TITULO

Implementación de un controlador de acceso integrado para el sistema de seguridad de los laboratorios de la FIEC.

AUTORES

David Domínguez Bonini[1], Carlos Monsalve[2]

[1] Ingeniero en Electricidad especialización Electrónica, 1998.

[2] Director de Tesis, Ingeniero en Electricidad especialización Computación, Escuela Superior Politécnica del Litoral, 1990, Postgrado EEUU, Purdue University, 1995, Profesor de la ESPOL desde 1990.

RESUMEN

Este artículo reseña los aspectos más importantes del proceso de diseño e implementación de un sistema integrado encargado de controlar las puertas de acceso a los laboratorios de la FIEC. Este sistema es la más reciente contribución a una estrategia de seguridad que se ha venido desarrollando desde hace varios años, la cual consiste en la implementación de un servidor central de seguridad, el cual recibe pedidos de autorización de acceso de sistemas clientes ubicados en las puertas de acceso a las áreas que se desea controlar.

Nuestro trabajo consiste en la implementación de una versión mejorada del componente cliente del sistema de seguridad arriba descrito. Al inicio del artículo hacemos una descripción del sistema global de seguridad, y realizamos una comparación entre nuestro cliente de seguridad y las anteriores implementaciones del mismo. A continuación pasamos a describir los distintos procesos de diseño que tuvimos que realizar para el desarrollo del sistema, y reseñamos los aspectos más importantes y/o interesantes de los mismos. Como conclusión del artículo, realizamos una comparación entre los logros obtenidos con el proyecto y los objetivos iniciales del mismo.

INTRODUCCION

Desde hace algunos años la FIEC viene estudiando y desarrollando un esquema de seguridad para las distintas dependencias bajo su control. Uno de los componentes de este esquema es la implementación de un sistema de control de acceso para los laboratorios de la facultad. Este tema ha sido abordado ya por varios proyectos de tesis y tópicos de graduación, incluyendo aquel sobre el cual está basado este artículo.

CONTENIDO

El sistema de control de acceso proyectado para los laboratorios de la FIEC se compone, en su estado actual, de un servidor central que contiene una base de datos de usuarios del sistema, y de clientes remotos que son utilizados por los usuarios para solicitar acceso a las dependencias controladas por estos últimos. El proceso de

autorización de acceso (ver la figura 1) es iniciado por el usuario, el cual ingresa su código de identificación (número de matrícula o de cédula) mediante una lectora de código de barras o (en el caso de números de cédula) mediante el teclado numérico, seguido (opcionalmente) por una clave secreta de acceso ingresada en el teclado. El pedido de acceso con los datos del usuario es enviado por el cliente hacia el servidor a través de una red TCP/IP, utilizando Ethernet como medio de conectividad física. El servidor procesa el pedido tomando en cuenta diversas políticas de seguridad y factores adicionales a la simple identificación del usuario, y responde positiva o negativamente al pedido realizado por el cliente. Este último procede entonces a abrir la puerta de la dependencia a la que el usuario desea ingresar (si es que el servidor así lo ha dispuesto).

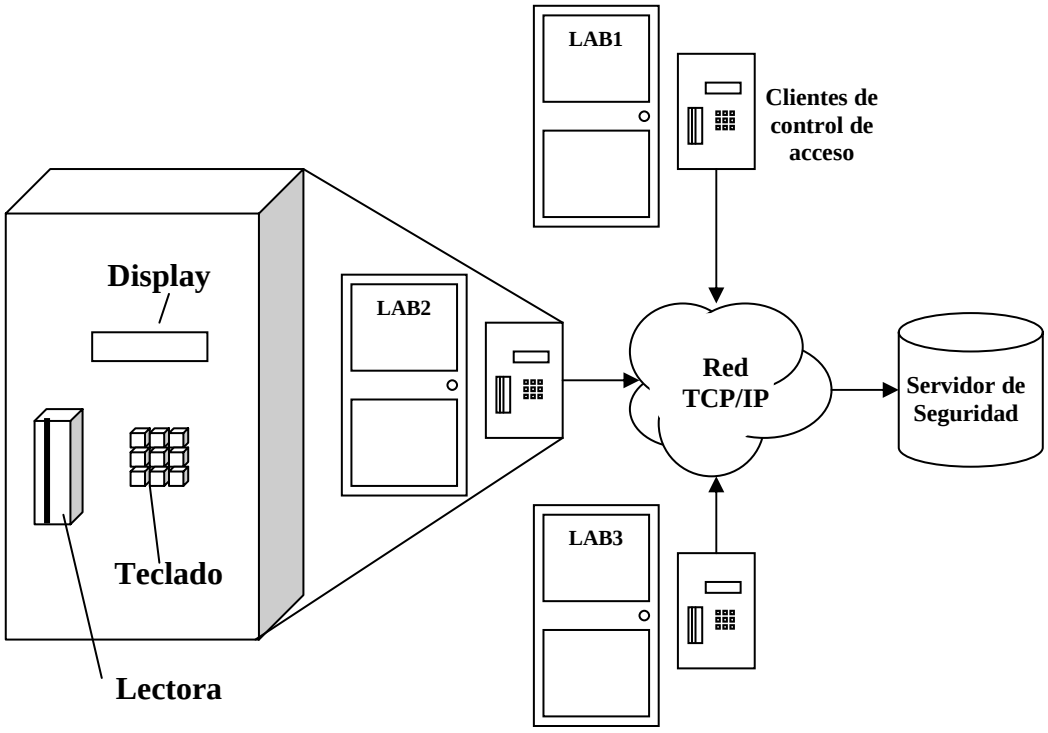

Figura 1: Esquema del sistema de seguridad

Los trabajos previos al nuestro han concentrado sus esfuerzos en el desarrollo del sistema de seguridad propiamente dicho (interacción cliente-servidor, políticas de seguridad), en el desarrollo del servidor de seguridad, y en la implementación de clientes de control de acceso basados en computadores personales. La contribución de nuestro proyecto consiste en el diseño e implementación de un dispositivo electrónico dedicado a la función de cliente de control de acceso, con la finalidad de facilitar la implementación y mantenimiento del sistema de seguridad.

Los clientes de control de acceso utilizados hasta ahora consisten en programas diseñados para ejecutarse en ambientes DOS o Windows, para lo cual se requiere la utilización de un computador personal y sus accesorios respectivos (monitor, teclado, ratón, tarjeta de red, etc.). Para rebajar el costo de implementación de estos clientes al mínimo, se han utilizado computadores tipo i386, los cuales pueden ser obtenidos a precios bastante reducidos, dada su actual obsolescencia. Sin embargo, existen una

serie de inconvenientes en la utilización de este tipo de computadores (y en el uso de computadores personales en general) como controladores de acceso. Debido a la antigüedad del equipo a utilizarse, es inevitable la existencia de heterogeneidad en el inventario de controladores, dificultad en la obtención de partes de repuesto, y un elevado nivel de fallas de hardware. Todos estos problemas, unidos a la necesidad de instalar los equipos en áreas semidescubiertas hacen suponer serias dificultades de implementación y mantenimiento del sistema.

Dados estos problemas, se consideró deseable intentar el desarrollo de un cliente de control de acceso de diseño integrado y miniaturizado, el cual permita homogeneidad y reducción de inventario, facilidad de implementación y mantenimiento, y costos reducidos. El diseño de nuestro equipo ha sido mentalizado para conseguir cumplir hasta donde sea posible con estas metas. Un requerimiento adicional que debe ser mencionado, es que el nuevo controlador debe ser capaz de interoperar con los equipos y programas ya desarrollados, específicamente con el servidor de seguridad existente.

Debido a la necesidad de operar de manera similar a los controladores ya existentes, nuestro equipo debe incluir una interface de red Ethernet para conectividad hacia el servidor central, además de las interfaces necesarias para recoger los datos del usuario y para abrir la puerta. A nivel de programación nuestro equipo debe ser capaz de codificar los datos ingresados por el usuario, comunicarse con el servidor a través de una red TCP/IP, enviar pedidos de autorización de acceso e interpretar las respuestas del servidor.

La implementación electrónica de nuestro controlador de acceso se realizó usando un microcontrolador Intel 80C31 como unidad central de proceso. El uso del 80C31 nos permite abaratar el costo del sistema, y reducir su complejidad, aunque hace un poco más difícil su proceso de desarrollo (debido a la escasez y costo de las herramientas de programación compatibles con este dispositivo). Este microcontrolador de 8 bits puede manejar un máximo de 64 Kbytes de memoria (en espacios separados de código y datos), lo cual nos presenta una serie de limitaciones a la hora de implementar la programación de nuestro sistema, como veremos más adelante. Además, el 80C31 posee 32 líneas de entrada/salida de datos (no todas disponibles en nuestra implementación) las cuales utilizamos para controlar los distintos subsistemas que posee nuestro equipo. La presencia de líneas de entrada/salida de datos es una gran ventaja para el diseño de dispositivos integrados, ya que nos permite reducir considerablemente el uso de lógica externa para controlar periféricos; lo cual no es el caso si se utiliza microprocesadores de propósito general, como la serie Intel x86.

La unidad central de proceso de nuestro controlador debe interoperar con una serie de subsistemas para poder realizar sus labores. Estos sistemas subsidiarios incluyen: una interface de red Ethernet, una interface hacia un display fluorescente, una interface de comunicaciones tipo teclado AT para operar un teclado numérico y una lectora de código de barras, y una interface eléctrica hacia el relay encargado de abrir la puerta controlada del sistema. Estos subsistemas varían en importancia y complejidad, siendo el más notable aquel que se encarga de la comunicación de datos hacia la red Ethernet conectada al equipo.

Nuestra interface de red Ethernet está basada en el National DP83902A ST-NIC, un dispositivo que integra en un solo paquete (PLCC de 84 pines) todas las funciones necesarias para la implementación de interfaces Ethernet tipo AUI y tipo 10BaseT. Este circuito integrado es ampliamente utilizado en la industria de networking, debido a que en él se basan los conocidos adaptadores de red NE1000 y NE2000. La implementación de nuestro subsistema de acceso a red es muy similar al utilizado por estos adaptadores (y por sus incontables clones), es decir que se basa en una estructura de transferencias programadas, con un buffer de almacenamiento de paquetes de red, y un puerto asincrónico de transferencia de datos entre la memoria principal del sistema y el buffer de red.

Las comunicaciones de datos y comandos entre la unidad central de proceso de nuestro sistema y los distintos periféricos bajo su control se realizan utilizando, según sea el caso, el bus externo de ocho bits del 80C31 ó las líneas de entrada/salida de datos de este último. Así, la interface hacia el display fluorescente de nuestro sistema utiliza el bus externo, las interfaces de teclado/lectora y del portero eléctrico utilizan líneas de entrada/salida, y la interface de red Ethernet utiliza una combinación de ambos esquemas. Para facilitar la implementación física del controlador, utilizamos unidades de lógica programable (PALs) para integrar todas las funciones lógicas necesarias para la interacción entre el 80C31 y sus distintos periféricos; debido a esto, el número de circuitos integrados utilizados ha sido reducido al mínimo.

En lo que se refiere a la implementación del microcódigo ejecutado por la unidad central de proceso de nuestro sistema, este ha sido desarrollado mayormente en lenguaje ANSI C, con pequeñas secciones escritas en lenguaje ensamblador, lo cual les da una mayor eficiencia y rapidez que lo que es posible obtener con un compilador C. El microcódigo de nuestro sistema está organizado como un lazo infinito de respuesta a eventos externos (entrada de paquetes de red, ingreso de datos de parte de un usuario), y de labores periódicas de mantenimiento y control. La parte más significativa e importante del microcódigo es la implementación TCP/IP utilizada por nuestro sistema.

Los controladores de acceso anteriormente desarrollados utilizan el protocolo TCP como transporte de datos. Esto no representa un problema para estas implementaciones, ya que al estar basadas en plataformas x86, tienen normalmente espacios de memoria RAM en exceso de 1 Mbyte. Este no es nuestro caso, dado que nuestro microcontrolador puede manejar un máximo de 64 Kbytes de memoria. Debido a esto, el uso de fragmentación de paquetes IP y el uso de TCP como transporte se hacen muy difíciles. Nuestro sistema debe entonces basar sus interacciones de red en el protocolo UDP, lo que requirió hacer modificaciones en algunas secciones de los programas servidores anteriormente desarrollados. De manera general, nuestra implementación de la arquitectura TCP/IP implementa los siguientes protocolos: Ethernet II y ARP a nivel de enlace de datos, IP e ICMP a nivel de red, UDP a nivel de transporte, y finalmente el protocolo propietario de encapsulación de datos utilizado por nuestro sistema de seguridad. Por las razones ya mencionadas, y también para ahorrar espacio de código y almacenamiento de datos, nuestra implementación de TCP/IP es parcial; las funcionalidades no utilizadas son: fragmentación de paquetes IP, campos de opciones de IP, la mayoría de las funciones de diagnóstico de ICMP, y finalmente, el protocolo TCP. Consideramos que nuestra

implementación de la arquitectura TCP/IP puede ser de gran utilidad para el estudio e implementación de aplicaciones de networking en sistemas integrados.

CONCLUSIONES

Para concluir quisiéramos decir que nuestro sistema de control de acceso cumple, en mayor o menor grado, con todos los objetivos planteados al inicio del proyecto. Nuestro equipo es mucho más compacto (y por lo tanto fácil de instalar) que las anteriores implementaciones; además, no posee partes móviles y su diseño está totalmente documentado, por lo que su confiabilidad y facilidad de mantenimiento son superiores. Su costo de implementación desgraciadamente no es marcadamente inferior a lo que se podría obtener usando PCs descartados de otras tareas como controladores, pero consideramos que a largo plazo podría resultar más económico, por las razones mencionadas arriba. Todo esto no toma en cuenta el que quizás es el elemento más importante a favor de la implementación de este tipo de equipos, el cual es el impulso que dan a las áreas de investigación y desarrollo de equipos electrónicos en la ESPOL.

REFERENCIAS

1. D. Domínguez, “Diseño e implementación de un sistema de control de acceso manejado por un servidor remoto a través de una red Ethernet; para ser utilizado en las diferentes áreas e instalaciones de la FIEC.” (Tesis, Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica del Litoral, 1998)