Seguridad protocolo DNP3

María Campos Pichel

***Abstract*-DNP3 es un protocolo de comunicación industrial utilizado entre componentes en los sistemas de automatización de procesos. Fue desarrollado para comunicación entre varios tipos de dispositivos de control y adquisición de datos. Se trata de un protocolo con funciones críticas y vulnerabilidades de seguridad.**

Con el fin de evitar fallos de seguridad en la comunicación de las infraestructuras SCI (Sistemas de Control Industrial), en este documento se enumeran los diferentes problemas de seguridad del protocolo, se presenta un estándar de autenticación seguro de DNP3 y se aporta recomendaciones para evitar los fallos de seguridad.

Palabras clave-SCI, DNP3, seguridad, protocolo.

I. INTRODUCCIÓN

Hasta hace unos años la seguridad en los SCI (Sistemas de Control Industrial) no era un tema muy importante, pero en los últimos años los SCI se han convertido en uno de los principales objetivos de ataque haciendo de la seguridad un tema realmente importante.

DNP3 es un protocolo industrial para comunicaciones entre equipos inteligentes (IED) y estaciones controladoras, componentes de sistemas SCADA. Se trata de un protocolo muy utilizado en el sector eléctrico con gran popularidad en Estados Unidos y Canadá. Cuenta con menos popularidad en Europa debido al uso de alternativas como IEC-60870 101 y IEC-60870 104.

DNP3 cuenta con algunos retos de seguridad que pueden hacer peligrar la confidencialidad, autenticidad e integridad de los mensajes.

En este artículo se presentarán las características principales del protocolo DNP3, sus funciones principales, algunos de los factores de riesgo del protocolo y recomendaciones de seguridad para una implementación más segura del protocolo.

II. INFRAESTRUCTURAS SCI

Sistemas de control industrial son dispositivos, sistemas, redes y controladores utilizados para operar y/o automatizar procesos industriales. Se encuentran cada vez más expuestos a la interacción con otros sistemas del entorno de internet y han pasado a ser un objetivo importante de ataques.

III. DNP3

Es un protocolo industrial para comunicaciones entre equipos inteligentes y estaciones de control, componentes de sistemas SCADA [4].

DNP3 presenta varias funcionalidades que hacen de él un protocolo más robusto, eficiente, y compatible que otros protocolos más antiguos como puede ser Modbus. También se trata de un protocolo más complejo.

Es un protocolo de tres capas según el modelo OSI:

- Nivel de enlace
- Nivel de aplicación
- Nivel de transporte también denominado pseudo-nivel de transporte ya que no cumple con todas las especificaciones del modelo OSI.

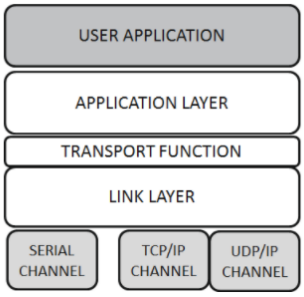

Ilustración 1.Estructura modular protocolo DNP3.

El formato de trama utilizado está basado en el FT3 recogido en las especificaciones IEC 608770-5 y hace uso de la comprobación de redundancia cíclica (CRC) para la detección de errores.

Tipos de datos DNP3:

La información de DNP3 se clasifica en cuatro tipos básicos [5]:

- Entradas binarias.
- Salida binaria.
- Entrada analógica.
- Salida analógica.

A esos tipos básicos se les añaden dos más:

- Contadores.
- Entrada binaria doble

Cada dato DNP3 se denomina punto y se identifica por un índice. El valor actual del dato se denomina valor estático.

El punto puede generar eventos por cambios de valor o ante la recepción de comandos. Estos eventos pueden clasificarse como eventos de clase 1, clase 2 o clase 3.

El modelo de datos DNP3 está basado en un esquema de objetos.Alguno de los objetos más comunes utilizados en comunicaciones DNP3 son:

- **Objeto 1-**Entradas digitales: Permite la lectura de las entradas digitales.
- **Objeto 2-**Eventos de las entradas digitales.
- **Objeto 20**-Contadores: Este objeto permite la lectura o manipulación de contadores.

A. Capa de enlace:

Los mensajes a nivel de enlace en DNP3 se denominan tramas y el tamaño máximo de la trama es de 292 bytes.

La capa de enlace es la encargada de las tareas de direccionamiento y de detección de errores (CRC).

Una trama DNP3 consta de tres bloques:

- Cabecera
- Datos
- CRC

Ilustración 2. Trama DNP3.

B. Capa de transporte:

Los mensajes a nivel de capa de transporte se denominan segmentos. El tamaño máximo de los segmentos es de 149 bytes.

La función de la capa de transporte es permitir mensajes únicos y estructurados en múltiples tramas y múltiples fragmentos.

Esta capa trocea los fragmentos recibidos a través de la capa de aplicación y agrega la cabecera de transporte y ensambla en el extremo receptor las tramas recibidas a través de la capa de enlace.

C. Capa de aplicación:

Los mensajes a nivel de aplicación son denominados Fragmentos. El tamaño máximo de un fragmento está establecido en 1024 bytes.

La capa de aplicación se encarga de procesar los fragmentos recibidos de la capa de transporte.

Esta capa define funciones que se intercambian entre estaciones remotas y controladoras. Algunas de estas funciones son:

1:READ: Lectura de valor estático o eventos.

2: WRITE: Escritura de atributos del equipo.

3:SELECT: Servicio de control de selección.

4:OPERATE: Orden tras selección.

5:DIRECT_OPERATE: Orden directa sin selección.

7:IMMED_FREEZE: Orden de congelado inmediato.

9:FREEZE_CLEAR: Congelado y reset a 0.

13:COLD_RESTART: Reset total de la estación remota.

14:WARM_RESTART: Reset parcial de la estación remota.

20: ENABLE_UNSOLICITED: Se usan en estaciones remotas modernas para activar el envío espontáneo.

21: DISABLE_UNSOLICITED: Se usan en estaciones remotas modernas para desactivar el envío espontáneo. Si se desactiva la recogida de eventos se realiza por lectura de clase 1, 2 y 3.

22: ASSIGN_CLASS: Permite asignar a cada punto o tipo de punto una clase para los eventos que genera. Por lo general la estación remota ya los organiza, pero este servicio si se implementa le permite al master cambiar este orden.

IV. SEGURIDAD Y FACTORES CRÍTICOS

DNP3 es un protocolo que se encuentra centrado en maximizar la disponibilidad del sistema y deja de lado otros factores como son la confidencialidad e integridad de los datos. Se trata de un protocolo sin cifrado [3].

En el nivel de capa de enlace se incluyen funciones típicas de esta capa como detección de errores a través del CRC(lo que no es una medida de seguridad ya que cualquier que modifique las tramas podrá cambiar el CRC), pero no ninguna medida adicional que no ofrezca ethernet.

A nivel de aplicación existen un estándar de autenticación segura [1]. Este estándar proporciona autenticación, integridad y confidencialidad y se resuelven los problemas de:

- Suplantación de identidad.
- Modificación de mensajes.
- Ataques de reinyección de tráfico.
- Eavesdropping.

El protocolo DNP3 permite llevar a cabo diversas funciones que se han comentado en el apartado anterior. Algunas de estas funciones pueden ser críticas. Las funciones críticas de DNP3 son: write, operate, direct operate, direct operate no ack, cold_restart, warm_restart, abort y stop application.

V. RECOMENDACIONES DE SEGURIDAD

Con el fin de mejorar la seguridad de las comunicaciones realizadas a través del protocolo DNP3 será recomendable:

- Monitorizar las comunicaciones no DNP3 en los puertos TCP/UDP 20000.
- Prestar especial atención a las funciones críticas.
- Utilizar la versión segura de DNP3 siempre que sea posible. Si el uso de esta versión no es posible será recomendable el uso de DNP3 encapsulado en un protocolo de transporte seguro. Este podría ser TLS.

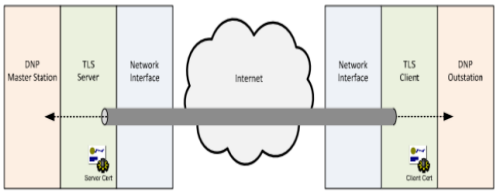

Ilustración 3. DNP3 encapsulado en TLS [3].

VI. CONCLUSIONES

Es este artículo se ha presentado el protocolo DNP3 y las funciones que se pueden realizar a través de este. Además hemos profundizado en la seguridad de este protocolo tratado tanto las funciones críticas como las vulnerabilidades del protocolo. Como último punto se han realizado una serie de recomendaciones con el fin de alcanzar una comunicación segura a través de DNP3.

VII. REFERENCIAS

[1]Overview of DNP3 Security Version 6
[2]https://ccaps.umn.edu/documents/CPE-Conferences/MIPSYCON-Papers/2019/AllAboutEve.pdf
[3]https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_protocolos_seguridad_red_sci.pdf
[4] https://es.wikipedia.org/wiki/DNP3
[5]https://www.ensotest.com/es/dnp3/introduccion-a-la-norma-ieee-1815-dnp3/