RUXCON '08

SCADA Penetration Testing

Hacking Modbus Enabled Devices

Daniel Grzelak [daniel.grzelak@sift.com.au]

SIFT

About Me

- SIFT
  - http://ww.sift.com.au/
  - Independent information security services
- Daniel Grzelak
  - daniel.grzelak@sift.com.au
  - Consultant and “breakererer of stuff”
  - Not a SCADA engineer

About this Presentation

- Seeks to standardise and illuminate Modbus testing
  - Release a toolkit to aid testing
  - Maybe have some fun along the way

- Based on
  - Research and experience
    - All screenshots in the presentation are from live Internet systems!
  - But also assumptions and conjecture

- What you won’t get
  - 0-day exploits

Outline

i. Brief introduction to Modbus

ii. Motivation for this presentation

iii. Modbus Internet landscape

iv. Penetration testing framework and toolkit

v. Conclusions and acknowledgements

vi. Questions

SCADA

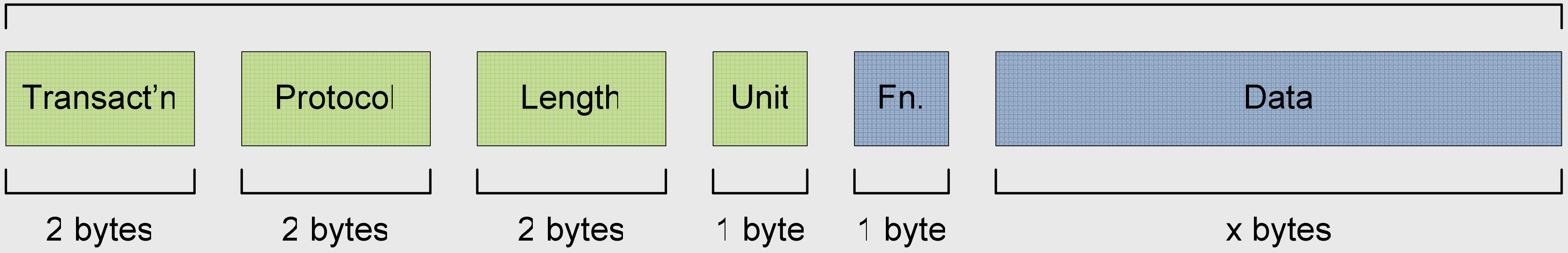
- Supervisory Control and Data Acquisition
- AKA Controlling cool stuff
  - Manufacturing plants
  - Traffic signaling
  - Water supply and filtration
  - Power generation
- Infinite
  - Fun (for hackers)
  - Damage (for crackers)
  - Headaches, fear, and pain (for controllers)
- Difficult to research

Modbus

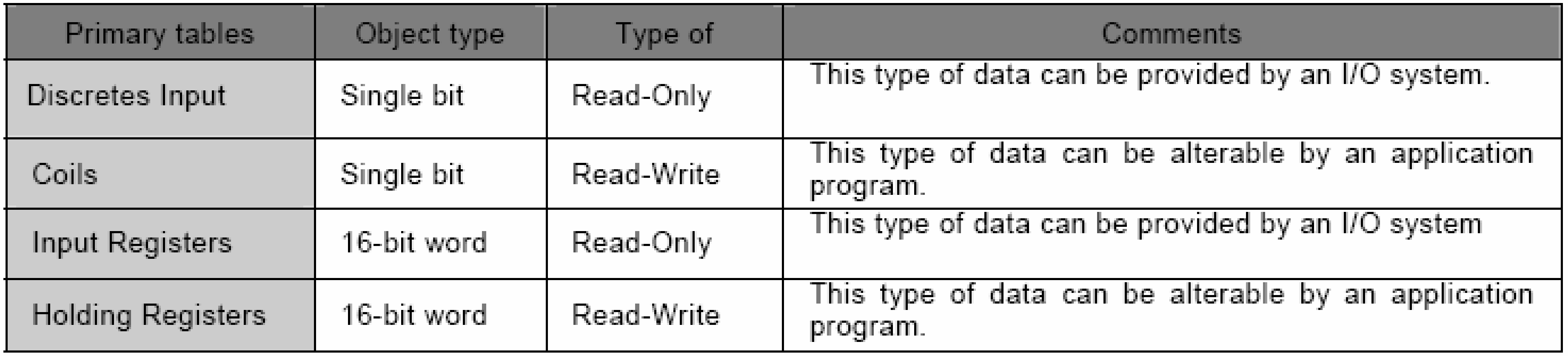
- Open standard
  - www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf
  - www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf
- Application layer protocol
  - For communicating with automation devices
  - Was a serial protocol but now TCP/IP enabled
  - Simple and widely deployed
- Useful Terminology
  - RTU – remote terminal unit (slave)
  - MTU – master terminal unit
  - PLC – programmable logic controller

Modbus/TCP

Modbus TCP/IP Application Data Unit (ADU)



Transact'n	Protocol	Length	Unit	Fn.	Data
2 bytes	2 bytes	2 bytes	1 byte	1 byte	x bytes



Primary tables	Object type	Type of	Comments
Discretes Input	Single bit	Read-Only	This type of data can be provided by an I/O system.
Coils	Single bit	Read-Write	This type of data can be alterable by an application program.
Input Registers	16-bit word	Read-Only	This type of data can be provided by an I/O system
Holding Registers	16-bit word	Read-Write	This type of data can be alterable by an application program.

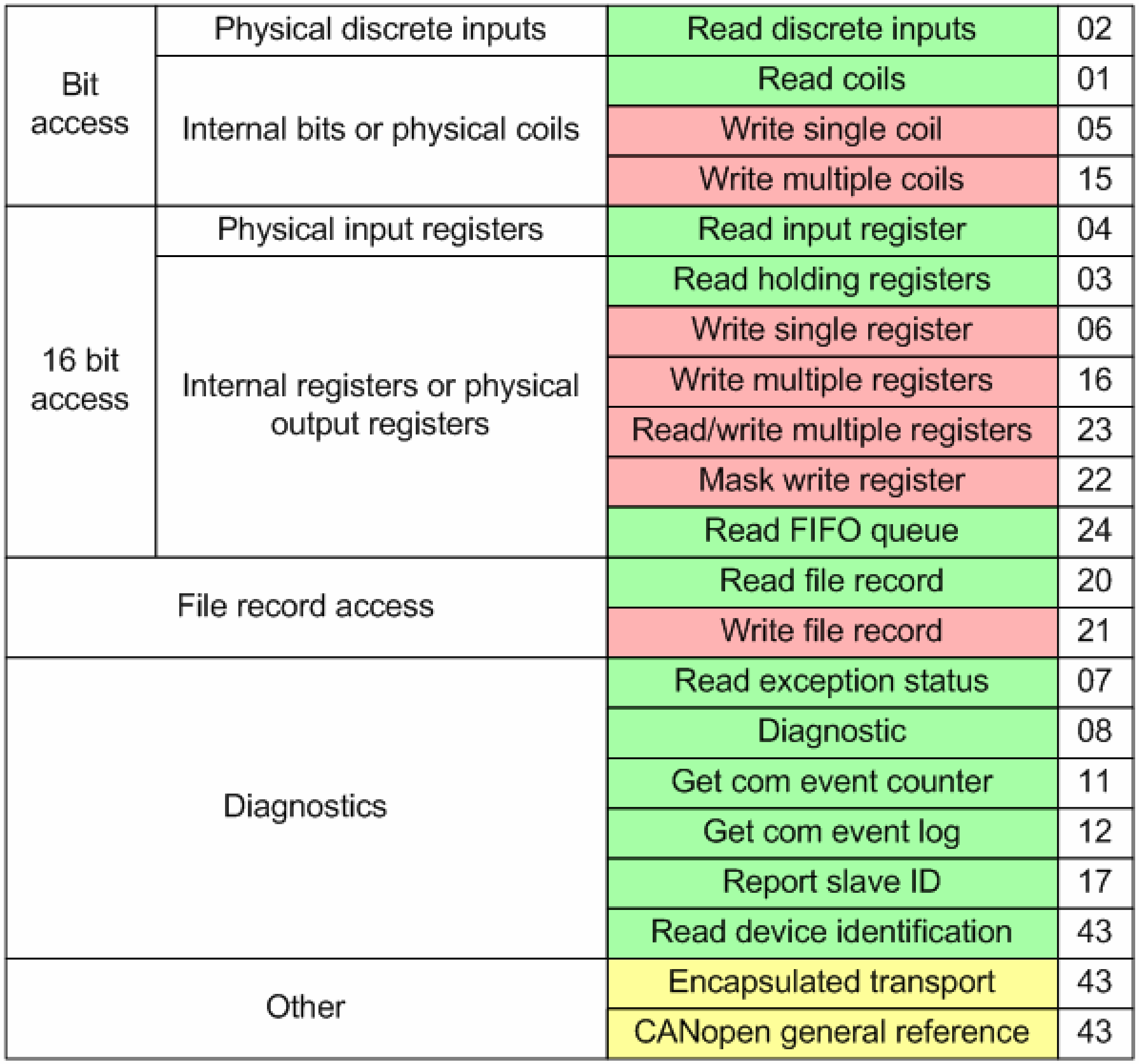
Modbus/TCP Basics

- Synchronous request-response protocol
  - Max packet size of 260 bytes
  - Response function code = request function code (+0x80 error)

- Components
  - Transaction ID usually incremented
  - Protocol ID always 0
  - Length
  - unit/slave ID = 0 - 255
  - function code = 1 – 255

- Protocol number restrictions are always fun!

Common Functions



Bit access	Physical discrete inputs	Read discrete inputs	02
	Internal bits or physical coils	Read coils	01
		Write single coil	05
		Write multiple coils	15
16 bit access	Physical input registers	Read input register	04
	Internal registers or physical output registers	Read holding registers	03
		Write single register	06
		Write multiple registers	16
		Read/write multiple registers	23
		Mask write register	22
		Read FIFO queue	24
File record access		Read file record	20
		Write file record	21
Diagnostics		Read exception status	07
		Diagnostic	08
		Get com event counter	11
		Get com event log	12
		Report slave ID	17
		Read device identification	43
Other		Encapsulated transport	43
		CANopen general reference	43

Current State of Modbus Pen Testing

- Process Control Systems Forum (PCSF) Annual Meeting [March, 2007]
  - Setup honeynet with simulated Modbus PLC
  - Attendees given access to wireless AP hosting honeynet and told go wild
  - "One attendee performed 913 function code 1 reads to an unavailable address/reference (39999)…"
  - IDS identified the following attacks:
    - Unauthorised read
    - Unauthorised write
    - Incorrect packet length (finally something fun)

- https://www.pcsforum.org/library/files/1174588590-PCSF_SCADA_Honeynet.pdf

Current State of Modbus Pen Testing

- Nessus
  - **Modbus/TCP Coil Access** - Modbus uses a function code of 1 to read "coils " in a Modbus slave. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a "write coil" message.
  - **Modbus/TCP Discrete Input Access** - The Modbus protocol function code of 2 reads discrete inputs from Modbus slaves. The ability to read discrete inputs may help an attacker profile a system.
  - **Modicon Modbus/TCP Programming Function Code Access** - Finds hosts with the proprietary Modbus/TCP function code 126 active
  - Little more than reading and writing data values ☹
- http://blog.tenablesecurity.com/2006/12/nessus_3_scada_.htm

Current State of Modbus Pen Testing

- ModScan by Mark Bristow - Defcon 2008
  - Scanner presented by Mark Bristow at Defcon 2008
  - “Modscan Scans the IP range provided for open TCP 502”
  - “When an open port is found it finds the SID via brute force”
  - Little more than “nmap –p 502” ☹
- http://onelittlewindow.org/blog/wp-content/uploads/2008/08/modscan_defcon_2008.pdf

- Clearly something more in-depth is needed!

Future of Modbus Pen Testing

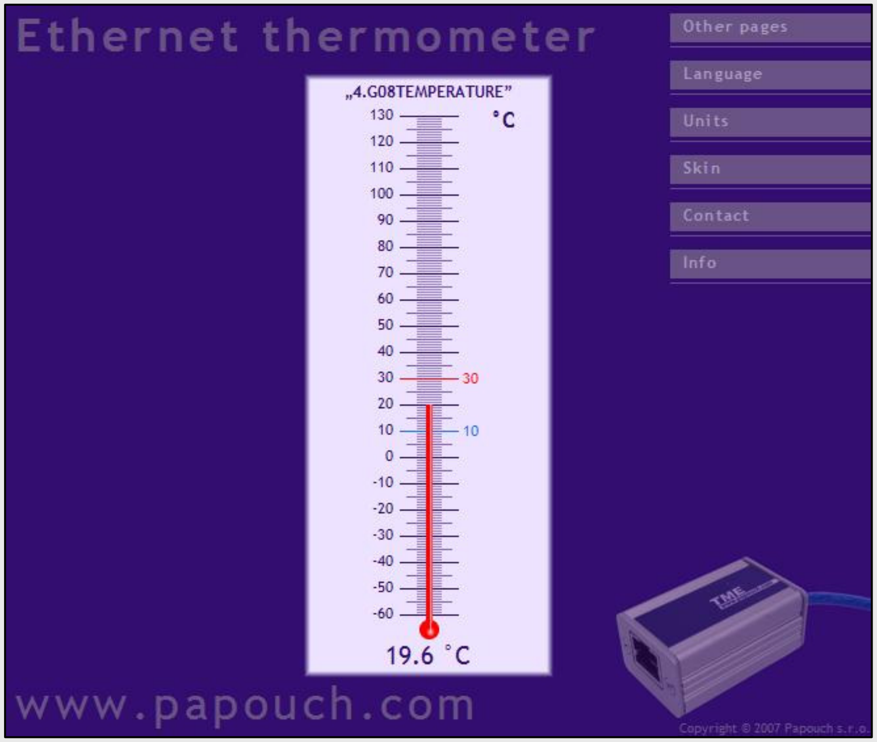
- Process
  - Identification
  - Fingerprinting
  - Vulnerability identification
  - Exploitation
  - Control
- Toolkit
  - Automation
  - Interaction
  - Analysis

But First, a Little Fun

- Show of hands please…
  - Who thinks it’s a good idea to make Modbus devices Internet accessible?
  - Who thinks it’s a good idea to attach web interfaces to Modbus devices?

What is out there?

- Verified
  - Electrical generators
  - Electrical meters
  - Cameras
  - Thermometers
  - Ovens ☺


Ethernet thermometer

„4.G08TEMPERATURE"

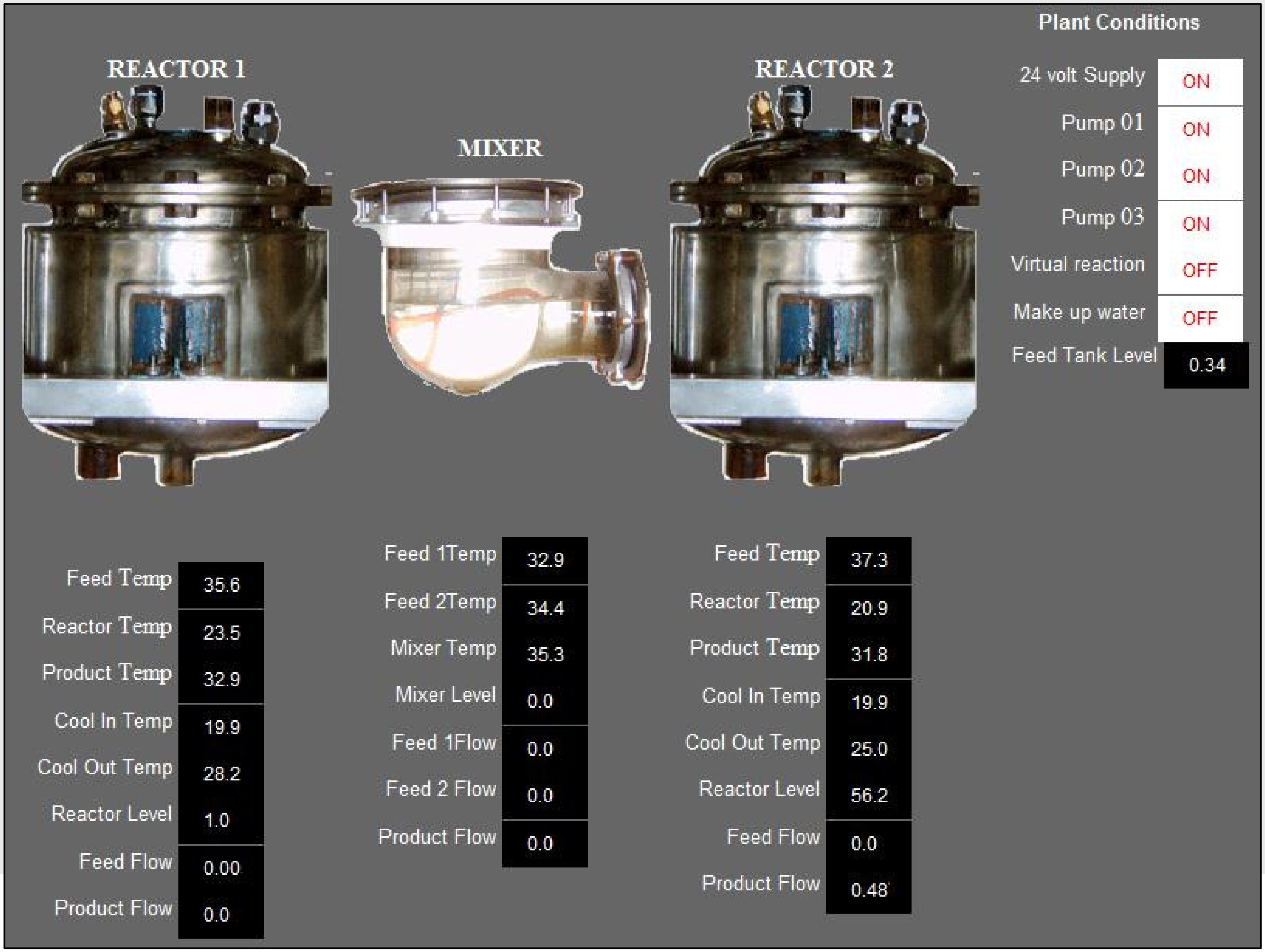
19.6 °C

www.papouch.com

Copyright © 2007 Papouch s.r.o.

- Theorised
  - Everything mechanical
    - Water, waste, power, chemical, manufacturing, traffic control…

Live on the Internet



Plant Conditions

24 volt Supply	ON
Pump 01	ON
Pump 02	ON
Pump 03	ON
Virtual reaction	OFF
Make up water	OFF
Feed Tank Level	0.34

REACTOR 1

Feed Temp	35.6
Reactor Temp	23.5
Product Temp	32.9
Cool In Temp	19.9
Cool Out Temp	28.2
Reactor Level	1.0
Feed Flow	0.00
Product Flow	0.0

MIXER

Feed 1Temp	32.9
Feed 2Temp	34.4
Mixer Temp	35.3
Mixer Level	0.0
Feed 1Flow	0.0
Feed 2 Flow	0.0
Product Flow	0.0

REACTOR 2

Feed Temp	37.3
Reactor Temp	20.9
Product Temp	31.8
Cool In Temp	19.9
Cool Out Temp	25.0
Reactor Level	56.2
Feed Flow	0.0
Product Flow	0.48

Identification

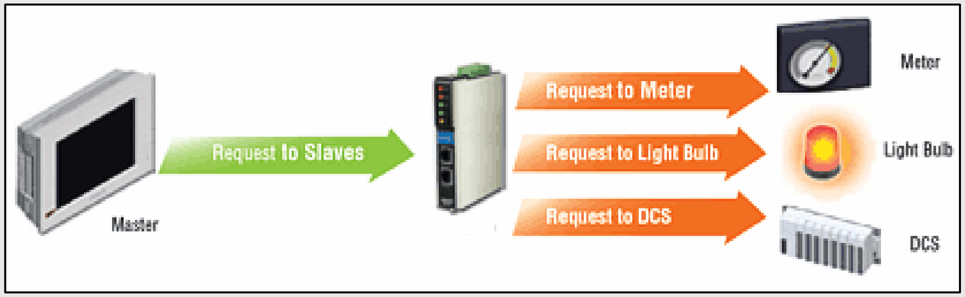
- …removed

Identifying Slaves

- An open port does not indicate a single device
  - But when it does, usually *slave id = 1*
- Read coils/registers/inputs
  - If read address is not valid
    - Do not respond; or
    - Return illegal data address (E2) ☹
  - Illegal data address response require further investigation
- Report slave id (F17)
  - Serial line only and usually reports illegal function (E1)

Identifying Gateways

- Modbus gateways
  - Connect several devices via a single interface
  - Often translate serial to TCP



- Can be identified through exceptions
  - Gateway path unavailable (E10)
    - By far the most common
  - Gateway target device failed to respond (E11)

Fingerprinting

- Fingerprinting Modbus devices can be difficult
  - Modbus is very simple
  - Modbus devices return numbers
  - There are an infinite number of devices

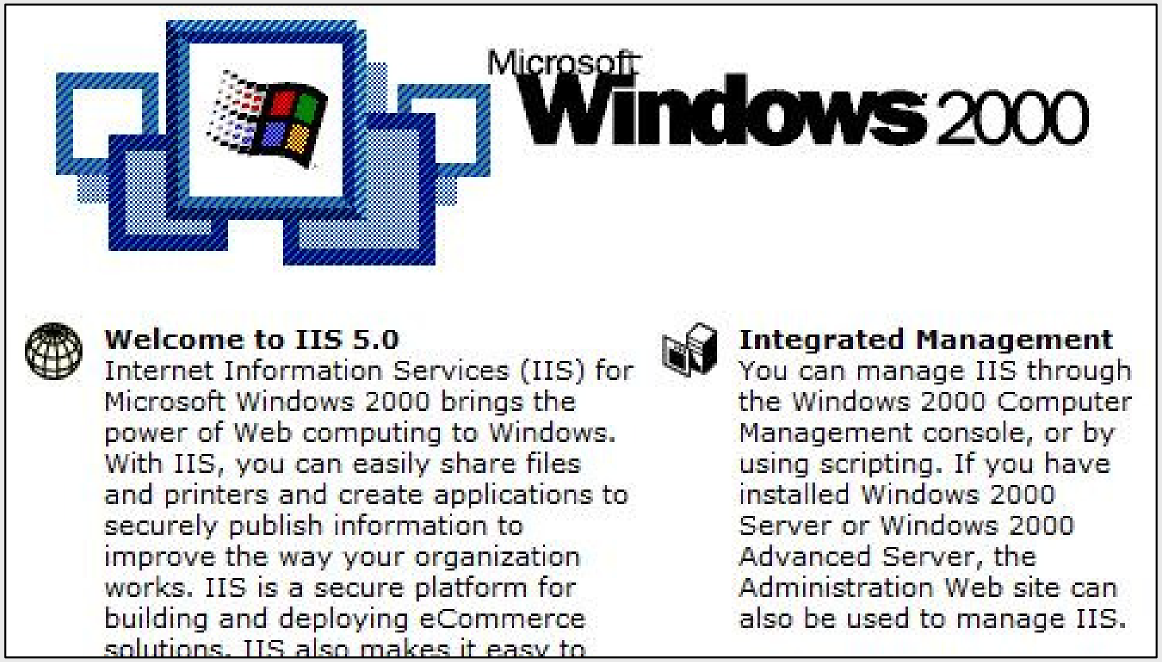
- Operating system
  - Run nmap
- Device type/model
  - Web interface? Get lucky?
- Purpose
  - Review environment

DNS

- DNS is so helpful!
  - internoc-generator-ctrl.###.edu
  - labs.###energy.###
  - electric.###.edu
  - ###.chem.eng.###.edu.###
  - ###.###.gov
  - env-plc.###.edu.###
  - factorycast1.###.fr
  - meter-master-eb1.###.edu.###
  - hvac3.###.###.edu
- Often an insight into device type and purpose

Web

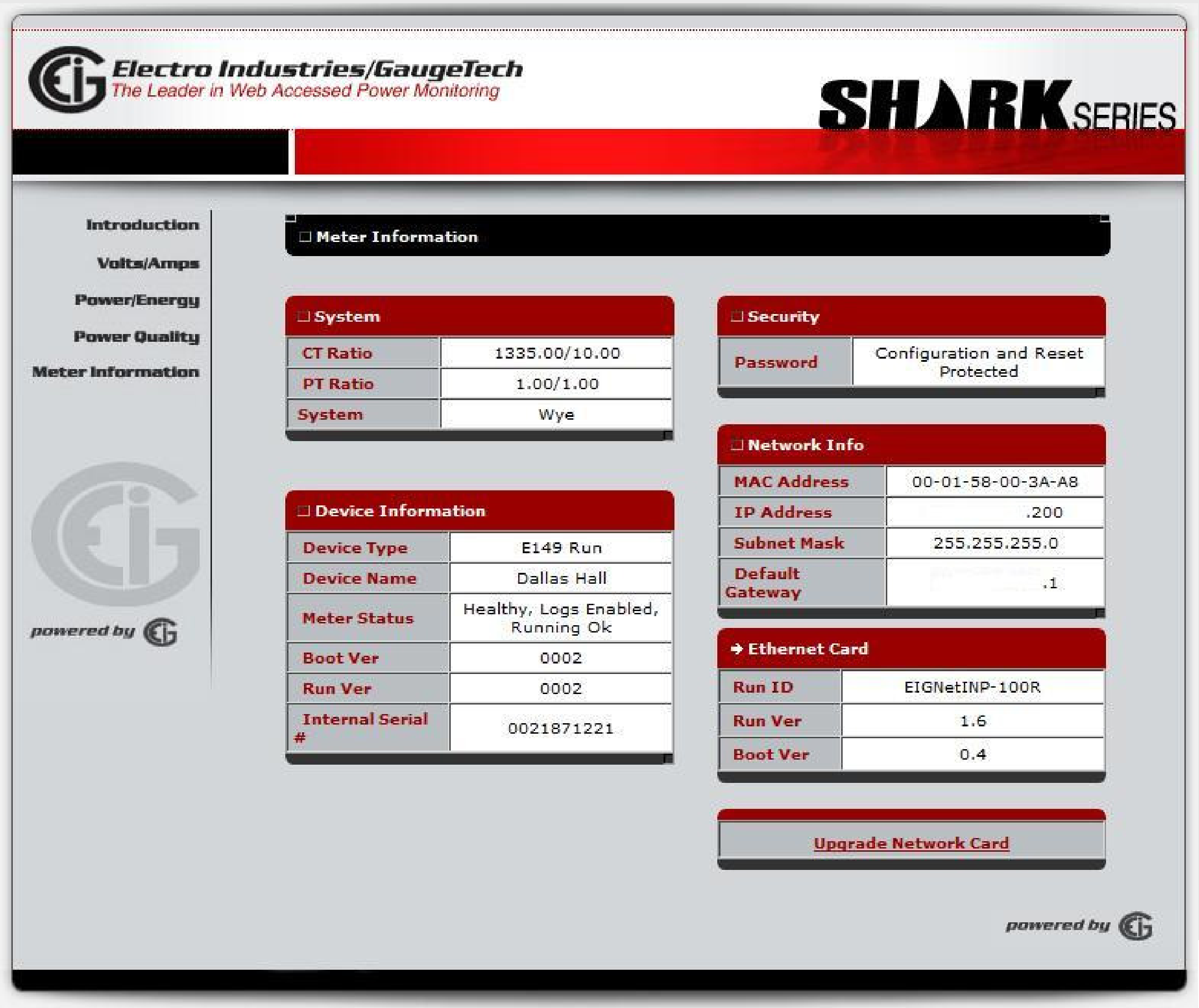
- Turns out, using the web is the often the easiest way
  - 80% of Modbus/TCP devices have web interfaces
  - Other research shows most devices run Windows 2k



Welcome to IIS 5.0
Internet Information Services (IIS) for Microsoft Windows 2000 brings the power of Web computing to Windows. With IIS, you can easily share files and printers and create applications to securely publish information to improve the way your organization works. IIS is a secure platform for building and deploying eCommerce solutions. IIS also makes it easy to

Integrated Management
You can manage IIS through the Windows 2000 Computer Management console, or by using scripting. If you have installed Windows 2000 Server or Windows 2000 Advanced Server, the Administration Web site can also be used to manage IIS.

Web



Electro Industries/GaugeTech
The Leader in Web Accessed Power Monitoring

SHARK SERIES

Introduction

Volts/Amps

Power/Energy

Power Quality

Meter Information

powered by

□ Meter Information

□ System

CT Ratio	1335.00/10.00
PT Ratio	1.00/1.00
System	Wye

□ Device Information

Device Type	E149 Run
Device Name	Dallas Hall
Meter Status	Healthy, Logs Enabled, Running Ok
Boot Ver	0002
Run Ver	0002
Internal Serial #	0021871221

□ Security

Password	Configuration and Reset Protected

□ Network Info

MAC Address	00-01-58-00-3A-A8
IP Address	.200
Subnet Mask	255.255.255.0
Default Gateway	.1

→ Ethernet Card

Run ID	EIGNetINP-100R
Run Ver	1.6
Boot Ver	0.4

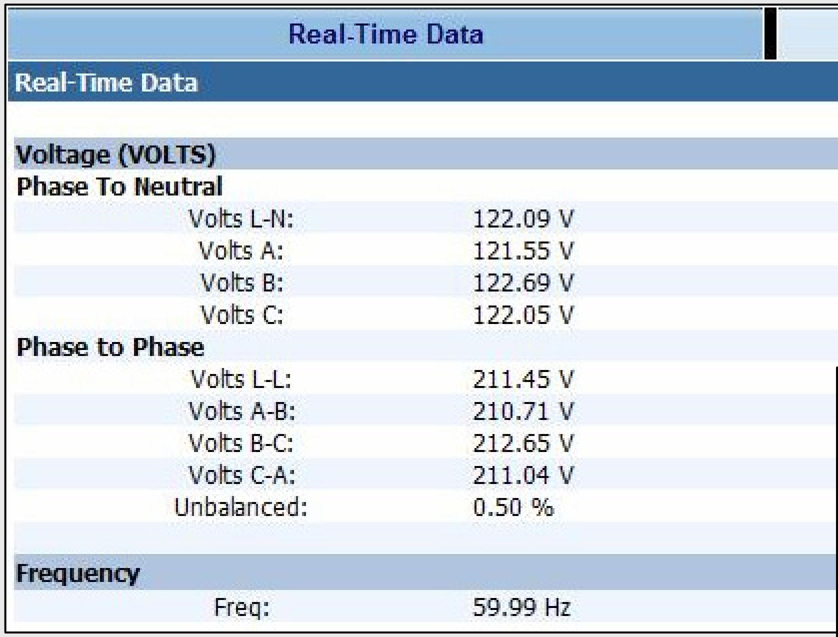
Upgrade Network Card

powered by

SIFT

Environment

- Interface found on adjacent IP address



Real-Time Data

Real-Time Data

Voltage (VOLTS)

Phase To Neutral

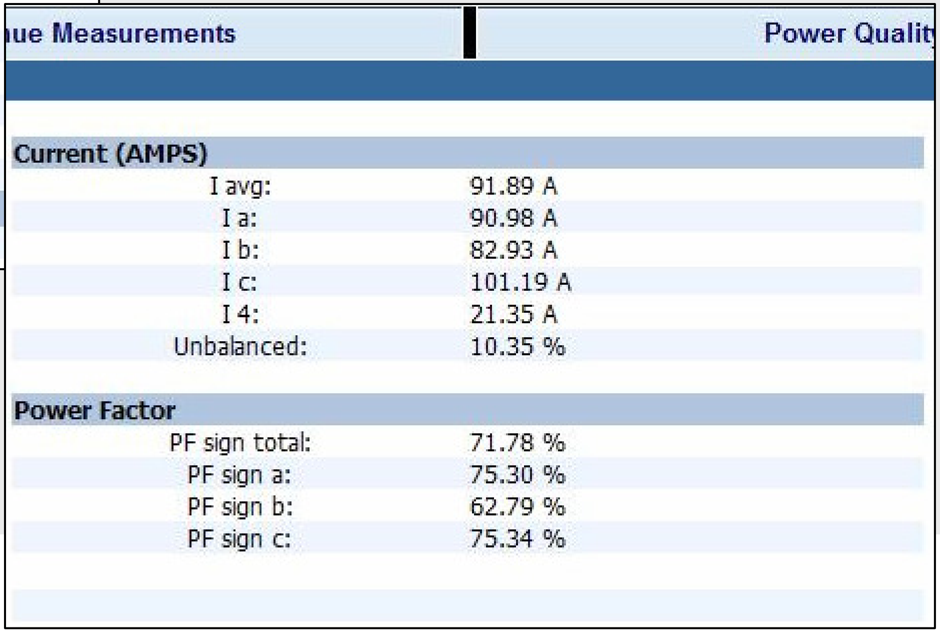
Volts L-N:	122.09 V
Volts A:	121.55 V
Volts B:	122.69 V
Volts C:	122.05 V

Phase to Phase

Volts L-L:	211.45 V
Volts A-B:	210.71 V
Volts B-C:	212.65 V
Volts C-A:	211.04 V
Unbalanced:	0.50 %

Frequency

Freq:	59.99 Hz



ue Measurements

Power Qualit

Current (AMPS)

I avg:	91.89 A
I a:	90.98 A
I b:	82.93 A
I c:	101.19 A
I 4:	21.35 A
Unbalanced:	10.35 %

Power Factor

PF sign total:	71.78 %
PF sign a:	75.30 %
PF sign b:	62.79 %
PF sign c:	75.34 %

SIFT

Vulnerability Identification

- Send the packets and they will come
  - Issue “activation” can be automated
  - Issue “capturing” can only sometimes be automated

- Device responses
  - Differ between device types/configurations
  - Some tests elicit normal response (FC=FC)
  - Some don’t respond at all and require manual investigation
  - Some give various exceptions

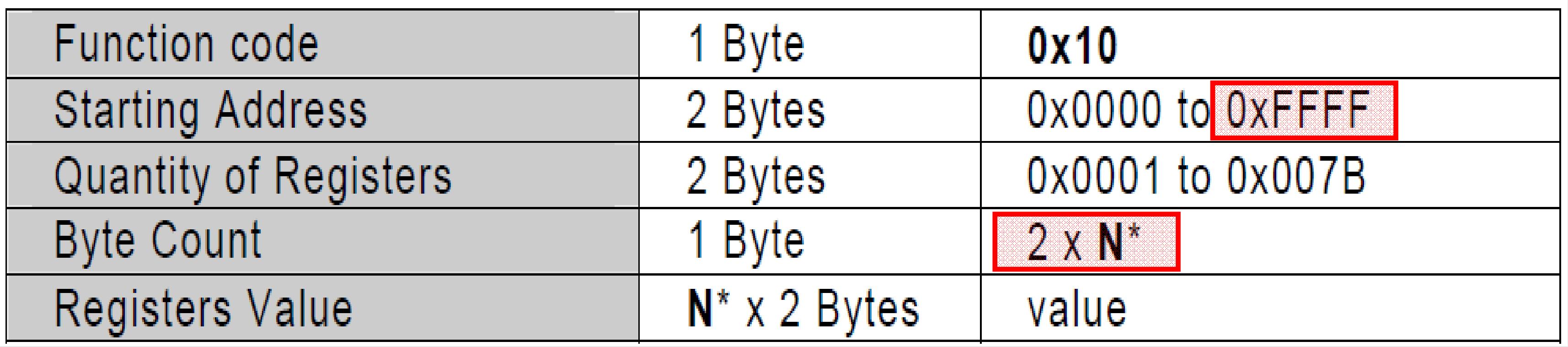
Modscan

- Remember those protocol element restrictions in slide 8 that looked really juicy…
  - Modscan attempts to test for these

- Tests configurable via XML
- Currently supports the following classes of test
  - Undefined function codes
  - Reserved functions codes
  - Invalid data lengths
  - Invalid packets
  - Serial-only functions

Sample Issues

- Write multiple registers (F15) with a high starting address
  - Devices may corrupt memory or just throw and exception

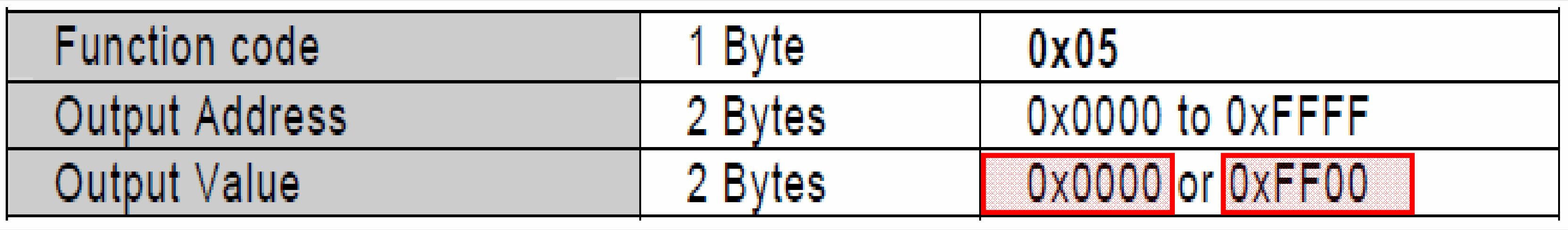


Function code	1 Byte	**0x10**
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of Registers	2 Bytes	0x0001 to 0x007B
Byte Count	1 Byte	2 x N*
Registers Value	N* x 2 Bytes	value

Sample Issues

- Send a packet with function code 0
  - Device might throw an exception (E1)
  - Some devices might go into undefined states

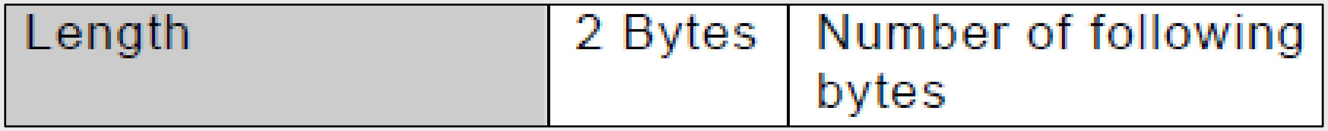
- Write undefined value to coil
  - Write 0xFAFA (for example)
  - By specification these should be ignored
  - Devices may corrupt memory or just throw and exception



Function code	1 Byte	**0x05**
Output Address	2 Bytes	0x0000 to 0xFFFF
Output Value	2 Bytes	0x0000 or 0xFF00

Sample Issues

- Send a packet with length field of 0
  - No space for unit identifier or function code!
  - Some devices might go into undefined states



Length	2 Bytes	Number of following bytes

- Send a packet with length field of 0xFFFF
  - PDU exceeds maximum allowable length
  - May cause memory corruption
  - Some devices might go into undefined states

ModScan Demo

- Demonstration scenario
  - Your SCADA engineering team has simulated a Modbus device
  - You want to test its security

Diagnostics

- SC01 - Restart communications option
  - Restart and perform confidence tests
  - Short term denial of service
- SC04 - Force listen only mode
  - Stop device from processing messages
  - Long term denial of service – till SC01 is received
- SC14 - Return slave message count
  - Number of valid messages processed since last restart
  - Useful for profiling device usage
    - Identify optimal times for testing

Moddiag

- Tool for accessing Modbus diagnostic functions
  - Supports all diagnostic function codes and sub codes
  - Non-intrusive
  - Great for profiling
  - Also useful for fingerprinting

- Moddiag found a minor bug in a SCADA product during development

Modcli and Modmut

- Modcli
  - Generates stream of valid Modbus packets
  - To be used in conjunction with a mutation fuzzer
  - Can also be used as DoS/stress tester

- Modmut (Not yet written ☹)
  - Modbus mutation fuzzer proxy
  - Sits between modcli and the target
  - Randomly changes packet field values

My Fuzzing Results

- Not many ☹
- Testing software parses the protocol safely
  - Wireshark
  - Modbus Slave
  - SimSCADA
- Real devices unlikely to be so robust
  - No evidence to support this view
  - Anyone want to donate some devices?

Modping

- Probably the most useful tool in the suite
- Generates custom Modbus packets
  - So we can poke around
  - Decomposes responses only up to function code
  - Use in conjunction with Wireshark

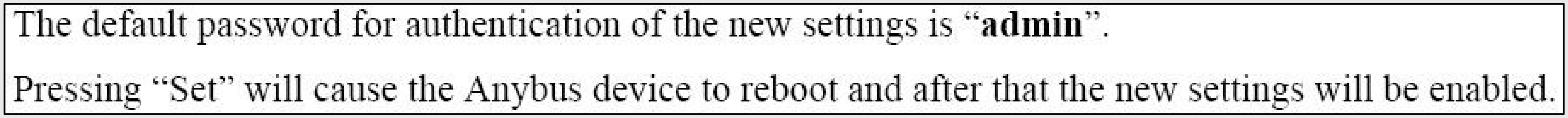
Exploitation

- Exploitation ranges in difficulty
  - Accessing functions is trivial
  - Memory issues are going range per device
  - Lots of “dark ages” issues

- Generic devices are usually programmable by the consumer
  - Usually in memory unsafe languages
  - Even if they aren’t exploitable by default, that can change

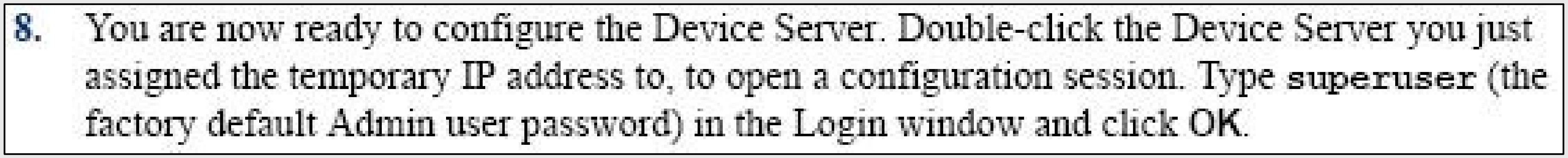
Doing a Little Research

- Manuals are a great source of information
  - Who here believes default passwords get changed?

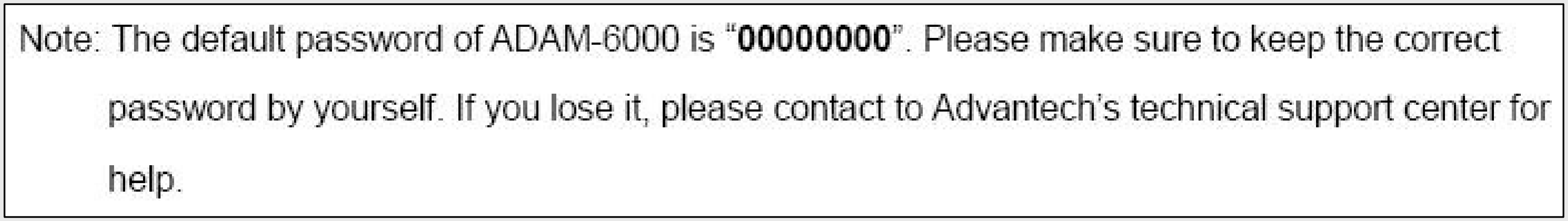


The default password for authentication of the new settings is “**admin**”.

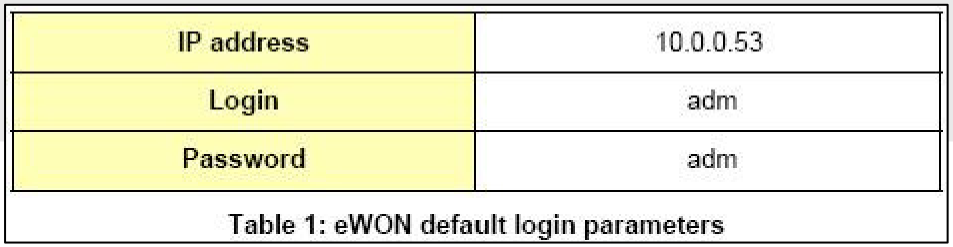
Pressing “Set” will cause the Anybus device to reboot and after that the new settings will be enabled.



8. You are now ready to configure the Device Server. Double-click the Device Server you just assigned the temporary IP address to, to open a configuration session. Type **superuser** (the factory default Admin user password) in the Login window and click OK.



Note: The default password of ADAM-6000 is “**00000000**”. Please make sure to keep the correct password by yourself. If you lose it, please contact to Advantech’s technical support center for help.

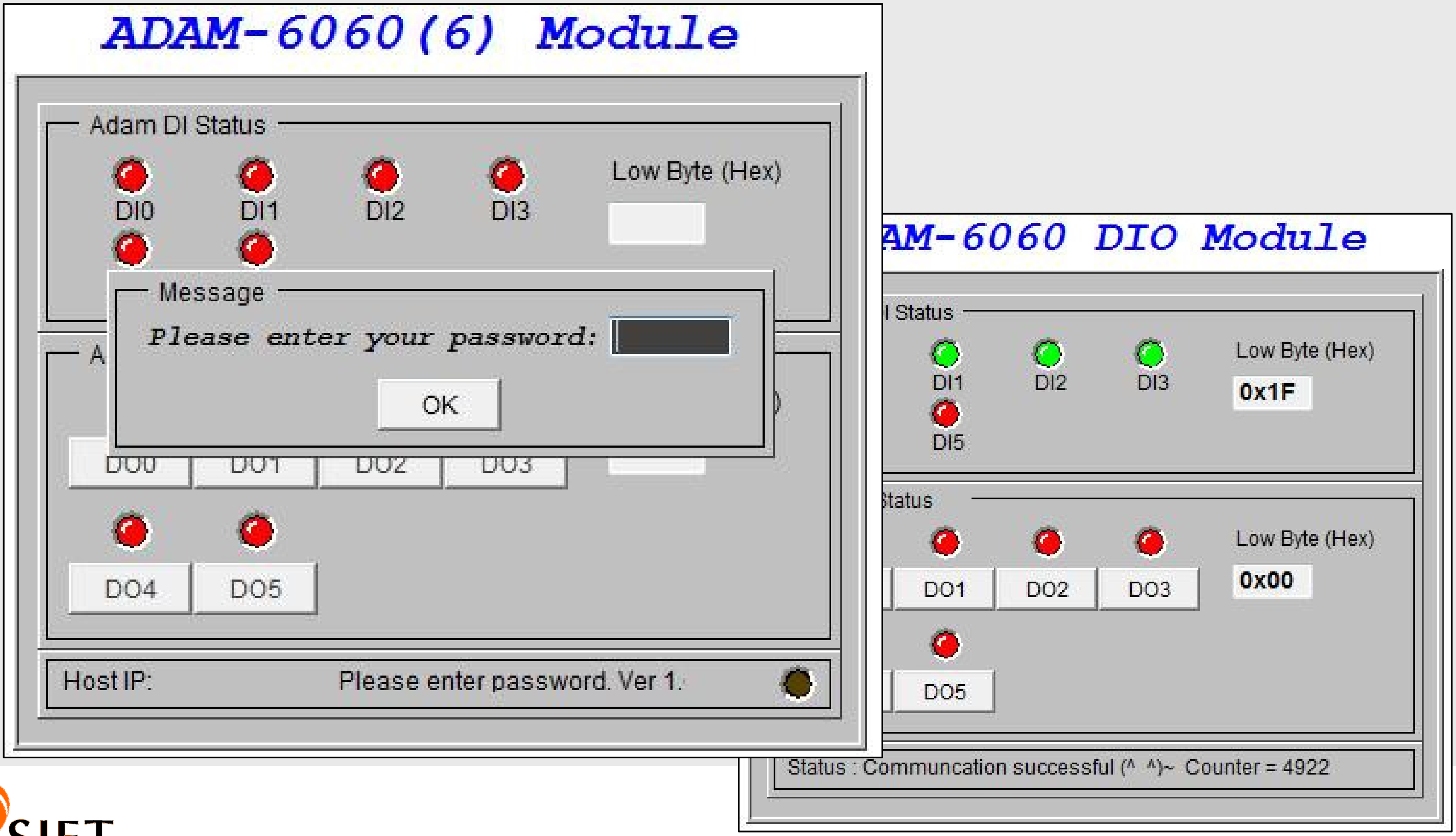


IP address	10.0.0.53
Login	adm
Password	adm

Table 1: eWON default login parameters

Web Logins

- Applets…



ADAM-6060(6) Module

Adam DI Status

Low Byte (Hex)

Message

Please enter your password:

Host IP: Please enter password. Ver 1.

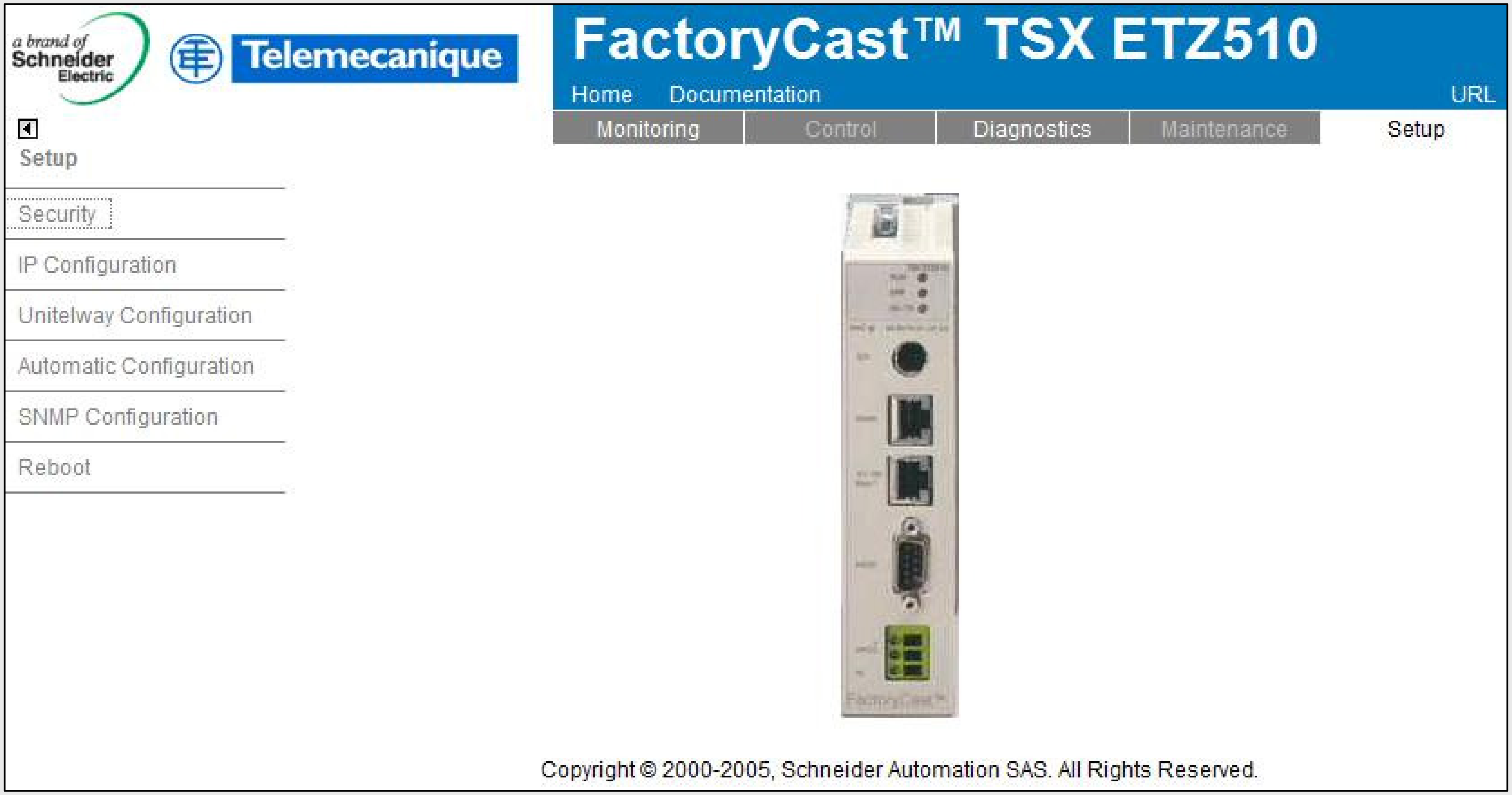
AM-6060 DIO Module

Low Byte (Hex) 0x1F

Low Byte (Hex) 0x00

Status : Communcation successful (^ ^)~ Counter = 4922

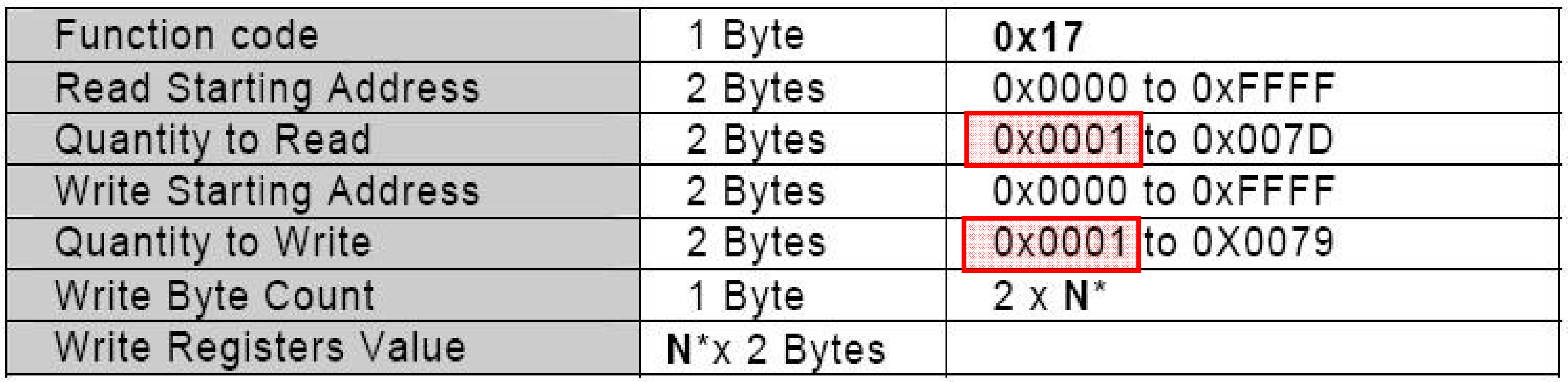
Web interfaces



Copyright © 2000-2005, Schneider Automation SAS. All Rights Reserved.

Zero Read/Write

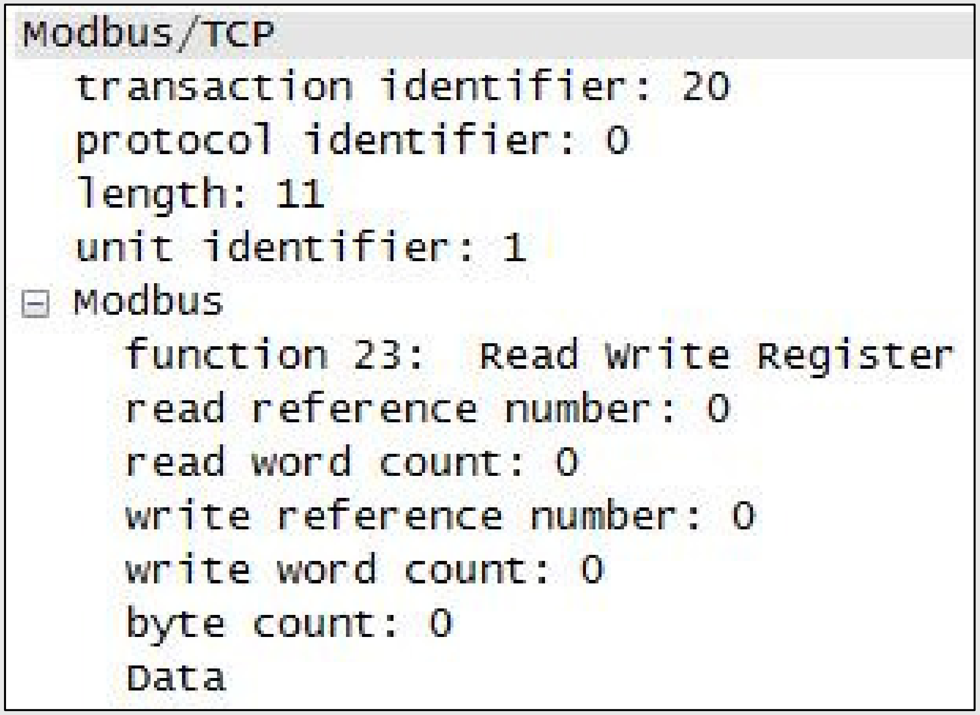
- Read/write multiple registers (F23) requires a non-zero read and non-zero write
  - Some devices may not handle zero reads/writes well
  - Can only do this with modping



Function code	1 Byte	**0x17**
Read Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity to Read	2 Bytes	0x0001 to 0x007D
Write Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity to Write	2 Bytes	0x0001 to 0X0079
Write Byte Count	1 Byte	2 x **N***
Write Registers Value	**N***x 2 Bytes	

Zero read/write

- modping -t 10.1.1.1 -p 502 -x 20 -o 0 -f 23 -l 11 -d 0x0000000000000000000



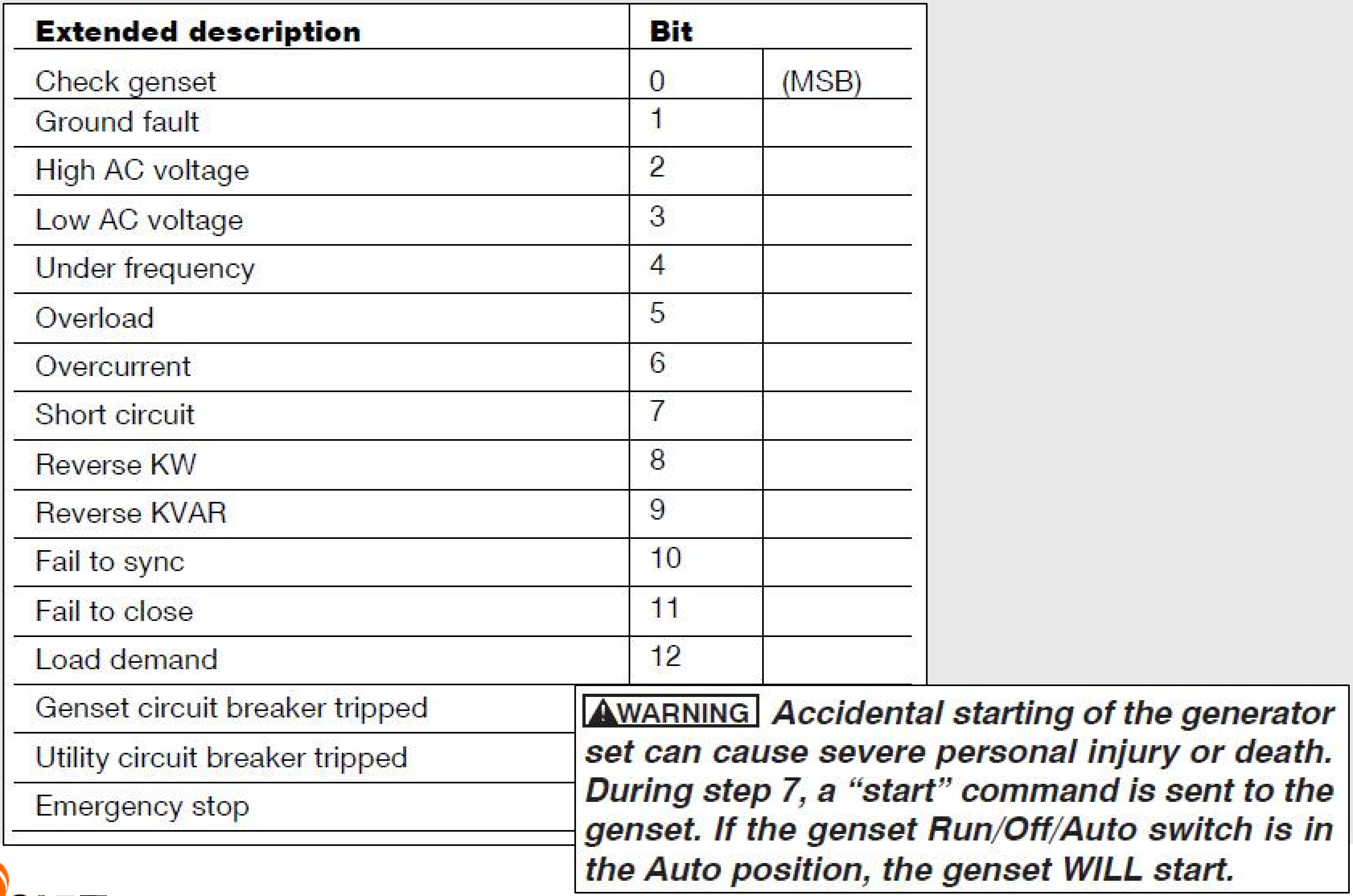
```
Modbus/TCP
  transaction identifier: 20
  protocol identifier: 0
  length: 11
  unit identifier: 1
⊟ Modbus
    function 23:  Read Write Register
    read reference number: 0
    read word count: 0
    write reference number: 0
    write word count: 0
    byte count: 0
    Data
```

Control

- End goal of the penetration test
  - Control devices by writing coils and registers
  - Sometimes through extended functions codes
  - This action should not be taken lightly
    - “Somebody is gonna get a hurt real bad…”

- Control is dependant on the device
  - 2 types of device – generic and specific
  - For specific device the best source of information is the manual
  - Generic programmable devices will require internal documentation
  - Traffic can be observed to gain “some” insights

Example Instruction Set



Extended description	Bit	
Check genset	0	(MSB)
Ground fault	1	
High AC voltage	2	
Low AC voltage	3	
Under frequency	4	
Overload	5	
Overcurrent	6	
Short circuit	7	
Reverse KW	8	
Reverse KVAR	9	
Fail to sync	10	
Fail to close	11	
Load demand	12	
Genset circuit breaker tripped		
Utility circuit breaker tripped		
Emergency stop		

⚠WARNING ***Accidental starting of the generator set can cause severe personal injury or death. During step 7, a "start" command is sent to the genset. If the genset Run/Off/Auto switch is in the Auto position, the genset WILL start.***

SIFT

Modread

- Tool for reading data from a device
  - Read coils (FC1)
  - Read discrete inputs (FC2)
  - Read holding registers (FC3)
  - Read input registers (FC4)

- Set
  - Function code
  - Field count
  - Set starting address

```
> modread -t 10.1.1.1 -f 3 -n 5 -a 0

Register | Value
0 = 0
1 = 23
2 = 34
3 = 435
4 = 1
```

Modwrite

- Tool for writing data to a device
  - Write single coil (FC05)
  - Write single register (FC06)
  - Write multiple coils (FC15)
  - Write multiple registers (FC16)

- Set
  - Function code
  - Field count
  - Set starting address
  - Data

Control Demo

- I have a great MP3 collection to choose from
- And a Modbus enabled MP3 player

- Someone please choose a song

Spoofing

- Modbus has no authentication!
  - Devices are usually black-box so cant use OS
  - MITM, evil twin etc are all possible
  - Usually configured with IP addresses not DNS names
    - DNS spoofing rare
  - ARP spoofing generally a free-for-all

Attack Detection

- Symantec Signature
  - Severity: Medium
  - This signature detects a Modbus TCP packet that exceeds the maximum length.
  - An attacker creates a specially crafted packet longer than 260 bytes and sends it to a Modbus client and server. If the client or server were programmed incorrectly, this could lead to a successful buffer overflow or denial-of-service attack.
  - Response: Drop the connection with a TCP reset.

- http://www.symantec.com/business/security_response/attacksignatures/detail.jsp?asid=20676

DigitalBond Snort Signatures

- DigitalBond has produced a baseline set of signatures
  - http://www.digitalbond.com/wiki/index.php/Modbus_TCP_IDS_Signatures

- The signatures can be broadly grouped in the following categories:
  1. Unauthorised modbus use - Authorised Modbus clients and servers are entered as variables in the IDS, and the signatures identify when unauthorised systems send requests with variable severity levels dependent on the request.
  2. Modbus Protocol Errors - these signatures will be triggered when an attacker is attempting to fuzz the protocol.
  3. Scanning - once a control system is deployed there are a number of errors and function codes that should be exceedingly rare unless someone is scanning a Modbus server.

Bypassing Signatures

- Signatures only trigged with protocol id of 0
  - Some devices don't check and don't care
- Protocol errors occur naturally
  - But can be increased artificially to create noise
- List and code scans
  - Can be slowed and randomised and slowed

Conclusions

- More importantly:
  - Modbus is inherently insecure and obscurity does not save it
  - Keep an asset inventory of Modbus devices
  - Implement infrastructure controls to protect devices
  - Ask vendors for security assessment results
  - Perform security testing of devices
  - Watch this space

The End

- Next steps
  - The toolkit will be released progressively in near future
  - All tools will be free (no source sorry ☹)
  - Accepting liquid gold in exchange for pre-release versions
- Future research?
  - Looking for research partnerships with device manufactures
  - Lots of gaps exist
- Thanks to:
  - Opal Software for donating a software license for research

Questions?

?

RUXCON '08

SCADA Penetration Testing

Hacking Modbus Enabled Devices

Daniel Grzelak [daniel.grzelak@sift.com.au]

SIFT