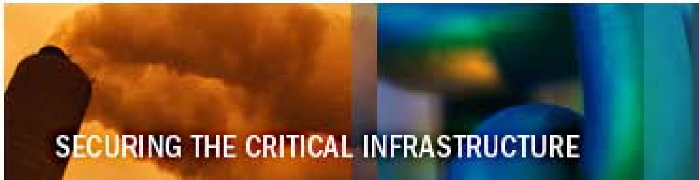


```
Macintosh-3:~ krwightm$ telnet 192.168.63.240
Trying 192.168.63.240...
Connected to 192.168.63.240.
Escape character is '^]'.

Linux 2.4.31-adeos (192.168.63.200) (pts/0)


10.0.0.201 login: user
Password:
-sh-3.00$ su
Password:
-sh-3.00# passwd
Changing password for root
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Re-enter new password:
passwd: An error occurred updating the password file.

-sh-3.00#
```

WAGO Ladder Logic

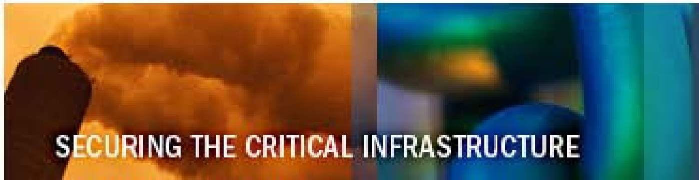
3S-Software CoDeSys

- Most amazing ladder logic implementation ever
- Used by hundreds of manufacturers
- Security--



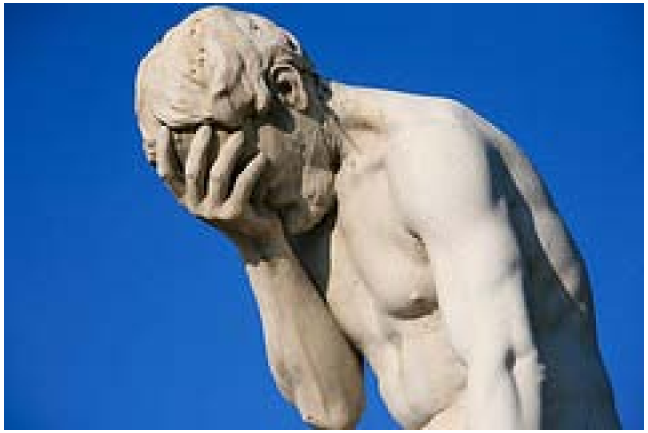
CoDeSys – How it works

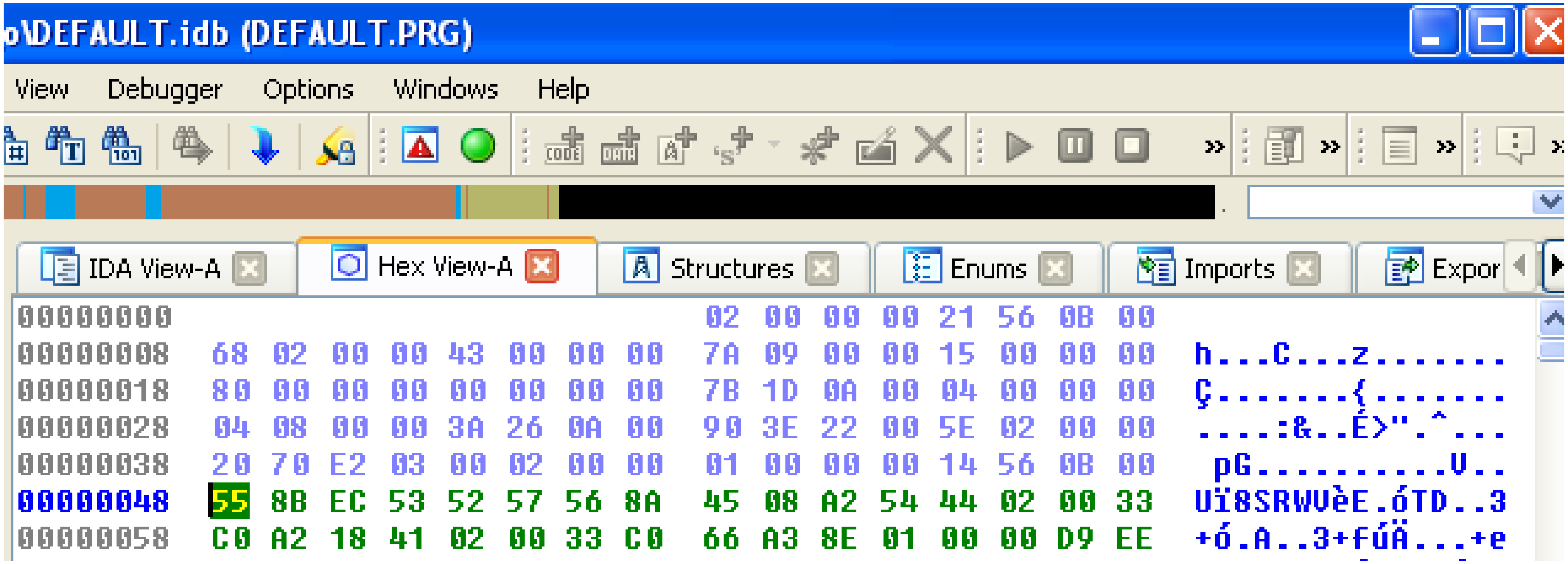
1) Engineer writes their logic
2) Engineering software compiles binary
3) Binary transferred to PLC (no authentication!)
4) PLC loads binary into memory, jumps inside



Remember PLC Notes?

- Very few PLCs use MMU
- WAGO does (Linux on x86, yay)
- ...But the CoDeSys process runs as root





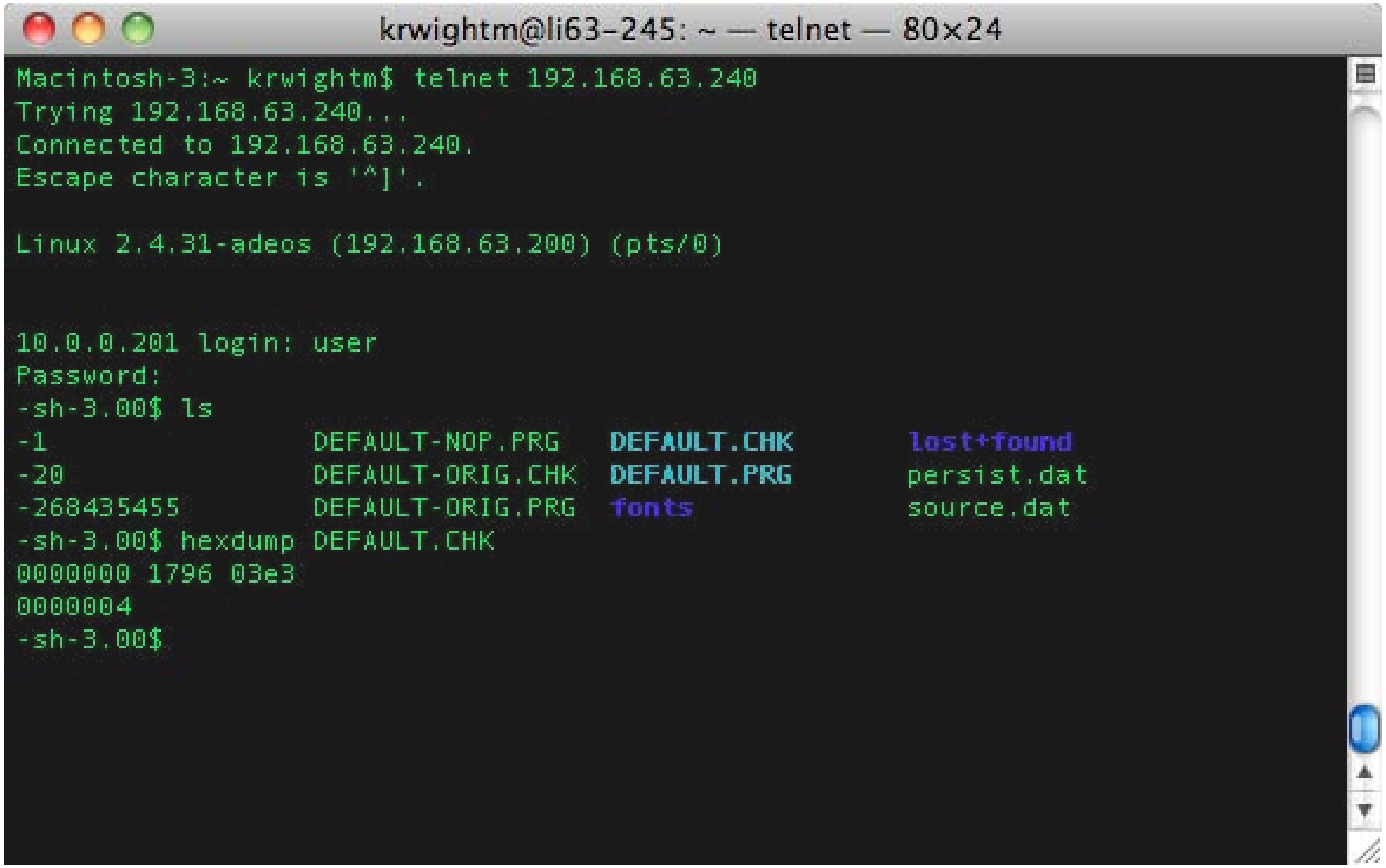
```
00000000                                    02 00 00 00 21 56 0B 00
00000008  68 02 00 00 43 00 00 00  7A 09 00 00 15 00 00 00  h...C...z.......
00000018  80 00 00 00 00 00 00 00  7B 1D 0A 00 04 00 00 00  Ç.......{.......
00000028  04 08 00 00 3A 26 0A 00  90 3E 22 00 5E 02 00 00  ....:&..É>".^...
00000038  20 70 E2 03 00 02 00 00  01 00 00 00 14 56 0B 00   pG..........V..
00000048  55 8B EC 53 52 57 56 8A  45 08 A2 54 44 02 00 33  Uï8SRWVèE.óTD..3
00000058  C0 A2 18 41 02 00 33 C0  66 A3 8E 01 00 00 D9 EE  +ó.A..3+fúÄ...+e
```

CoDeSys Project Format

- Header
- X86 binary
- Footer
- Don’t really need to understand it to exploit it

CoDeSys Project Format

- World’s longest NOP-sled?
- ~750kb of NOPs followed by a bind shell
- Uploaded to WAGO
- Sadly, FAIL – CRC failure
- Need to RE the CRC (32-bit CRC, stored as .CHK file on filesystem)
- Expect an update and metasploit poc in a few weeks



```
Macintosh-3:~ krwightm$ telnet 192.168.63.240
Trying 192.168.63.240...
Connected to 192.168.63.240.
Escape character is '^]'.

Linux 2.4.31-adeos (192.168.63.200) (pts/0)


10.0.0.201 login: user
Password:
-sh-3.00$ ls
-1                DEFAULT-NOP.PRG   DEFAULT.CHK       lost+found
-20               DEFAULT-ORIG.CHK  DEFAULT.PRG       persist.dat
-268435455        DEFAULT-ORIG.PRG  fonts             source.dat
-sh-3.00$ hexdump DEFAULT.CHK
0000000 1796 03e3
0000004
-sh-3.00$
```

Dear 3S-Software

- You are in an amazing position to promote secure ladder logic transfer
- A little goes a long way in this area

Basecamp responses

- A-B decent
  - gave quick mitigation information
  - provided Snort signatures
  - ...still waiting for long-term fix for CIP
- Schneider has said little since Rubén’s backdoor disclosure
  - “We take security seriously...”
  - (Nevermind the backdoors + other flaws)
- GE has shared nothing
- Koyo has shared nothing