Control de acceso a las instalaciones de la Universidad Autónoma de Aguascalientes

Marco Teórico

Beristain Urrea Edgar Eduardo

Molina Vargas Carlos Daniel

Universidad Autónoma de Aguascalientes

Ingeniería en Sistemas Computacionales

Departamento de ciencias básicas

21 de junio de 2020

Marco teórico

- **Control de acceso**
    - Sistema de seguridad que permite mantener protegidos al personal de las instalaciones, pues mantiene la seguridad de forma remota o física, Permiten brindar una verificación del usuario para autorizar o no su acceso a ciertas zonas**.** Se pueden implementar tres tipos de identificaciones:
        - **Sistema de trazabilidad:** Mecanismo que debe cumplir con la verificación en dos pasos, es decir, que se realice una confirmación de un movimiento al complementarse junto con un conjunto de disciplinas.
        - **Sistema de autenticación:** Métodos que necesitan una verificación por medio de diferentes medios (clave de acceso, huella, código, por voz, facial, por matrícula, etcétera), para permitir el acceso al usuario a cierta información o sección del sistema.
        - **Sistema de autorización:** Acción que para completarse necesita una autorización del sistema o una aplicación de terceros para obtener información en distintas localidades.
- **Tipos de sistemas**
    - **Sistemas autónomos:** Sistemas simples que no están conectados entre sí, no tienen muchas complicaciones, por lo que no almacenan ningún tipo de registro. Éstos se encargan de controlar los accesos a uno o varios lugares.
    - **Sistemas de acceso en red:** Sistemas opuestos a los autónomos, estos son complejos y están totalmente interconectados a un computador que registra cada movimiento, tales como tipo de acceso, fecha, hora y usuario al que se le autoriza el acceso. Tienen una alta monitorización, por lo que son los más usados.
    - Se implementará un sistema de acceso en red, pues el caso es tener un acceso seguro por las diferentes vías de acceso de la universidad, y este mismo sistema puede aplicarse para las diferentes instalaciones con las que cuenta la UAA.
- **Consideraciones a tomar en cuenta al diseñar un sistema de control de acceso**

- El sistema de acceso se debe de planear de manera específica para que cumpla las necesidades del espacio para el cual se deberá de proteger. Se busca diseñar un sistema que sea óptimo, para evitar complicaciones a futuro, por lo que se deben de tomar en cuenta varios factores:
  - **Tiempo de ingreso:** Se deberá de mantener en lo mínimo posible para evitar ralentizar las actividades del personal.
  - **Tráfico:** Ligado al punto anterior, pues una gran cantidad de tráfico puede saturar los sistemas de acceso, por lo que se debe de pensar en el punto pico para medir el tiempo.
  - **Efectividad:** Se debe de medir que tan efectivo es el sistema y calcular la probabilidad de que este falle.
  - **Aislamiento:** Estudiar donde se colocara el sistema de acceso y verificar su efectividad. Ver si es mejor que el sistema actual o si causa más o menos incomodidades.

- **Importancia del control de acceso**
  - "Un control de acceso es aquel sistema de seguridad que innegablemente nos permite mantener una diversa cantidad de opciones al tratarse de que estemos protegidos, pues lo que no solo se limita a un área o espacio como tal, sino a un control total, lo que protege nuestra seguridad de forma: remota, móvil, integrada o física e incluso poder contar con un servicio contra incendios" [1].
  - La principal razón para implementar un módulo de acceso en el sistema es el uso constante de las tecnologías en la actualidad, arrasando por completo sobre las herramientas físicas. Esto conlleva a la necesidad de utilizar infraestructuras basadas en red, sin embargo, esta necesidad trae consigo un alto riesgo de oportunidades de vulnerabilidades, las cuales pueden ser aprovechadas por usuarios externos con fines maliciosos. Por lo que el sistema de acceso debe de contar con una llave segura para poder acceder a las instalaciones. Existen diversas formas de comprobar la identidad de una persona, puede ser por características físicas, de comportamiento o llaves externas al usuario.

    Entre los métodos de reconocimiento por medio de características físicas tenemos:

- **Lector de huella dactilar: "**La huella dactilar es una manera segura de garantizar la identidad de un individuo, pues esta es única por persona y no cambian con la edad" [2] , por lo que no importa cuanto tiempo pase, se puede verificar de quién es la huella que se colocó en el lector (si esta se encuentra en la base de datos). Hay dos partes cruciales para verificar una huella, crestas: las partes levantadas que forman una serie de líneas que siguen un patrón, y valles: la parte inferior de la huella. Estas características se pueden comparar contra una foto de referencia o contra un patrón de capacitancia (los valles no se pueden comprobar por este método). Los sensores pueden variar de precio, pero suelen tener un costo relativamente bajo, dependiendo mucho de la calidad de este. También se podría hacer uso de sensores de smartphones.
- **Reconocimiento facial:** Puede resultar muy efectiva si se cuenta con la tecnología adecuada, pues es fácil que una técnica de bajo coste pueda fallar. Se escanea la forma y la localización de las características de un rostro de una persona. Estos datos se comparan con la información almacenada en la base de datos. Hay sensores con tecnología 3D que resultan altamente efectivos, mucho mejores que los sensores que solo toman información de una foto en 2D, sin embargo estos resulta, con costos muy altos.
- **Reconocimiento de retina e iris:** También existen los escáneres de retinas y de iris, los de retina iluminan el ojo de la persona para tomar una foto del patrón que esta sigue, tienen la desventaja de que es fácil que este patrón cambie tras pasar por una cirugía o al traer anteojos. Los de iris analizan la parte de color del ojo, traducen a texto el patrón del músculo en esta área y lo empata con la base de datos, el iris no suele verse afectado tras operaciones o al traer lentes.

"Para las características de comportamiento tenemos opciones como verificar una firma electrónica o reconocimiento de voz" [2]. Estos métodos no suelen ser muy confiables ya que resultan difícil verificar, pues errores mínimos pueden denegar el acceso. Un dia con la mano hábil lastimada o si se tiene la garganta inflamada pueden impedir que se logre el acceso de una persona que tiene el permiso de hacerlo.

Para los métodos con llaves de acceso ajenas a la persona, contamos con varias opciones factibles:

- **Tarjeta de acceso con banda magnética:** Se pasa la tarjeta por un escáner y este verifica si la información que esta contiene es correcta. Es un método rápido y sencillo de controlar el acceso, sin embargo cuenta con varias desventajas. La información se almacena en la banda magnética, por lo que esta puede dañarse y ya no funcionar por lo que se denegará el acceso. También es fácil de extraviar, por lo que alguien más puede hacerse de ella y pasar por los controles.
- **Contraseña:** Se puede simplemente poner un pad numérico y solicitar por un contraseña. Sencillo y de bajo costo, pero puede resultar fácil de descifrar o de que alguien ajeno a las instalaciones vea cómo se ingreso la clave de acceso. Así como resulta bastante lento si se cuenta con una gran cantidad de tráfico.
- **Token de acceso:** Similar a la contrasenia, pero cada vez que se quiere ingresar a cierta sección, se solicita un token de acceso el cual dura por un tiempo limitado, este se ingresa y caduca, por lo que no importa si alguien mas ve la clave ingresada, no le funcionaria. Este token se pueden otorgar por medio de mensajería, correos, o una aplicación diseñada para otorgarlos. Más seguro que la contraseña pero el problema del tráfico se repite.
- **Código de barras:** Se puede tener un código de barras en una tarjeta, en una imagen guardada en el celular o en cualquier accesorio que resulte cómodo. El código de barras cuenta con una clave de acceso la cual es escaneada por un sensor. Este método resulta cómodo y barato, ademas de que el tráfico fluye rápidamente pues el sensor puede comprobar la clave de manera inmediata. Sin embargo, si esta clave se conserva puede ser copiada.

La idea es hacer uso de los dos puntos anteriores, se otorgará un token de acceso por medio de una aplicación, el cual será transformado a código de barras o qr para su fácil y rápida lectura, y así garantizar el acceso del personal adecuadamente. Como la Universidad Autónoma de Aguascalientes es un espacio de acceso público, a quien no cuente con el token de acceso no se le denegara, sin embargo se deberá

de capturar sus datos para tener todo bajo control. La captura se haría por medio de una foto a una identificación o placas del automóvil si el usuario cuenta con este.

Referencias

1. Camilo Eduardo Gamba Roa, Sebastián Mojica Mojica. (2010). Control De Acceso Con Verificación De Identidad Por Medio De Código De Barras. 20/04/2020, de Pontificia Universidad Javeriana Facultad De Ingeniería Departamento De Electrónica Sitio web: https://repository.javeriana.edu.co/bitstream/handle/10554/7043/tesis488.pdf?sequence=1&isAllowed=y
2. Zynnia Verónica Vargas Vergara. (2013). Sistema de Control de Acceso y Monitoreo con la Tecnología RFID para el Departamento de sistemas de la Universidad Politécnica Salesiana Sede Guayaquil. 20/04/2020, de Universidad Politécnica Salesiana Sede Guayaquil Sitio web: https://l.facebook.com/l.php?u=https%3A%2F%2Fdspace.ups.edu.ec%2Fbitstream%2F123456789%2F5380%2F1%2FUPS-GT000473.pdf%3Ffbclid%3DIwAR3GVS0w2dSjjOay8EeYFzbPVl4ih95jK0ygkmUNA7dpgjXOdsEGkvKEzb8&h=AT2FdnW3e3Nu-hGj1z7wIzw-7wu1WPHVOMoSaU3f_apFDj4_N6KdnKDhj5VzlqwMJ3SUOPRdxdMjGq098T9ywaff_EdnAE2XcxVowYeIqRt9j2xX8qEQLZdCN802c-hN-IPcL5ycSNu6Rw
3. S/A. (2018). Control de Acceso: Qué es y su Importancia. 20/04/2020, de Viserco Sitio web: https://www.viserco.com/control-de-acceso-que-es-y-su-importancia?fbclid=IwAR0hit0nNikOZ-G7eHLMqSwoS1kLizxFT60RqgV6BCqm0_XHun--gBhvglA
4. S/A. (S/A). ITS 421 - Tactical Perimeter Defense. 20/04/2020, de Steve Vincent Sitio web: https://stevevincent.info/ITS421_2016_7.htm?fbclid=IwAR2_-Ezf6Fu4MQ9o5FsTKP7d8bWbutxkLk8evF9KapZ68Pdp_8hXxVd5TAQ
5. Thomas Wilhelm, Jason Andress. (2011). Physical Access Control. 20/04/2020, de Sciencedirect Sitio web: https://www.sciencedirect.com/topics/computer-science/physical-access-control?fbclid=IwAR11DcpHd2F40i5YGMbAqqf4cDSOJS915hbh6Qlt84YixoyDRC82zq24Pao

6. S/A. (S/A). ¿Qué es un Sistema de Control de Acceso? . 20/04/2020, de Tecno Seguro Sitio web: https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso?fbclid=IwAR1PUA_qx64OnD70NRzvq1yXvA3KoCaEc9KvywZYrUof04oyuvFN27W_A6s