Ciberseguridad e infraestructura crítica

Juan Rodrigo Anabalón R.

MonkeysLab


SEMINARIO DE
CIBERSEGURIDAD
Expo ciber Emprendimiento
06/JUNIO SEDE APOQUINDO
Av. Apoquindo 7282, Las Condes, Región Metropolitana
10100 100010 010100
110101 001001 001010
10001 001011 110100 110101
ORGANIZA:
nacap
KANCERBERO
SEGURIDAD INFORMATICA

Juan Anabalon

- http://www.monkeyslab.cl/jar
- Especialista ciberseguridad e infraestructura crítica, informática forense, privacidad, vigilancia, censura y cuestiones políticas y sociales de Ciberseguridad.
- Certificación NIST CSF, ES-C2M2, Transportation Roadmap y CARMA para proteger la infraestructura de líneas de vida en los subsectores de Agua, Electricidad, Aviación e Internet.
- Académico en Seguridad Informática y Ethical Hacking en IP Santo Tomás.
- Académico en Diplomado en Ciberseguridad en Universidad de Santiago de Chile (USACH).
- Co-fundador y Presidente del Information Systems Security Association – ISSA Chile, capítulo chileno de ISSA International.
- Consultor en ciberseguridad en MonkeysLab.

Agenda

- Seguridad nacional y ciberseguridad
- Importancia
- Ataques, infracciones e incidentes
- Activos
- Sistema de control industrial
- Infraestructura crítica
- NIPP 2013
- Identificación de sistemas críticos
- Segmentación de red y aislamiento de sistemas
- Defensa en profundidad
- Protocolos
- DNP – DNP3
- Amenazas
- Monitoreo con Wireshark
- Recomendaciones

Seguridad nacional y ciberseguridad

- Seguridad nacional tiene por objetivo salvaguardar a una nación de la destrucción catastrófica interna

Ciberseguridad

Es un componente integral de la protección de la infraestructura crítica

¿Por qué?

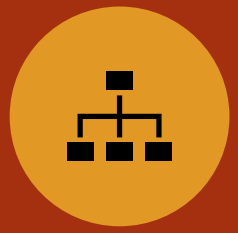
El ciberespacio proporciona una vía para atacar la infraestructura crítica de cualquier parte del mundo.

Los componentes cibernéticos hacen a las infraestructuras críticas susceptibles de subversión, interrupción o destrucción.

Y el ciberespacio es una infraestructura crítica, en la que dependen muchas otras infraestructuras críticas.

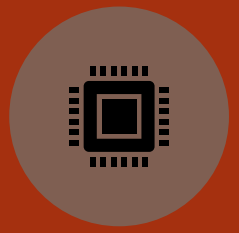
Ataques, infracciones e incidentes

NUEVAS AMENAZAS PARA LAS REDES INDUSTRIALES. MALWARES, EXPLOITS Y APTS



ESTO PODRÍA SER UNA ACCIÓN DELIBERADA DE UN INDIVIDUO U ORGANIZACIÓN.

TAMBIÉN PUEDE SER UN ACTO GUBERNAMENTAL RESPALDADO POR LA GUERRA CIBERNÉTICA



EFECTO SECUNDARIO DE UN VIRUS INFORMÁTICO QUE SE PROPAGA DESDE UNA RED DE NEGOCIOS A UN SERVIDOR ICS.

UNA TARJETA DE RED DEFECTUOSA

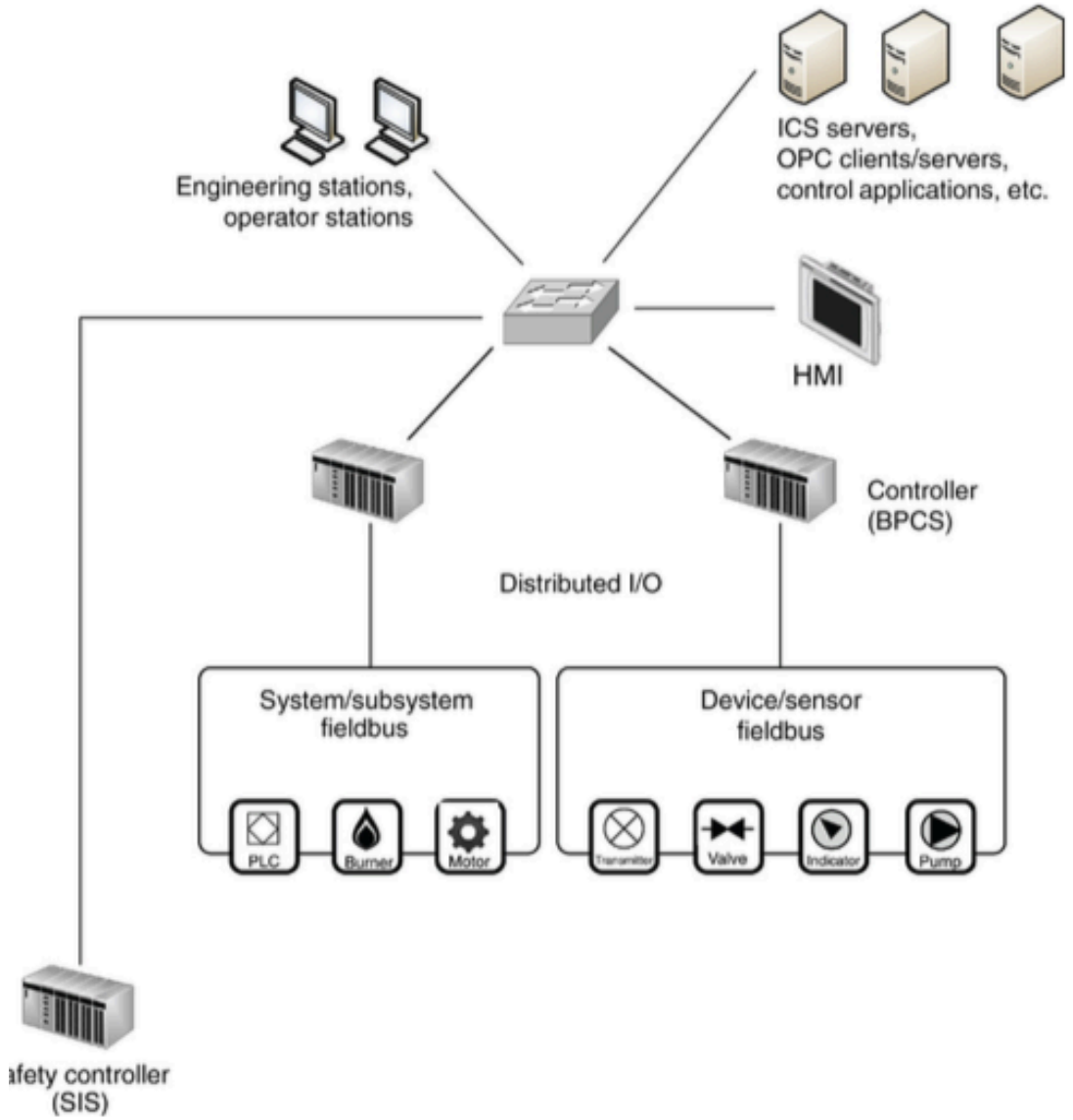
Activos

- Un activo es simplemente un término para un componente que se utiliza dentro de un sistema de control industrial.

Físicos	Lógicos (dentro del activo físico)
• Estación de trabajo • Servidor • switch • PLC • Sensores • Actuadores	• Gráfico de procesos • Base de datos • Programa lógico • Conjunto de reglas de firewall • Firmware

Sistema de control industrial

- Un sistema de control industrial (ICS) es una amplia clase de sistemas de automatización utilizados para proporcionar control y supervisión de la funcionalidad en la fabricación y facilidades industriales.
  - Sistemas de control de procesos (PCS)
  - Sistemas de control distribuido (DCS)
  - Sistemas de control de supervisión y adquisición de datos (SCADA)
  - Sistemas instrumentado de seguridad (SIS)
  - y muchos otros.



Infraestructura crítica

- EEUU

Homeland Security Presidential Directive Seven (HSPD-7):

"HSPD7 establece una política nacional para los departamentos y agencias federales para identificar y priorizar [la] infraestructura crítica de los Estados Unidos y los recursos clave y protegerlos de los ataques terroristas."

Infraestructura crítica

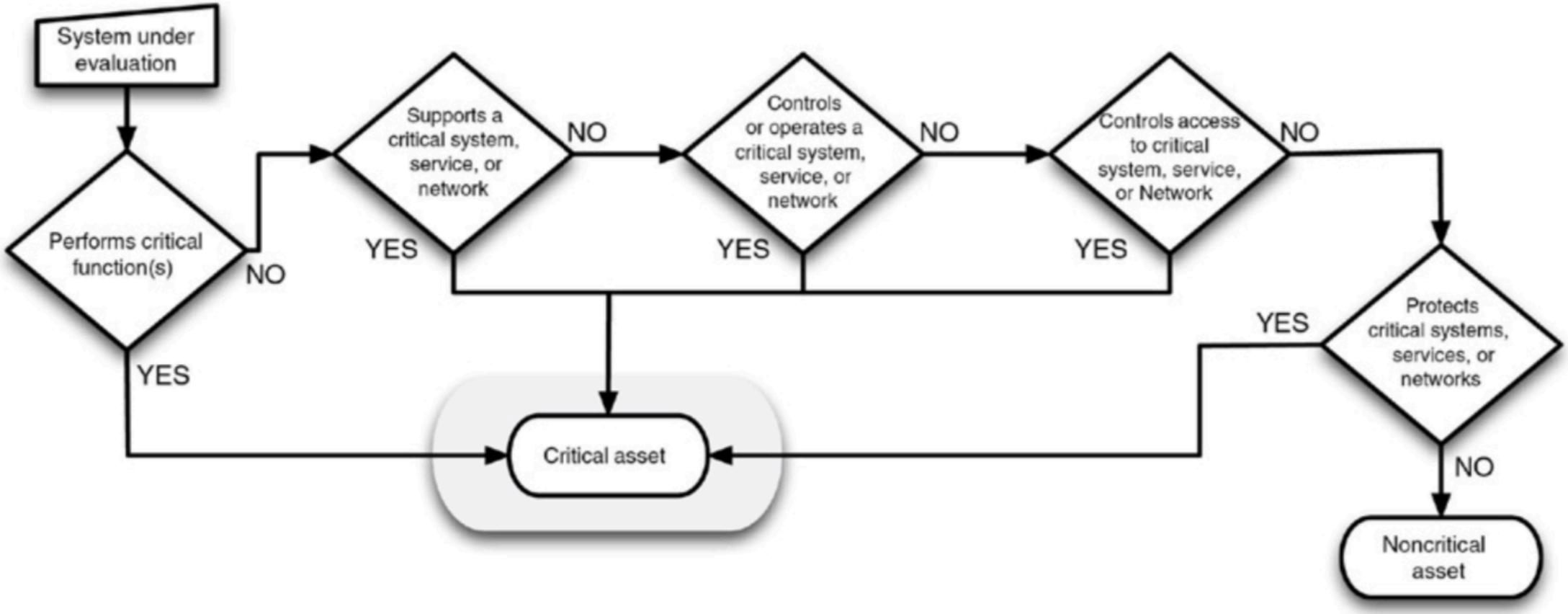
- PPD-21 de la administración Obama identifica 16 sectores de infraestructura diferentes.
- De estos sectores, el 2013 El Plan Nacional de protección de infraestructuras designa a cuatro infraestructura de Lifeline.

NIPP 2013

Estos cuatro sectores de Lifeline engloban 14 subsectores

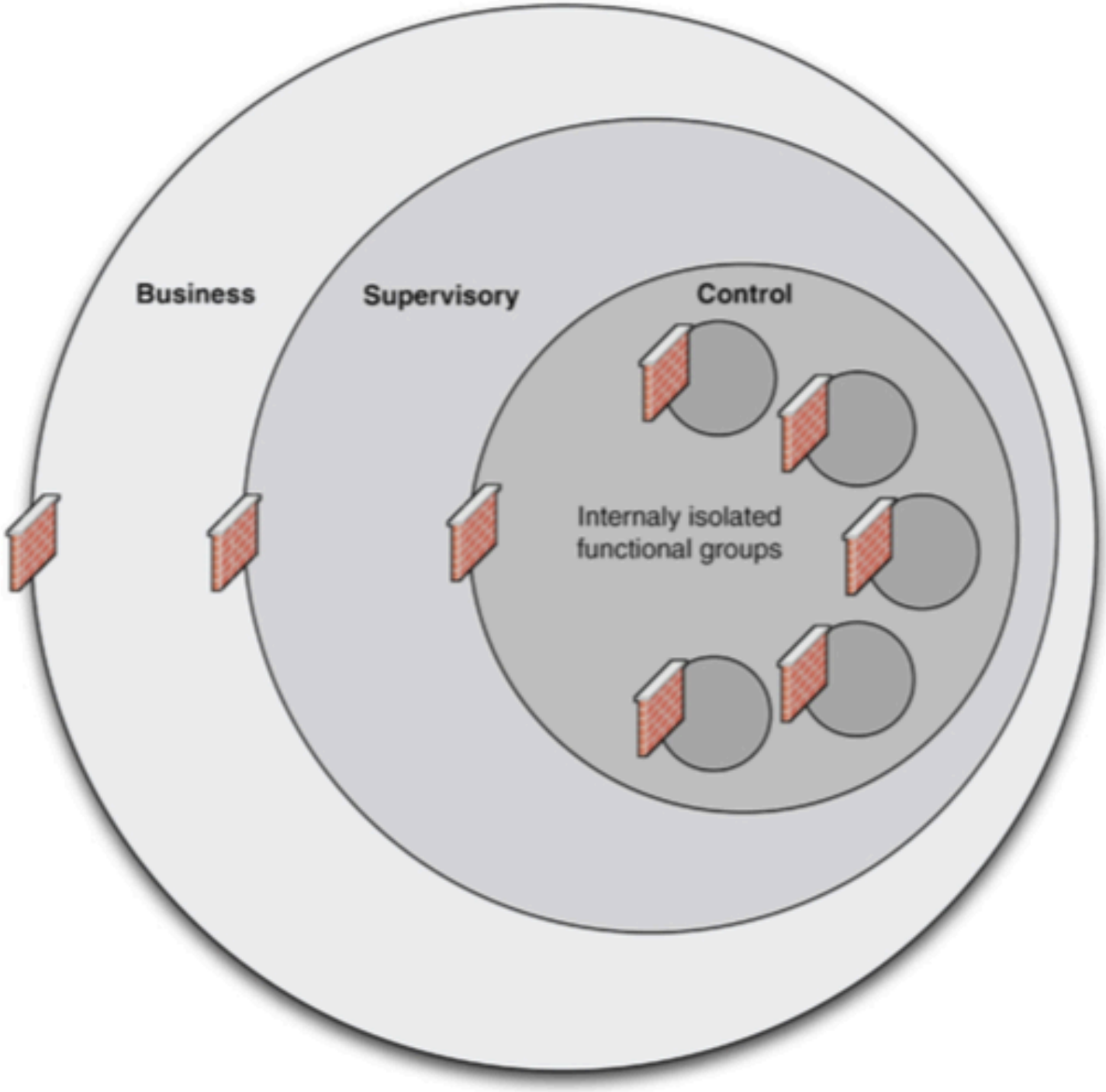
#	Sector	Subsector	System Asset	Concerning Party
1	Water/Wastewater	Water	Water Treatment & Distribution Utility	Utility Owner/Operator
2		Wastewater	Sewer Treatment & Collection Utility	Utility Owner/Operator
3	Energy	Electricity	Electrical Utility	Utility Owner/Operator
4		Natural Gas	Gas Utility	Utility Owner/Operator
5		Oil	Oil Refinery	Refinery Owner/Operator
6	Transportation	Aviation	Passenger/Cargo Jet	Air Service Owner/Operato
7		Highway	Major Transportation Bridge	State DOT
8		Rail Freight	Rail Freight Service	Rail Owner/Operator
9		Mass Transit	Major Transportation Corridor	Route Owner/Operator
10		Pipeline	Oil Pipeline	Pipeline Owner/Operator
11		Maritime	Shipping Port	Port Owner/Operator
12		Maritime	Cruise Ship	Cruise Line Owner/Operatc
13	Information	Internet	Internet Exchange Point	Internet Service Provider
14		Internet	Domain Name Servers	Root Server Administrator

Identificación de sistemas críticos



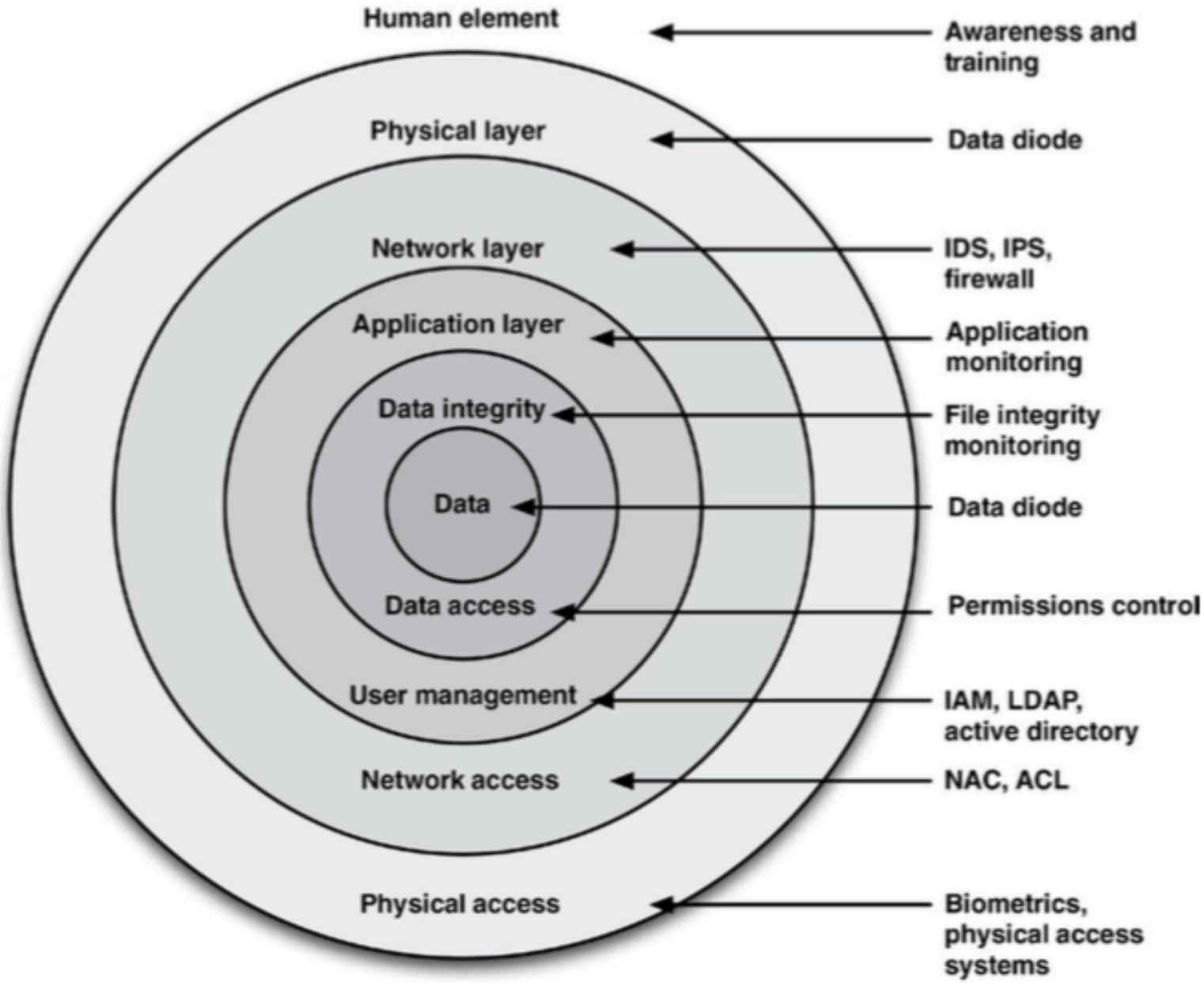
U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71 (New Regulatory Guide) Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, Washington, DC, January 2010.

Segmentación de red y aislamiento de sistemas



La vieja confiable

Defensa en profundidad

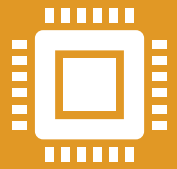


Protocolos

- ICS utilizan uno o más protocolos especializados que pueden incluir protocolos patentados específicos del proveedor:
  - Honeywell CDA
  - General Electric SRTP
  - Siemens S7
  - Etc.
- Protocolos no patentados y/o licenciados
  - OPC
  - Modbus
  - DNP3
  - ICCP
  - CIP
  - PROFIBUS

Protocolos

Diseñados originalmente para comunicaciones seriales



Adaptados para operarse sobre Ethernet utilizando UDP

Ahora también se trabajan con TCP

Distributed Network Protocol

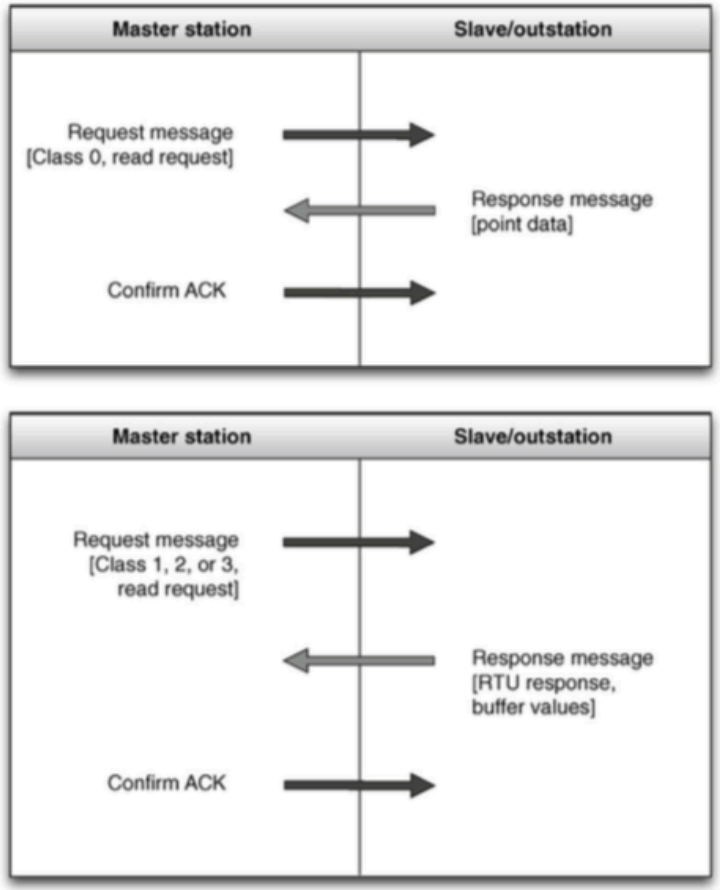
- Diseñado para su uso entre "estaciones maestras" o "estaciones de control" y dispositivos esclavos llamados "outstations".
- Utilizado en RTU y IED.
- DNP3 es una extención para trabajar sobre IP a través de encapsulación en paquetes TCP o UDP en 1998.
- Utilizado en industria eléctrica.
- DNP3 es más confiable que ModBUS, eficiente y bien adaptado para la transferencia de datos en tiempo real .
- DNP3 es más confiable debido al uso frecuente de comprobaciones cíclicas de redundancia (CRC) — una sola trama DNP3 puede incluir hasta 17 CRC (Más detalles enseguida).
- DNP3 es bidireccional

Que hace

- Envía información de control
- Datos binarios o analógicos directos para la interacción directa con dispositivos, tales como RTUs y IEDs.
- Ambos Link-Layer frame (or LPDU) header y la carga útil de datos contienen los CRC.
- La carga útil de los datos contiene realmente un par de octetos CDN por cada 16 octetos de datos.
- Esto proporciona un alto grado de garantía de que cualquier error de comunicación será detectado.
- DNP3 retransmitirá las tramas defectuosas si se detectan errores. También hay problemas de integridad de la capa física además de la integridad del marco.
- DNP3 utiliza una confirmación adicional de la capa de enlace para superar evitar que aun se pierdan paquetes.

Como funciona

- DNP3 proporciona un método para identificar los parámetros del dispositivo remoto y, a continuación, utilizar búferes de mensajes correspondientes a las clases de datos de evento 1 a 3 para identificar los mensajes entrantes y compararlos con los datos de puntos conocidos.
- Comunicaciones iniciales suelen ser una solicitud de clase 0 de la estación maestra a una estación de salida, que se utiliza para leer todos los valores de punto en la base de datos de la estación maestra
- Cada fotograma requiere una dirección de origen y una dirección de destino
- Con los protocolos puramente del Master/Slave, no hay necesidad de una dirección de origen pues el dispositivo que origina es siempre el Master

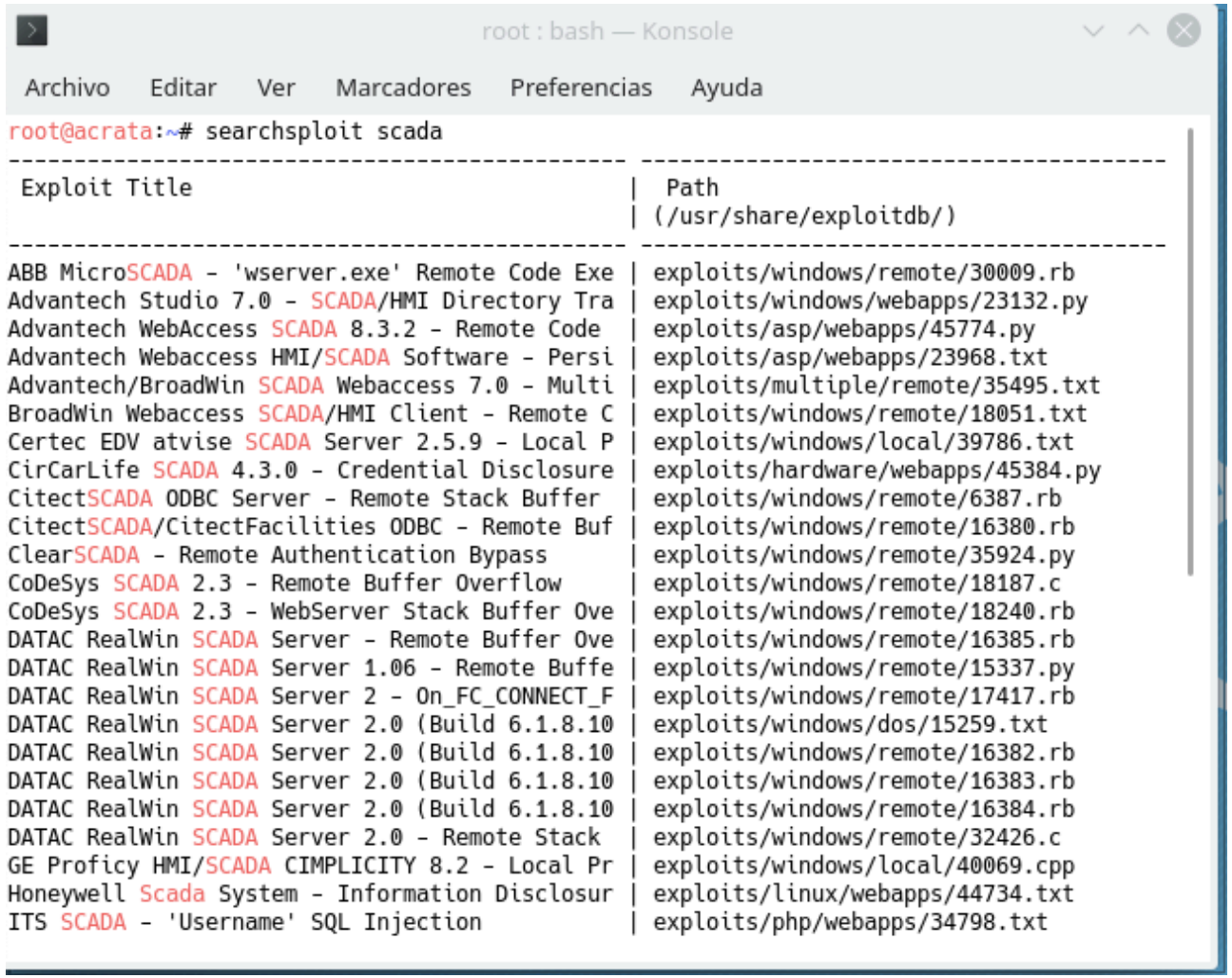


Donde se utiliza

- Entre una estación de control principal y una Remote Terminal Units (RTU) en una estación remota
- El medio de transmisión puede incluir la conexión inalámbrica, de radio y dial-up.
- DNP3 también se utiliza ampliamente para interconectar los RTUs y los IEDs.
- A diferencia de Modbus, DNP3 es muy adecuado para topologías de punto a multipunto jerárquicas y agregadas, además de las topologías lineales punto a punto y serie punto a multipunto que son soportadas por Modbus.

Seguridad

- Se presta mucha atención a la integridad del marco de datos
- Pero no hay autenticación o cifrado inherente dentro de DNP3 (aunque hay dentro de Secure DNP3)
- Resulta relativamente fácil manipular una sesión DNP3 debido a la naturaleza bien definida de los códigos de función DNP3 y los tipos de datos de la misma manera que el protocolo Modbus.
- Hay varias vulnerabilidades reportadas en ICS-CERT.
- Se recomienda hardening evaluaciones de seguridad periódicas y parchado de sistemas DNP3.
- Hay exploits conocidos.

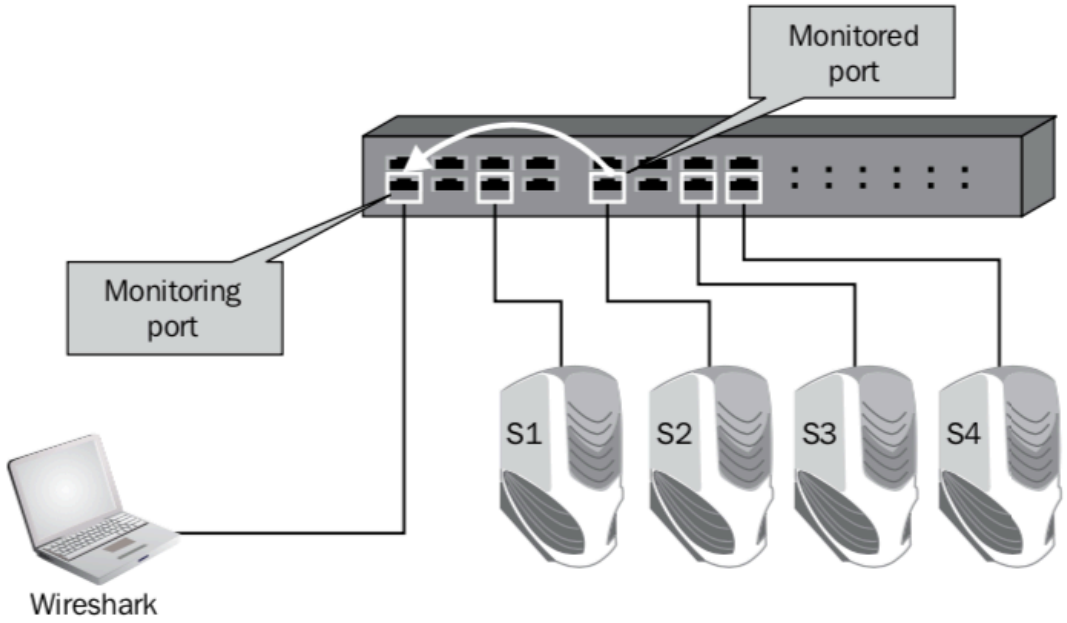


Amenazas

- Desactivación de informes no solicitados para suprimir alarmas.
- Suplantación de respuestas no solicitadas a la estación maestra para falsificar eventos y engañar a un operador a tomar acciones inadecuadas.
- Realizar un ataque DoS a través de inyección de broadcasts, creando tormentas comportamiento en toda la extensión del sistema DNP3.
- Manipulación de datos de sincronización de hora, lo que resulta en pérdida de sincronización y los errores de comunicación subsiguientes.
- Manipulación o eliminación de mensajes de confirmación que obligan a un estado de retransmisión continua.
- Emitir paradas no autorizadas, reinicios u otras funciones que podrían interrumpir las operaciones.

Donde monitorear

- Después de entender el problema y de decidirse a utilizar Wireshark, el primer paso sería decidir dónde localizarlo. Para este propósito, necesitamos tener un diagrama de red preciso (al menos la parte de la red que sea relevante para nuestra prueba).
- El principio es localizar el dispositivo que desea monitorear, conectar su computado portátil al mismo router al que está conectado y configurar un port mirror o monitor en el dispositivo supervisado. Esta operación le permite ver todo el tráfico entrando y saliendo del dispositivo supervisado.



Direct Operate Function Code

Function Code	Function Code Description
0x00	Confirm Function Code
0x01	Read Function Code
0x02	Write Function Code
0x03	Select Function Code
0x04	Operate Function Code
0x05	Direct Operate Function Code
0x0d	Cold Restart Function Code
0x0e	Warm Restart Function Code
0x12	Stop Application Function Code
0x1b	Delete File Function Code
0x81	Response Function Code
0x82	Unsolicited Response Function Code

Que buscamos

- Tipos de tráfico que son normales y qué tráfico debe seguirse.
- Antes de comenzar con las pruebas, asegúrese de que tiene una topología actualizada de la red que incluye:
- Direcciones IP de los servidores y rangos de direcciones IP de LAN
- Routers, switches, y las direcciones IP y topología de otros equipos de comunicaciones
- Dispositivos de seguridad: firewalls, sistemas de detección de intrusiones/sistemas de prevención de intrusiones (IDS/IPS), firewalls de aplicaciones web (WAF), firewalls de bases de datos y aplicaciones, sistemas antivirus y cualquier otro dispositivo que tenga una dirección IP y genere, filtre, o reenvía el tráfico de red
- ¿Cuáles son las aplicaciones que funcionan a través de la red, incluidos los números de puerto TCP/UDP y las direcciones IP de software.

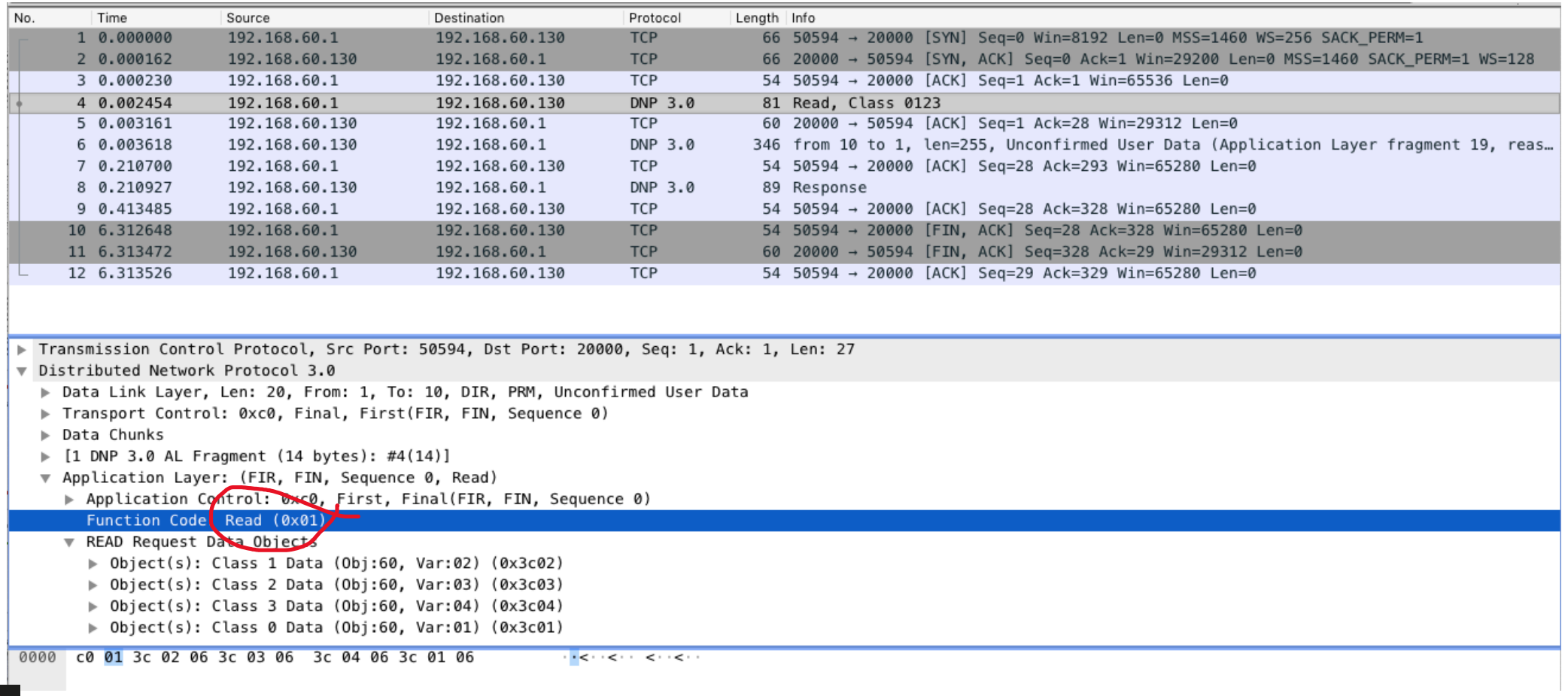
Debe revisar

- Tráfico que se genera a partir de direcciones conocidas (en la organización):
  - Normal: este es el tráfico de direcciones conocidas y rangos de direcciones
  - Sospechoso: este es el tráfico de direcciones que no conoce
- Aplicaciones y números de puerto:
  - Normal: Esto incluye los números de puerto estándar, 80 (HTTP), 137/8/9 (NetBIOS), 3389 (RDP), 20/21 (FTP), 25.110 (correo), 53 (DNS), DNP3 (19999/TCP, 20000/TCP, 20000/UDP) y así sucesivamente. Debe estar seguro de las aplicaciones que se ejecutan sobre la red, y verifique que éstos son los únicos números de puerto que usted ve.
  - Sospechoso: Esto incluye números de Puerto inusuales, es decir, números de puerto que no pertenecen a las aplicaciones que se ejecutan en el servidor (por ejemplo, los paquetes RDP al servidor Web).
- Patrones TCP:
  - Normal: TCP SYN/SYN-ACK/ACK que indica un establecimiento de conexión, reinicio único (RST) que indica una conexión rápida, paquetes FIN/FIN-ACK que indican una ruptura regular de una conexión, paquetes estándar, y Agradecimientos
  - Sospechoso: gran cantidad de paquetes SYN que van a uno o varios destinos o proceden de varias fuentes (normalmente en un patrón de escaneo que se describirán más adelante en este capítulo), combinaciones inusuales de banderas (RST/FIN, URG), y así sucesivamente
- Tráfico masivo a uno o varios sitios que usted no conoce:
  - Normal: los patrones de tráfico generalmente no son de ancho de banda fijo. Al guardar o abrir archivos, navegar por Internet, enviar o recibir correos, o acceder a un servidor con RDP, verá subidas y bajadas.
  - Sospechoso (en algunos casos): los patrones de ancho de banda fijo pueden indicar que alguien está conectado a su dispositivo, pero también puede indicar que alguien está escuchando la radio a través de Internet (100-150 Kbps), viendo el video (en algunos casos), y así sucesivamente.

Monitoreo y detección

- Se pueden detectar muchas amenazas a través del monitoreo de sesiones DNP3, y en busca de códigos de funciones y comportamientos específicos, incluyendo los siguientes:
  - Uso de cualquier comunicación no DNP3 en un puerto DNP3 (19999/TCP, 20000/TCP, 20000/UDP).
  - Uso de la función de configuración código 23 (desactivar respuestas no solicitadas).
  - Uso de los códigos de función de control 4, 5 o 6 (operar, operar directamente y operar directamente sin acuse de recibo).
  - Uso de la función de control de aplicaciones 18 (detener aplicación).
  - Múltiples respuestas no solicitadas a lo largo del tiempo (Response Storm) (82).
  - Cualquier intento no autorizado de realizar una acción que requiera autenticación.
  - Cualquier fallo de autenticación.
  - Cualquier comunicación DNP3 procedente o destinada a un dispositivo que no esté identifica explícitamente como un dispositivo de estación maestra DNP3 o de estación de salida.

Read function

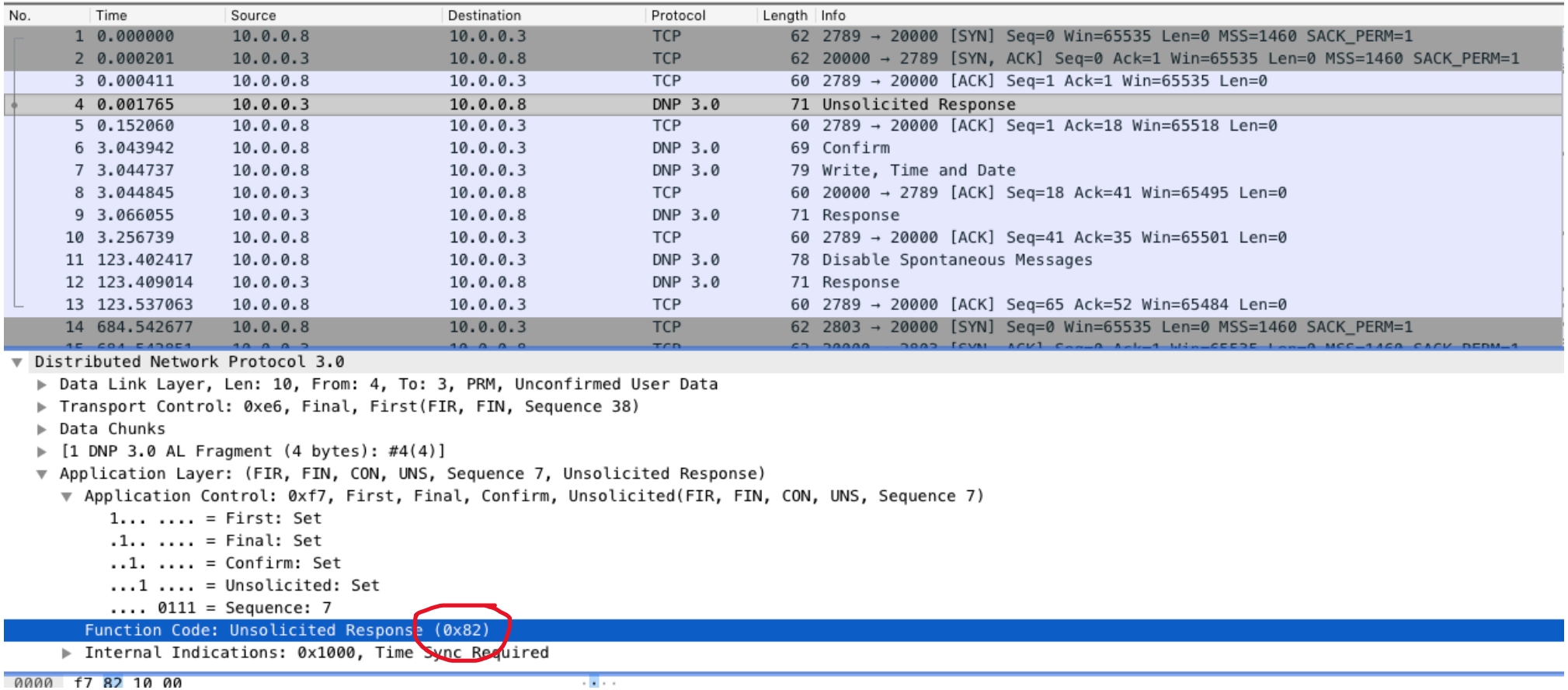


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.60.1	192.168.60.130	TCP	66	50594 → 20000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000162	192.168.60.130	192.168.60.1	TCP	66	20000 → 50594 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	0.000230	192.168.60.1	192.168.60.130	TCP	54	50594 → 20000 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.002454	192.168.60.1	192.168.60.130	DNP 3.0	81	Read, Class 0123
5	0.003161	192.168.60.130	192.168.60.1	TCP	60	20000 → 50594 [ACK] Seq=1 Ack=28 Win=29312 Len=0
6	0.003618	192.168.60.130	192.168.60.1	DNP 3.0	346	from 10 to 1, len=255, Unconfirmed User Data (Application Layer fragment 19, reas…
7	0.210700	192.168.60.1	192.168.60.130	TCP	54	50594 → 20000 [ACK] Seq=28 Ack=293 Win=65280 Len=0
8	0.210927	192.168.60.130	192.168.60.1	DNP 3.0	89	Response
9	0.413485	192.168.60.1	192.168.60.130	TCP	54	50594 → 20000 [ACK] Seq=28 Ack=328 Win=65280 Len=0
10	6.312648	192.168.60.1	192.168.60.130	TCP	54	50594 → 20000 [FIN, ACK] Seq=28 Ack=328 Win=65280 Len=0
11	6.313472	192.168.60.130	192.168.60.1	TCP	60	20000 → 50594 [FIN, ACK] Seq=328 Ack=29 Win=29312 Len=0
12	6.313526	192.168.60.1	192.168.60.130	TCP	54	50594 → 20000 [ACK] Seq=29 Ack=329 Win=65280 Len=0

```
▶ Transmission Control Protocol, Src Port: 50594, Dst Port: 20000, Seq: 1, Ack: 1, Len: 27
▼ Distributed Network Protocol 3.0
  ▶ Data Link Layer, Len: 20, From: 1, To: 10, DIR, PRM, Unconfirmed User Data
  ▶ Transport Control: 0xc0, Final, First(FIR, FIN, Sequence 0)
  ▶ Data Chunks
  ▶ [1 DNP 3.0 AL Fragment (14 bytes): #4(14)]
  ▼ Application Layer: (FIR, FIN, Sequence 0, Read)
    ▶ Application Control: 0xc0, First, Final(FIR, FIN, Sequence 0)
      Function Code: Read (0x01)
    ▼ READ Request Data Objects
      ▶ Object(s): Class 1 Data (Obj:60, Var:02) (0x3c02)
      ▶ Object(s): Class 2 Data (Obj:60, Var:03) (0x3c03)
      ▶ Object(s): Class 3 Data (Obj:60, Var:04) (0x3c04)
      ▶ Object(s): Class 0 Data (Obj:60, Var:01) (0x3c01)
```

```
0000  c0 01 3c 02 06 3c 03 06  3c 04 06 3c 01 06
```

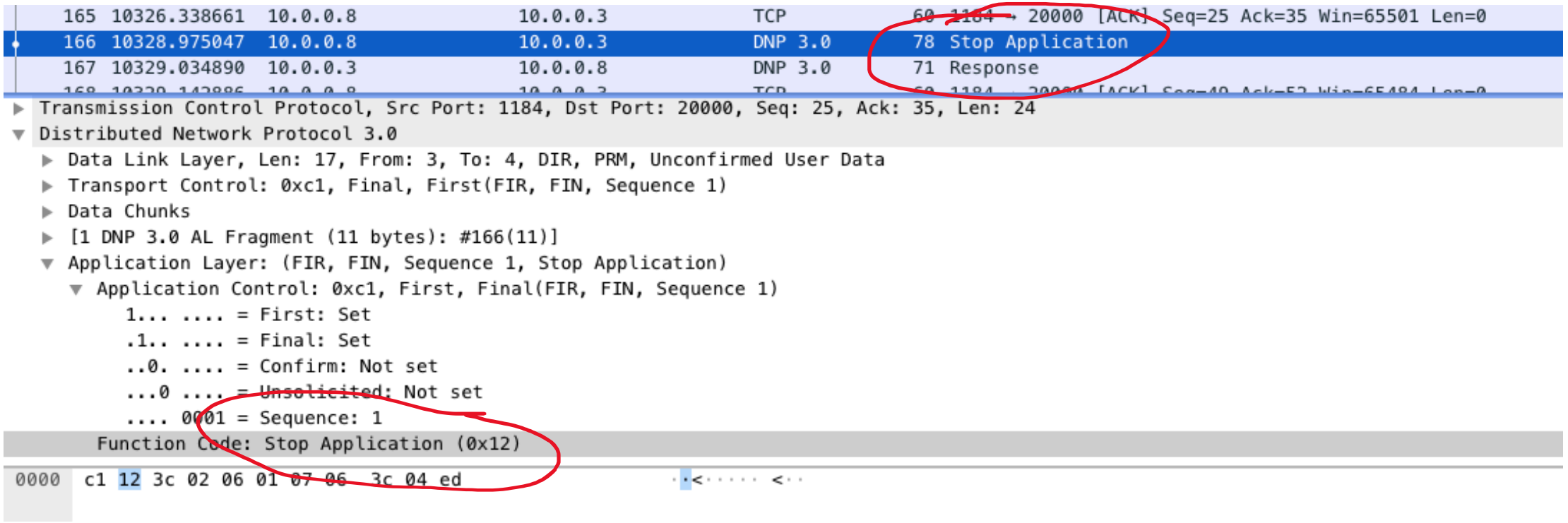
Unsolicited response function code



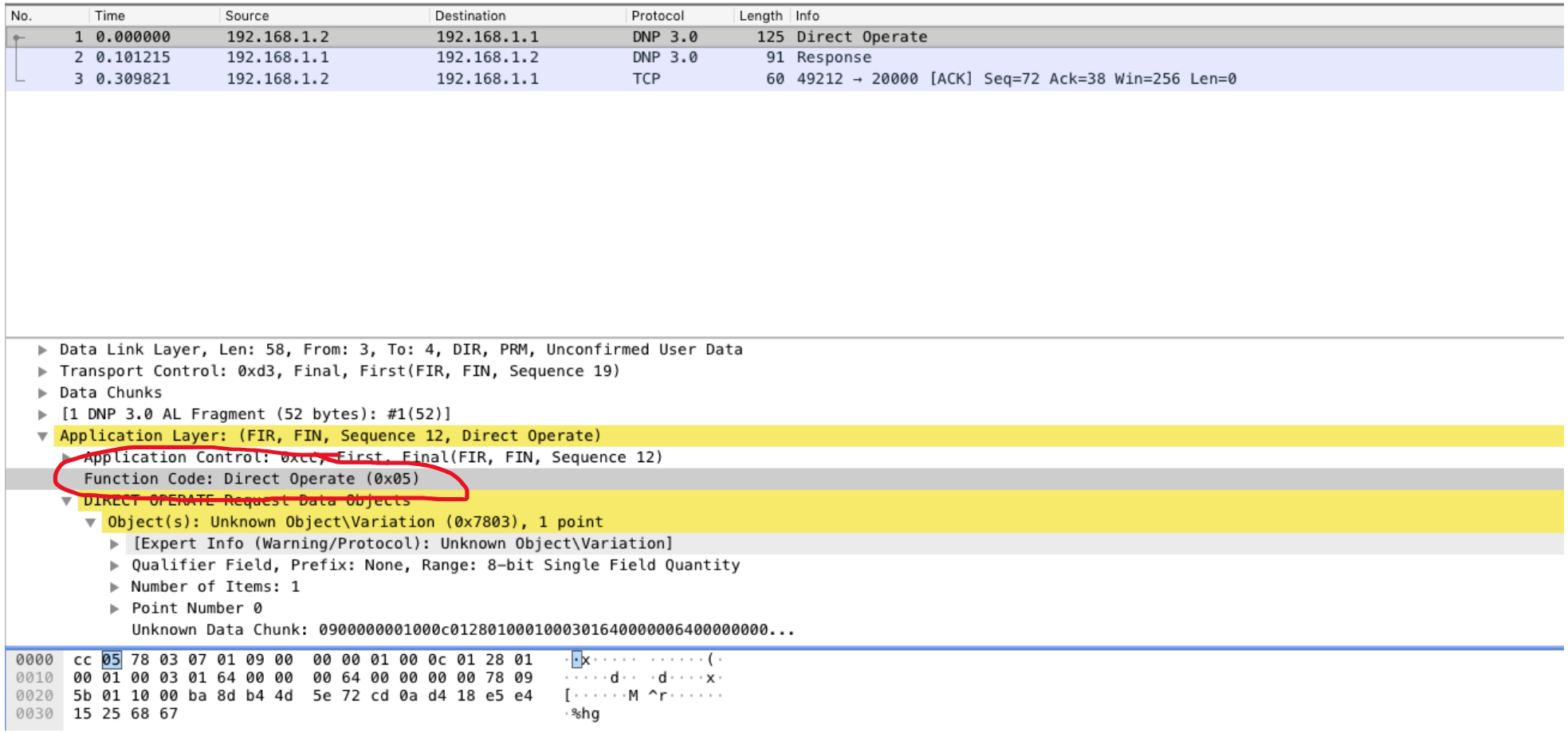
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.8	10.0.0.3	TCP	62	2789 → 20000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	0.000201	10.0.0.3	10.0.0.8	TCP	62	20000 → 2789 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
3	0.000411	10.0.0.8	10.0.0.3	TCP	60	2789 → 20000 [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.001765	10.0.0.3	10.0.0.8	DNP 3.0	71	Unsolicited Response
5	0.152060	10.0.0.8	10.0.0.3	TCP	60	2789 → 20000 [ACK] Seq=1 Ack=18 Win=65518 Len=0
6	3.043942	10.0.0.8	10.0.0.3	DNP 3.0	69	Confirm
7	3.044737	10.0.0.8	10.0.0.3	DNP 3.0	79	Write, Time and Date
8	3.044845	10.0.0.3	10.0.0.8	TCP	60	20000 → 2789 [ACK] Seq=18 Ack=41 Win=65495 Len=0
9	3.066055	10.0.0.3	10.0.0.8	DNP 3.0	71	Response
10	3.256739	10.0.0.8	10.0.0.3	TCP	60	2789 → 20000 [ACK] Seq=41 Ack=35 Win=65501 Len=0
11	123.402417	10.0.0.8	10.0.0.3	DNP 3.0	78	Disable Spontaneous Messages
12	123.409014	10.0.0.3	10.0.0.8	DNP 3.0	71	Response
13	123.537063	10.0.0.8	10.0.0.3	TCP	60	2789 → 20000 [ACK] Seq=65 Ack=52 Win=65484 Len=0
14	684.542677	10.0.0.8	10.0.0.3	TCP	62	2803 → 20000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1

Múltiples respuestas no solicitadas a lo largo del tiempo (Response Storm).

Stop Application



Direct operate function code



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.2	192.168.1.1	DNP 3.0	125	Direct Operate
2	0.101215	192.168.1.1	192.168.1.2	DNP 3.0	91	Response
3	0.309821	192.168.1.2	192.168.1.1	TCP	60	49212 → 20000 [ACK] Seq=72 Ack=38 Win=256 Len=0

```
▶ Data Link Layer, Len: 58, From: 3, To: 4, DIR, PRM, Unconfirmed User Data
▶ Transport Control: 0xd3, Final, First(FIR, FIN, Sequence 19)
▶ Data Chunks
▶ [1 DNP 3.0 AL Fragment (52 bytes): #1(52)]
▼ Application Layer: (FIR, FIN, Sequence 12, Direct Operate)
  ▶ Application Control: 0xcc, First, Final(FIR, FIN, Sequence 12)
    Function Code: Direct Operate (0x05)
  ▼ DIRECT OPERATE Request Data Objects
    ▼ Object(s): Unknown Object\Variation (0x7803), 1 point
      ▶ [Expert Info (Warning/Protocol): Unknown Object\Variation]
      ▶ Qualifier Field, Prefix: None, Range: 8-bit Single Field Quantity
      ▶ Number of Items: 1
      ▶ Point Number 0
        Unknown Data Chunk: 0900000001000c012801000100030164000000640000000000...
```

```
0000  cc 05 78 03 07 01 09 00  00 00 01 00 0c 01 28 01   ··x····· ·····(·
0010  00 01 00 03 01 64 00 00  00 64 00 00 00 00 78 09   ·····d·· ·d····x·
0020  5b 01 10 00 ba 8d b4 4d  5e 72 cd 0a d4 18 e5 e4   [·····M ^r·····
0030  15 25 68 67                                       ·%hg
```

Recomendaciones

- Preferir Secure DNP3
- Donde no hay Secure DNP3 use TLS
- Cuidado con los problemas de compatibiidad de dispositivos legados,
  - Versión 5 de la norma (adoptada como IEEE-1815-2012) no es compatible con versiones anteriores,
  - Versión 2 (adoptada como IEEE-1815-2010) ahora está reorientada y debe actualizarse.
- Las master stations y outstations DNP deben aislarse en zonas únicas.
- Defensa en profundidad
  - incluyendo firewall industrial y/o un IDS/IPS con estricto control sobre el tipo, fuente y destino del tráfico a través del enlace DNP3 entre conductos entre Zonas.
- Firmware actualizado
- Network Access Control (NAC)

Gracias

Juan Rodrigo Anabalón R.

jar@monkeyslab.cl