-=[ **CONTROLANDO TABLEROS ELECTRÓNICOS (PASAMENSAJES)**
-=[ nitr0us < nitrousenador@gmail.com >
-=[ http://www.genexx.org/nitrous/
-=[ 26/Agosto/2007
-=[ México

Este documento no explica como controlar algún tablero electrónico de cierta marca, ni tampoco como controlar los tableros electrónicos de X empresa, solamente es la demostración de una implementación insegura en el protocolo usado por cierta marca de tableros. Así que este documento debe tomarse como base para que el lector haga sus propios análisis con diferentes tableros.


Figura 1.- Ejemplos de tableros electrónicos pasamensajes.

Hace un par de meses me llegó a las manos uno de estos tableros pasa-mensajes con el software necesario para controlarlo. Estos funcionan a base de LEDs controlados por microcontroladores PIC y también cuentan con una tarjeta de red por medio de la cual se comunica con el software controlador.

Pues bueno, se me ocurrió analizar como se comunica el software (una interfaz gráfica simple para MS Windows) con los tableros haciendo varias pruebas para analizar el comportamiento del protocolo. Cabe mencionar que estos tableros cuentan con diferentes efectos (el tablero aquí analizado cuenta con diez), ocho de ellos solo permiten la escritura de 23 caracteres aproximadamente, mientras que los otros dos efectos más utilizados soportan más de de 60,000 caracteres ya que pasan el mensaje de derecha a izquierda o a la inversa.

Bien, lo primero que hice fue instalar un analizador de tráfico como Wireshark en la computadora donde se corre el software controlador y posteriormente me puse a enviar diferentes mensajes con diferentes efectos para luego analizar el tráfico en Wireshark. En las siguientes capturas de pantalla se muestra el tráfico analizado, desde la computadora con el software controlador (192.168.2.26) hasta el tablero electrónico (189.132.35.12), nótese que todo viaja en **texto plano**.

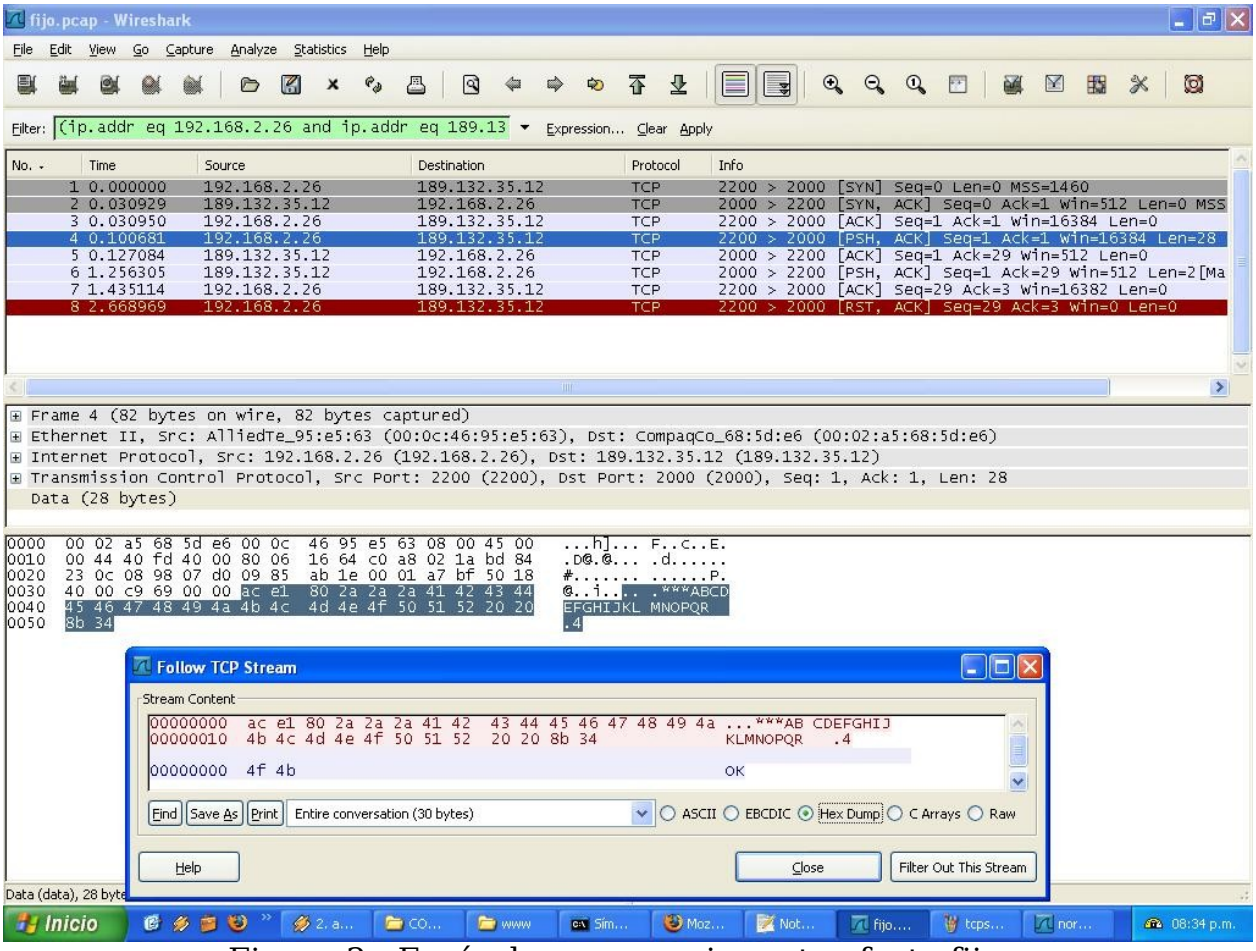

Figura 2.- Envío de un mensaje corto efecto fijo.

En la captura de pantalla anterior se envió un mensaje con un efecto fijo, es decir, el mensaje nunca se moverá y es por ello que solo acepta 23 caracteres de longitud. Los bytes seleccionados son del protocolo implementado por el fabricante, estos van sobre TCP/IP.

Viendo el flujo de datos de dicha conexión, vemos que el tablero responde con la palabra “OK” (bytes 0x4f 0x4b), y por intuición sabemos que el tablero responde al software siempre y cuando se ha publicado correctamente el mensaje.

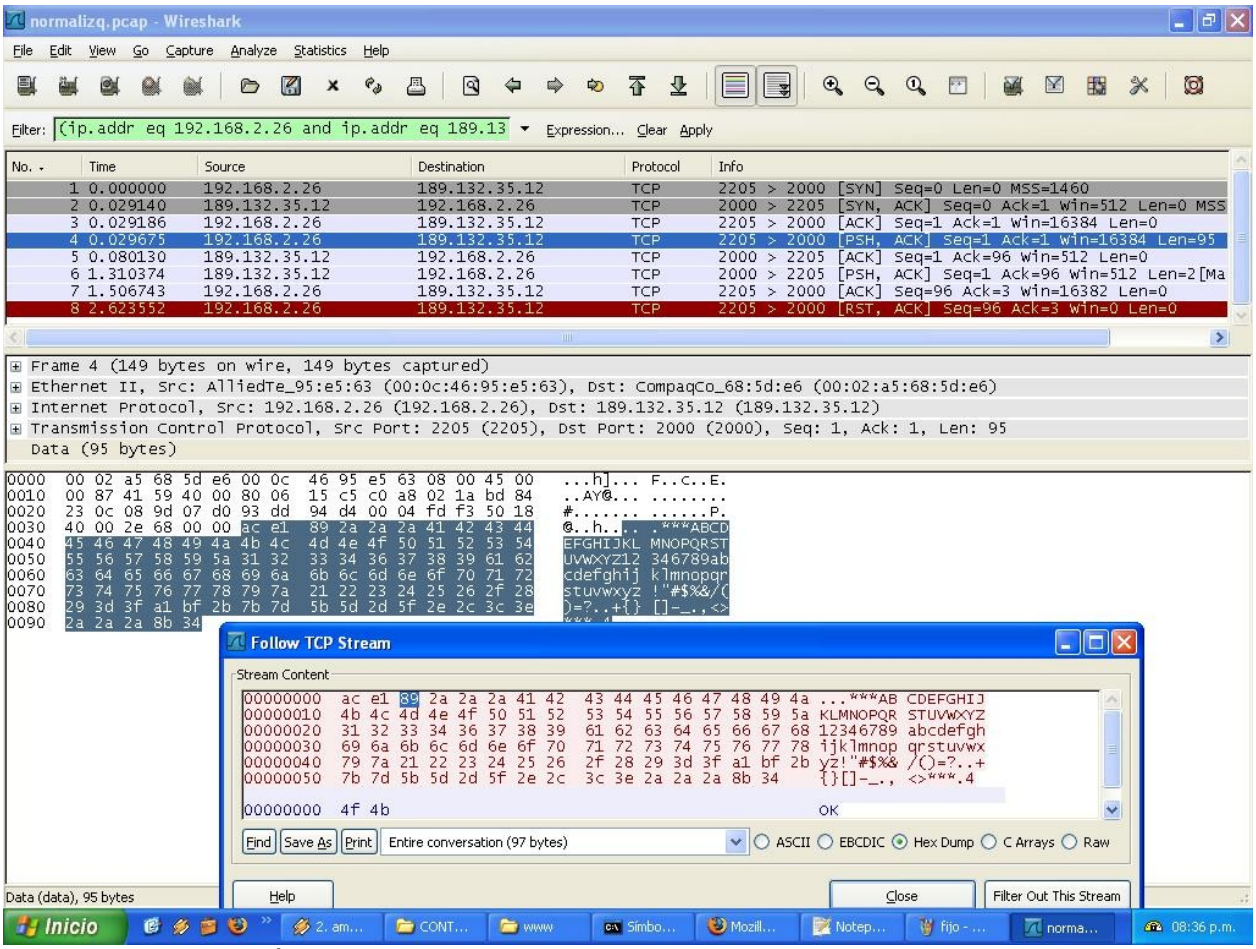


Figura 3.- Envío de un mensaje largo con efecto de desplazamiento a la izquierda.

En la siguiente prueba, se envió un mensaje con otro efecto y nótese que el byte en el offset 3 cambió. Luego de aplicar ingeniería inversa al protocolo concluimos con los siguientes puntos:

- **El tablero no verifica si quien le envía los datos es en realidad el software controlador(no autenticación).**
- **El tráfico va en texto plano (no encripción)**
- El fabricante usó la idea de delimitar el mensaje a nivel aplicación usando técnicas usadas a nivel de enlace de datos en el modelo OSI, es decir, usa los bytes 0xac y 0xe1 para indicar el inicio del mensaje y los bytes 0x8b 0x34 para indicar el fin del mismo.
- El tercer byte está destinado para indicar el efecto.
- Si el efecto implica la muestra estática del mensaje, entonces, este debe truncarse a 23 bytes (longitud máxima de caracteres imprimibles al mismo tiempo en el tablero).
- Finalmente, si el tablero publicó satisfactoriamente el mensaje, este devuelve la cadena OK al software controlador para chequeo de errores.

Y bien, ahora como prueba del concepto desarrolle mi propia implementación de este simple protocolo a nivel aplicación utilizando el lenguaje de programación PHP, así, puedo subir el programa a un servidor Web, y sabiendo la dirección IP pública de un tablero de cierta marca puedo enviarle el mensaje que quiera.


Figura 4.- Controlador de Tableros funcionando.

En conclusión, la seguridad del dispositivo tomado como caso de estudio es nula ya que cualquier persona puede publicar cualquier mensaje sabiendo solamente la dirección IP del tablero.

He visto muchos tableros en las calles, usado por agencias de viajes, tiendas de ropa, restaurantes y hasta ciertos departamentos del gobierno. Una vez encontrada una implementación con seguridad nula como esta, solamente es cuestión de conseguir la dirección IP y listo, a divertirse un rato. Una buena estrategia para conseguir dichas direcciones es usando ingeniería social, enviando correos a personas que trabajan dentro de ese mismo edificio y analizando los encabezados de los correos como respuesta.

A veces, la dirección IP del sitio Web es la misma del tablero, ya que he visto implementaciones en donde solamente usan el modem 2Wire de TELMEX para darle salida a Internet a todo el edificio, y si dicho establecimiento cuenta con un servidor Web pues es probable que el tablero esté conectado directamente al modem.

Por último, en este mismo paquete se anexan videos del tablero analizado y controlado por mí y el código fuente de mi implementación del protocolo. Espero hayan disfrutado y aprendido algo de este documento, cualquier duda o comentario a nitrousenador@gmail.com.

Saludos especiales a CRAc, underground.org.mx, #0hday.org, #hackerss, alt3kx, Marigel y a los que faltan ;).

//nitr0us