SCADA Security: Why is it so hard?

Amol Sarwate
asarwate@qualys.com
amol_s@yahoo.com

Version 1.0 (November 2011)

Abstract

Industrial control systems (ICS), distributed control systems (DCS), Supervisory Control and Data Acquisition systems (SCADA) all have been around for decades. But only recently these systems have received serious security considerations from the perspective of someone deliberately attacking or hacking them. The purpose of this paper is not to expose any specific exploits but to study the commonalities of such systems, determine exposure and enable organizations to take specific actions to safeguard against attacks.

Introduction

Supervisory Control and Data Acquisition (SCADA) systems are used for remote monitoring and control in the delivery of essential services products such as electricity, natural gas, water, waste treatment and transportation. This whitepaper uses the terms SCADA, ICS, DCS interchangeably.

SCADA is much more than a particular technology. SCADA solutions come in many different forms, but they're all built on the same principle - providing you with mission-critical data and control capabilities that you must have to effectively manage your operation. Usually a SCADA system is a common process automation system which is used to gather data from sensors and instruments located at remote sites and to transmit and display this data at a central site for either control or monitoring purposes. The collected data is usually viewed on one or more SCADA host computers located at the central or master site. A SCADA system can monitor and control thousands of I/O points.

Electric utilities use SCADA systems to detect current flow and line voltage, to monitor the operation of circuit breakers, and to take sections of the power grid online or offline. A typical Water SCADA application would be to monitor water levels at various water sources like reservoirs and tanks and when the water level exceeds a preset threshold, activate the system of pumps to move water to tanks with low tank levels. Transit authorities use SCADA to regulate electricity to subways, trams and trolleys and to automate traffic signals for rail systems, to track and locate trains and to control railroad crossing gates.

SCADA components, functions and relationships

Not all SCADA systems are same. But to study them from security point of view they can be broken down into components that are present in every system in one form or another. Each component has a well defined function or purposes. Furthermore each component has a specific relationship with the components that it communicated with. SCADA systems can be broken down into following major components. These components form a chain. Each component has a two way communication with the component before and after itself.

- Data Acquisition
- Data Conversion
- Data Communication
- Data Presentation and Control

Data acquisition

The first component in the chain is Data acquisition. It does not have any component before it, but has Data

Conversion component connected after it. Data acquisition consists of sensors, meters and field devices. Some examples are photo sensors, pressure sensors, temperature sensors and flow sensors. Depending on the type of SCADA system these devices could be physically located hundreds of miles away or could be inside into one plant. The primary function of these field devices is to sense physical parameters like light, temperature, pressure etc in the form of analog signals. In most cases the data which is acquired is analog. This component is also called as input output or I/O. There is a two way communication between Data Acquisition and Data Conversion which is the next component.

Data conversion

Data conversion received data generated by the acquisition component. Remote Terminal Unit (RTU), Intelligent Electronic Devices (IEDs) and in some cases Programmable Logic Controllers (PLC) are example devices that fall in this category. The functionality of these components has evolved over the years to include analog to digital conversion, sequential relay control, process control and now even networking. An RTU monitors the field digital and/or analog parameters and transmits it to the central data control via the Data Communication component. Early PLCs were designed to replace relay logic systems and were programmed in ladder logic. Modern PLCs can even be compared to desktop PCs in their power and functionality.

Data conversion has a two way communication with Data Presentation and Control via the Data Communication component.

Data Communication

Data communication consists of some communication medium that transfers data back and forth from data conversion to data control. The communication medium could be wired, wireless, radio, satellite or others. The communication takes place using one of the many SCADA protocols. Some protocols are open standard while some are propriety. Some example protocols are ModBus, DNP3, ControlNet, ProfiBus, ICCP, OCP, BBC 7200, Gedac 7020, DeviceNet , Tejas, UCA and others. It is estimated that that there are over 100 such protocols.

Data presentation and control

As the name suggests data presentation and control consists of devices used to monitor and control data received from various data communication channels. It may include Human Machine Interface (HMI) which the operator uses to monitor and react to alerts and alarms. It may consist of historian databases and other support systems.

Attack surface

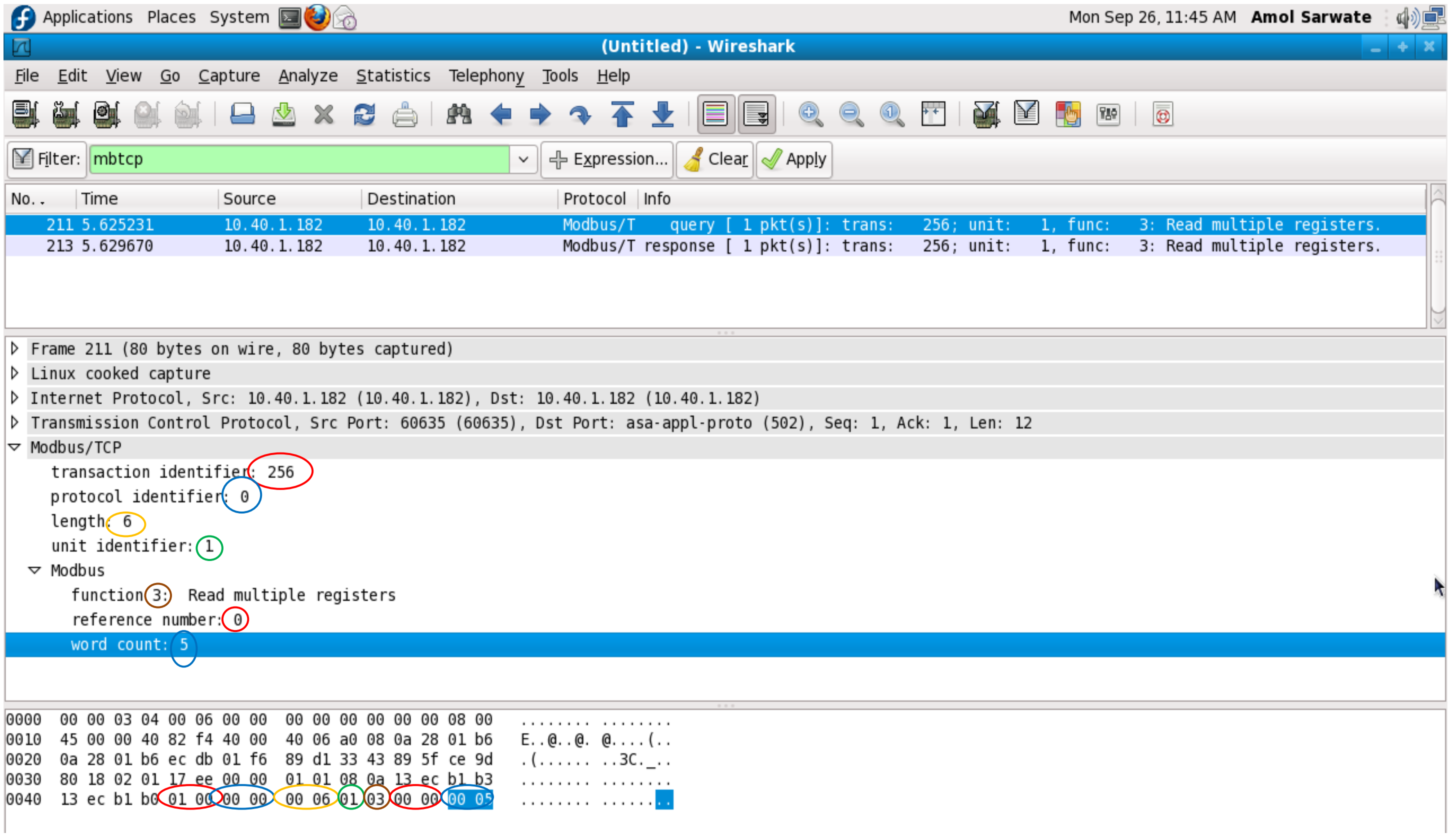
Each component in the SCADA system is a possible attack surface. We will briefly go over the various attacks that are possible on each component and when data is transmitted between them.

- Attacks on Data Acquisition

These types of attacks typically require physical access to the field equipment. Attacks on field equipment generally do not leak process knowledge of the entire system. Without process knowledge such attacks generally cause nuisance disruption. For example information on valve 16 or breaker 9B could be reviled or changed. Without the knowledge of its role in the entire system such attacks lead to vandalism or annoyance.

- Data Communication attacks

These include attacks on the underlying communication protocols, manipulating FEP directly or changing FEP output which is input for HMI. Protocol attacks are simple to execute. Protocols like MODBUS and DNP3 were designed around 1979 and 1990 respectively and were not initially designed for security against or to be run on TCP. MODBUS is a simple client server protocol and in case of SCADA the client is the


Applications Places System
Mon Sep 26, 11:45 AM Amol Sarwate
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: mbtcp
Expression... Clear Apply

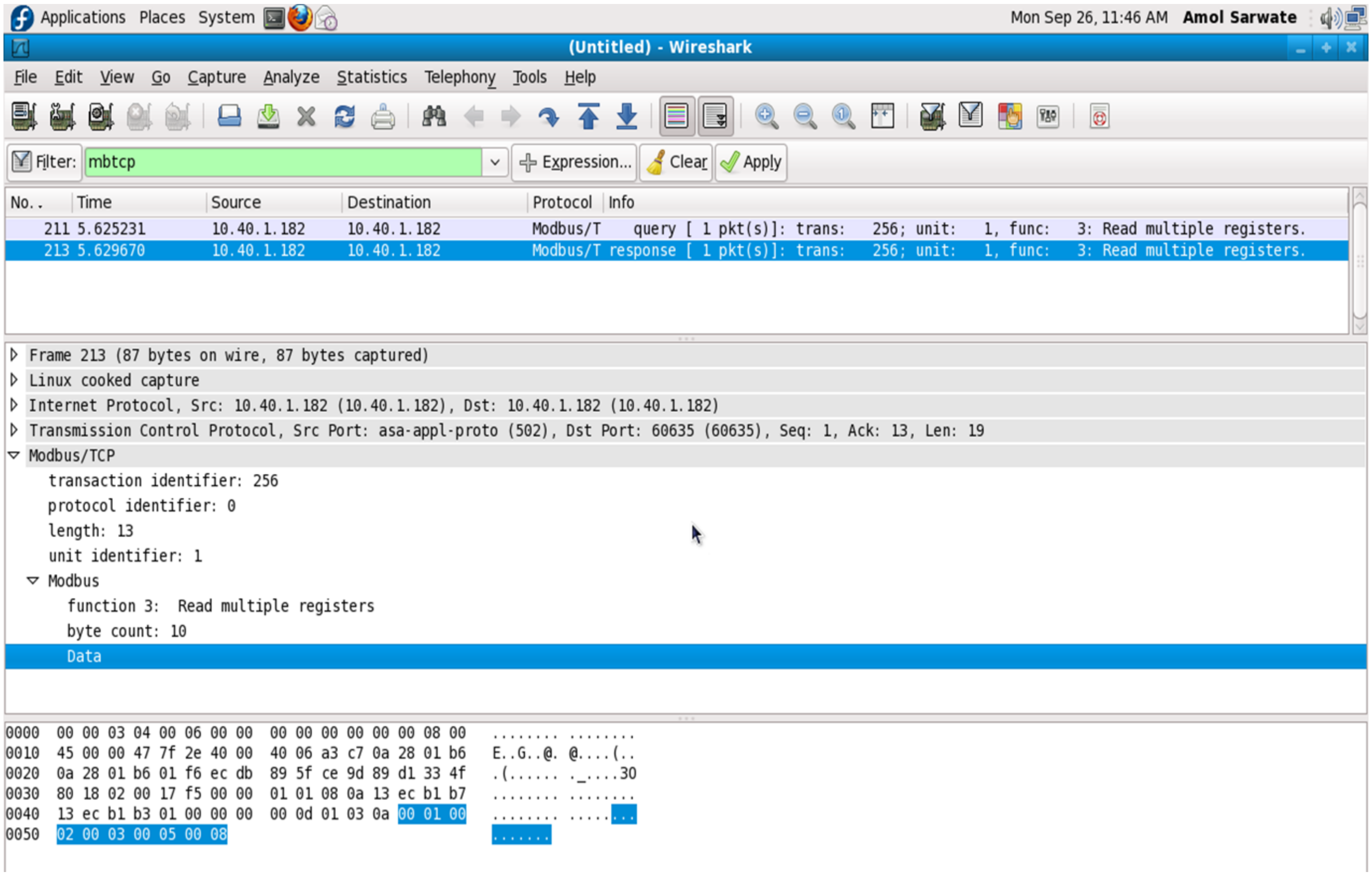
```
No. .  Time       Source        Destination   Protocol  Info
  211 5.625231    10.40.1.182   10.40.1.182   Modbus/T     query [ 1 pkt(s)]: trans:   256; unit:    1, func:    3: Read multiple registers.
  213 5.629670    10.40.1.182   10.40.1.182   Modbus/T response [ 1 pkt(s)]: trans:   256; unit:    1, func:    3: Read multiple registers.
```

```
▷ Frame 211 (80 bytes on wire, 80 bytes captured)
▷ Linux cooked capture
▷ Internet Protocol, Src: 10.40.1.182 (10.40.1.182), Dst: 10.40.1.182 (10.40.1.182)
▷ Transmission Control Protocol, Src Port: 60635 (60635), Dst Port: asa-appl-proto (502), Seq: 1, Ack: 1, Len: 12
▽ Modbus/TCP
    transaction identifier: 256
    protocol identifier: 0
    length: 6
    unit identifier: 1
  ▽ Modbus
      function 3: Read multiple registers
      reference number: 0
      word count: 5
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ........ ........
0010  45 00 00 40 82 f4 40 00  40 06 a0 08 0a 28 01 b6   E..@..@. @....(..
0020  0a 28 01 b6 ec db 01 f6  89 d1 33 43 89 5f ce 9d   .(...... ..3C._..
0030  80 18 02 01 17 ee 00 00  01 01 08 0a 13 ec b1 b3   ........ ........
0040  13 ec b1 b0 01 00 00 00  00 06 01 03 00 00 00 05   ........ ........
```

SCADA master in Data presentation and control while the server is the SCADA slave in the Data Conversion component. The packet capture on the previous page show a simple request from the client to the server to retrieve information for multiple registers. The response from the server is below. The protocol itself does not provide any confedinatlity (authntication and authorization), integrity or availiblity. When proted to TCP/IP networks that are connected intentionally or inadvertely to the internal corporate network or public facing intenet iteself, this provide a tremendous security issue.

DNP3 was specifically developed for use in Electrical Utility SCADA Applications. It is now the dominant protocol in electrical utility SCADA systems, and is gaining popularity in other industries, including Oil & Gas, Water, and Waste Water. DNP3 is a layered protocol and consist of the physical layer, data link layer, pseudo-transport layer and finally the application layer. It is a relatively newer protocol and provides major improvements over MODBUS as it has strictly defined data types. Within each type multiple variations may be supported.

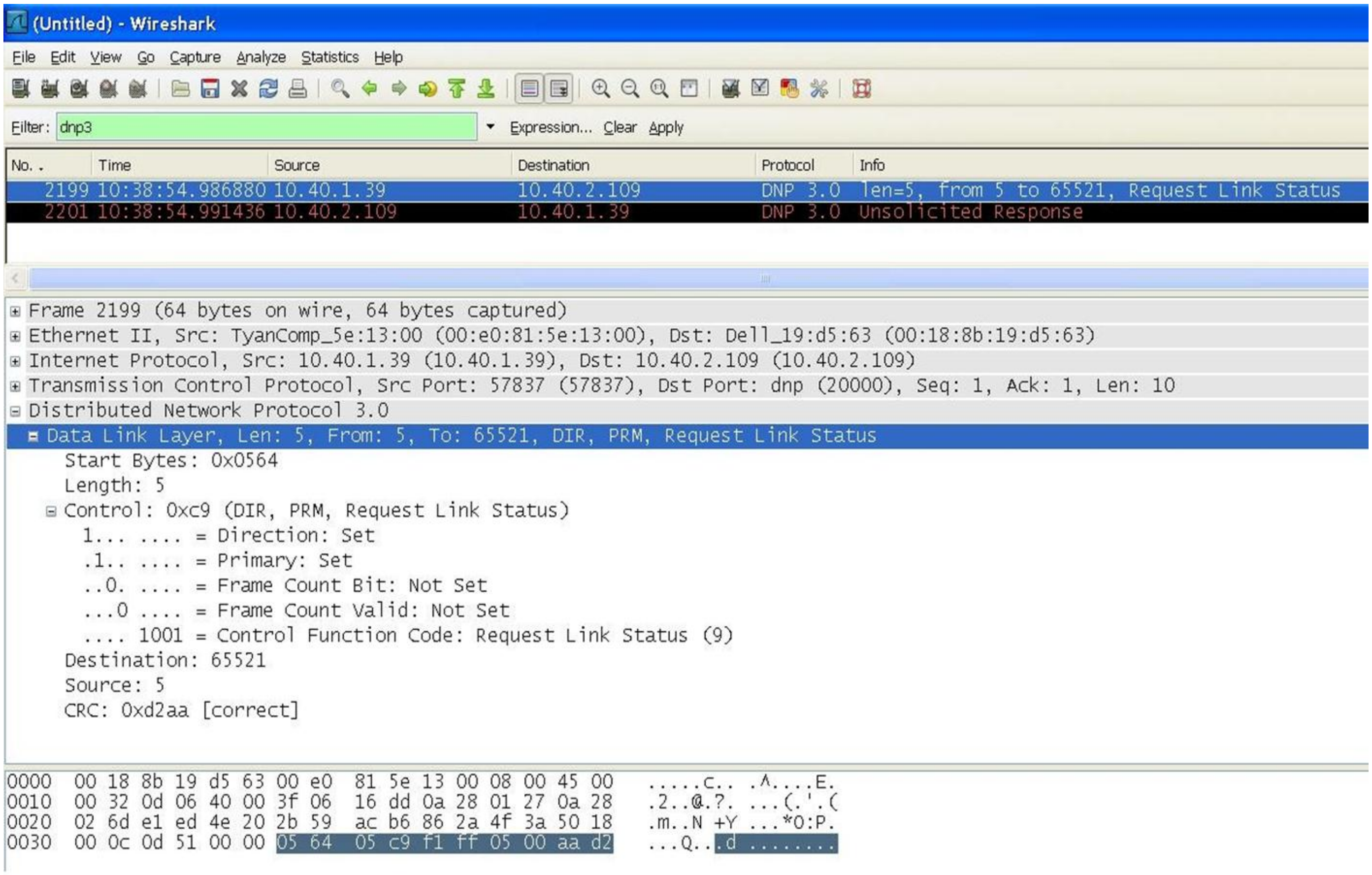

Applications Places System
Mon Sep 26, 11:46 AM Amol Sarwate
(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: mbtcp
Expression... Clear Apply

```
No. .  Time       Source       Destination   Protocol  Info
  211 5.625231   10.40.1.182  10.40.1.182   Modbus/T     query [ 1 pkt(s)]: trans:   256; unit:   1, func:   3: Read multiple registers.
  213 5.629670   10.40.1.182  10.40.1.182   Modbus/T response [ 1 pkt(s)]: trans:   256; unit:   1, func:   3: Read multiple registers.
```

```
▷ Frame 213 (87 bytes on wire, 87 bytes captured)
▷ Linux cooked capture
▷ Internet Protocol, Src: 10.40.1.182 (10.40.1.182), Dst: 10.40.1.182 (10.40.1.182)
▷ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: 60635 (60635), Seq: 1, Ack: 13, Len: 19
▽ Modbus/TCP
    transaction identifier: 256
    protocol identifier: 0
    length: 13
    unit identifier: 1
  ▽ Modbus
      function 3:  Read multiple registers
      byte count: 10
      Data
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ........ ........
0010  45 00 00 47 7f 2e 40 00  40 06 a3 c7 0a 28 01 b6   E..G..@. @....(..
0020  0a 28 01 b6 01 f6 ec db  89 5f ce 9d 89 d1 33 4f   .(...... ._....30
0030  80 18 02 00 17 f5 00 00  01 01 08 0a 13 ec b1 b7   ........ ........
0040  13 ec b1 b3 01 00 00 00  00 0d 01 03 0a 00 01 00   ........ ........
0050  02 00 03 00 05 00 08                               .......
```

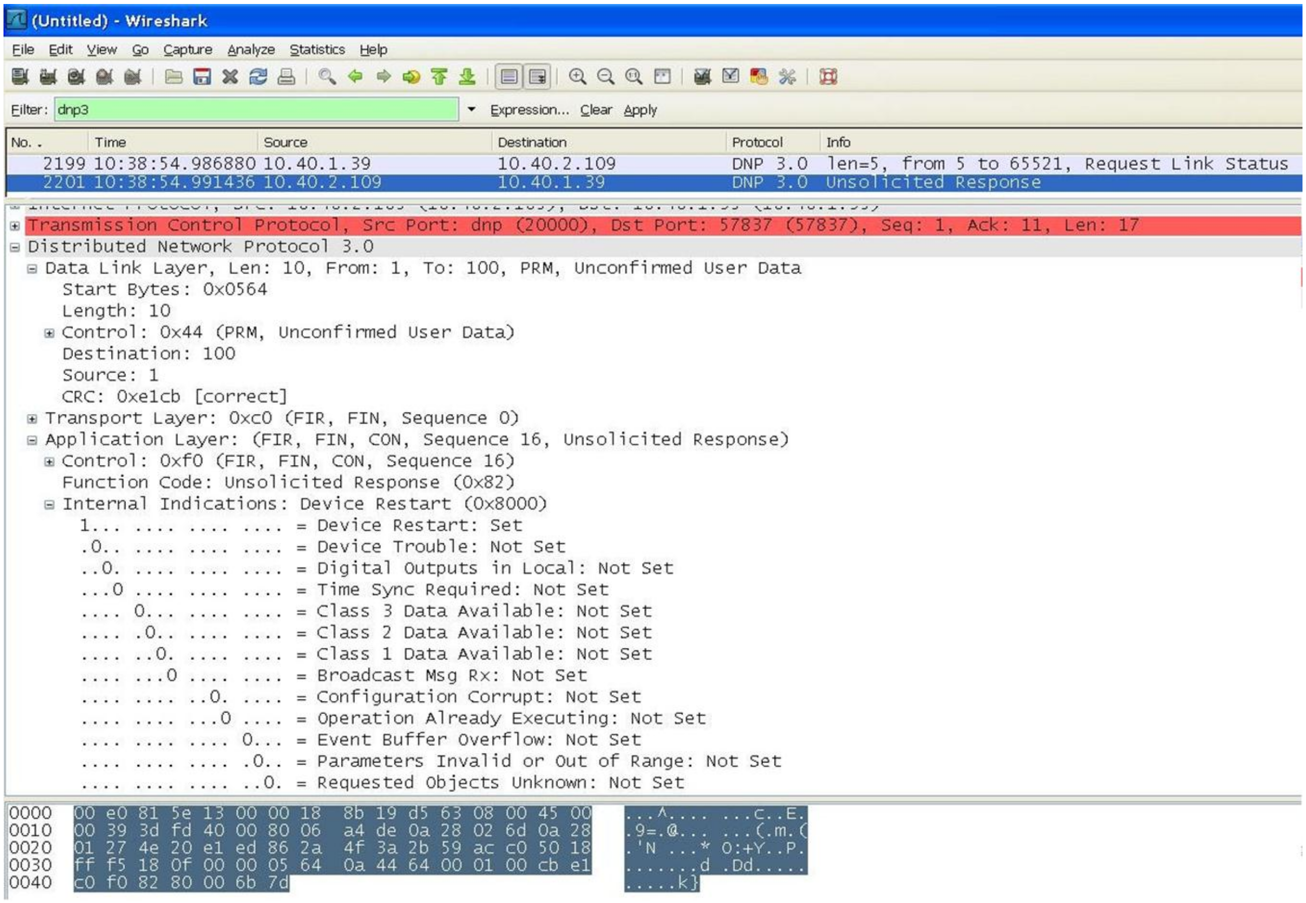
These variations may describe whether the data are sent as 16-bit or 32-bit integral values, 32-bit or 64-bit floating point values, with or without timestamps and with our without quality indicators. The DNP3 specification supports multiple methods of reading inputs individually or as a group. Multiple types of data can be encapsulated in a single message to improve efficiency. Time stamps and data quality information can also be included. DNP3 also supports change events. By polling for change events, the Master station can reduce overall traffic on the line, as only values that have changed are reported. This is commonly called Report by Exception (RBE). To further improve efficiency, DNP3 also supports unsolicited reporting. With unsolicited reporting, Slave devices can send updates as values change, without having to wait for a poll from the Master. DNP3 link layer request is shown below and its response is shown on the next page. The protocol itself does not provide any confedinatlity (authntication and authorization), integrity or availiblity. When proted to TCP/IP networks that are connected intentionally or inadvertely to the internal corporate network or public facing intenet iteself, this provide a tremendous security issue.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: dnp3
Expression... Clear Apply

```
No. .  Time               Source        Destination   Protocol  Info
  2199 10:38:54.986880 10.40.1.39    10.40.2.109   DNP 3.0   len=5, from 5 to 65521, Request Link Status
  2201 10:38:54.991436 10.40.2.109   10.40.1.39    DNP 3.0   Unsolicited Response

⊞ Frame 2199 (64 bytes on wire, 64 bytes captured)
⊞ Ethernet II, Src: TyanComp_5e:13:00 (00:e0:81:5e:13:00), Dst: Dell_19:d5:63 (00:18:8b:19:d5:63)
⊞ Internet Protocol, Src: 10.40.1.39 (10.40.1.39), Dst: 10.40.2.109 (10.40.2.109)
⊞ Transmission Control Protocol, Src Port: 57837 (57837), Dst Port: dnp (20000), Seq: 1, Ack: 1, Len: 10
⊟ Distributed Network Protocol 3.0
  ⊟ Data Link Layer, Len: 5, From: 5, To: 65521, DIR, PRM, Request Link Status
      Start Bytes: 0x0564
      Length: 5
    ⊟ Control: 0xc9 (DIR, PRM, Request Link Status)
        1... .... = Direction: Set
        .1.. .... = Primary: Set
        ..0. .... = Frame Count Bit: Not Set
        ...0 .... = Frame Count Valid: Not Set
        .... 1001 = Control Function Code: Request Link Status (9)
      Destination: 65521
      Source: 5
      CRC: 0xd2aa [correct]

0000  00 18 8b 19 d5 63 00 e0  81 5e 13 00 08 00 45 00   .....c.. .^....E.
0010  00 32 0d 06 40 00 3f 06  16 dd 0a 28 01 27 0a 28   .2..@.?. ...(.'.(
0020  02 6d e1 ed 4e 20 2b 59  ac b6 86 2a 4f 3a 50 18   .m..N +Y ...*O:P.
0030  00 0c 0d 51 00 00 05 64  05 c9 f1 ff 05 00 aa d2   ...Q...d ........
```


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

```
Filter: dnp3

No. .  Time             Source         Destination    Protocol  Info
  2199 10:38:54.986880 10.40.1.39     10.40.2.109    DNP 3.0   len=5, from 5 to 65521, Request Link Status
  2201 10:38:54.991436 10.40.2.109    10.40.1.39     DNP 3.0   Unsolicited Response

⊞ Internet Protocol, Src: 10.40.2.109 (10.40.2.109), Dst: 10.40.1.39 (10.40.1.39)
⊞ Transmission Control Protocol, Src Port: dnp (20000), Dst Port: 57837 (57837), Seq: 1, Ack: 11, Len: 17
⊟ Distributed Network Protocol 3.0
  ⊟ Data Link Layer, Len: 10, From: 1, To: 100, PRM, Unconfirmed User Data
      Start Bytes: 0x0564
      Length: 10
    ⊞ Control: 0x44 (PRM, Unconfirmed User Data)
      Destination: 100
      Source: 1
      CRC: 0xe1cb [correct]
  ⊞ Transport Layer: 0xc0 (FIR, FIN, Sequence 0)
  ⊟ Application Layer: (FIR, FIN, CON, Sequence 16, Unsolicited Response)
    ⊞ Control: 0xf0 (FIR, FIN, CON, Sequence 16)
      Function Code: Unsolicited Response (0x82)
    ⊟ Internal Indications: Device Restart (0x8000)
        1... .... .... .... = Device Restart: Set
        .0.. .... .... .... = Device Trouble: Not Set
        ..0. .... .... .... = Digital Outputs in Local: Not Set
        ...0 .... .... .... = Time Sync Required: Not Set
        .... 0... .... .... = Class 3 Data Available: Not Set
        .... .0.. .... .... = Class 2 Data Available: Not Set
        .... ..0. .... .... = Class 1 Data Available: Not Set
        .... ...0 .... .... = Broadcast Msg Rx: Not Set
        .... .... ..0. .... = Configuration Corrupt: Not Set
        .... .... ...0 .... = Operation Already Executing: Not Set
        .... .... .... 0... = Event Buffer Overflow: Not Set
        .... .... .... .0.. = Parameters Invalid or Out of Range: Not Set
        .... .... .... ..0. = Requested Objects Unknown: Not Set

0000  00 e0 81 5e 13 00 00 18  8b 19 d5 63 08 00 45 00   ...^.... ...c..E.
0010  00 39 3d fd 40 00 80 06  a4 de 0a 28 02 6d 0a 28   .9=.@... ...(.m.(
0020  01 27 4e 20 e1 ed 86 2a  4f 3a 2b 59 ac c0 50 18   .'N ...* O:+Y..P.
0030  ff f5 18 0f 00 00 05 64  0a 44 64 00 01 00 cb e1   .......d .Dd.....
0040  c0 f0 82 80 00 6b 7d                               .....k}
```

Secure DNP3, was released in 2007 which addresses much of the issues with DNP3 and provides authentication, cryptography with hashing for message authentication (HMAC), key management features as well as new function codes to support the new functionality. Users should carefully select communication protocols for modern data transfer and be aware of its security implications.

- Attacks on Presentation and Control

Presentation and Control SCADA systems and networks are increasingly being connected intentionally or inadvertely to internal company network or even internet. These systems are now ported to off the shelf hardware and operating systems like Windows and Unix. The combination of these two factors makes them vulnerable to a slew of attacks from worms, viruses and malware similar to a common desktop system. There is often a physical layer of security like a control room secured with biometric security where these systems are located. But viruses and worms do not need to enter these secured facilities physically and can hop-on from the internal network. There is often no authentication or per user-authentication to access these systems once an operator (or a worm) is on the system. If the system is password protected often the passwords are default or shared passwords without any password change policy or rights management. The systems are mostly not patched. This is due to the fact that there is no guidance from the SCADA vendor on what effect an operating system patch may have on the system. Some systems are not restarted for years and are legacy systems. In many cases since they are normal PCs they are plagued by all problems of a normal workstation like unnecessary services and others. Some modern HMI systems are based on components like Adobe Flash which are notoriously know for the lack of security features.

Challenges and recommendations

Long lifecycle of a SCADA system is one of the top challenges. Unlike desktop or sever systems that last only a few years SCADA systems last for many decades. It is difficult and costly to upgrade the system. Even if upgrades are done in phases and only parts of the systems are upgraded. SCADA vendors rarely give any guidance on operating system patches on which their systems run making it almost impossible for corporations to apply a patch with confidence that the patch will not interfere in normal operation. Data historians and other support servers also need patching as they could be the weakest link in terms of security.

It is recommended that organizations have a strategy for access control, authentication and authorization for the SCADA servers or HMI machines. Organizations should create a strategy for software updates of SCADA machines that run off the self operating systems and software. If possible organizations should try to create a test environment that is as close as possible to the production environment where they can test for patches and other software changes, giving them some degree of confidence before making changes. Organization should also demand from their SCADA vendors for testing and approval of operating system patched on which the SCADA control software runs. For PLCs, IEDs, RTUs and communication devices organizations should check the possibility of upgrades so that they can use secure protocols. Regular auditing and scanning of SCADA network for vulnerabilities is also recommended.

ScadaScan

scadascan is a command line tool that is being released with this whitepaper. This is an open source and freely available tool, currently in the alpha version. The tool can scan an IP or a network range and in a TCP/IP network. It currently identified MODBUS and DNP3 slaves. It also brute forces MODBUS to find the device IDs. In the beta version I plan to support scanning for SCADA master for known vulnerabilities. In the final version I plan to support authenticated scans and also create a framework where organization can plug in their signatures. This will make the tool robust for the community and can have signatures from a large population of SCADA devices.

Conclusion

Securing SCADA systems is tricky due to technical and organizational challenges. But the maze of SCADA security can be traversed by compartmentalizing the attack surface and applying security strategies for each component.

References

[1] ScadaScan: http://code.google.com/p/scadascan/

[2] http://laws.qualys.com

[3] http://www.nerc.com/page.php?cid=6%7C69

[4] http://www.ntsb.gov/doclib/safetystudies/SS0502.pdf

[5] http://www.nerc.com/docs/docs/blackout/Status_Report_081104.pdf

[6]http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20(2007).pdf

[7] http://www.bpa.gov/corporate/BPAnews/archive/2002/NewsRelease.cfm?ReleaseNo=297

[8]http://osgug.ucaiug.org/conformity/security/Shared%20Documents/Reference/UK%20-%20CPNI%20-%20GPG%20-%20Guide%204%20-%20Improve%20Awareness%20and%20Skills.pdf

[9] http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf