UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

INTRODUCCIÓN DE ASPECTOS DE SEGURIDAD EN UNA VIVIENDA INTELIGENTE

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Jesús Melo Solanes

Tutor: Joan Josep Fons Cors

2014-2015

Resumen

En este documento se encuentra la memoria del proyecto final de grado en el que se describen las aplicaciones y elementos de seguridad que debería utilizar un sistema domótico para poder autenticar a los usuarios con un margen de error despreciable. Al mismo tiempo debería resultar fácil y cómodo para las personas que lo vayan a utilizar, ser completamente seguro frente a posibles ataques desde el exterior o ante intentos de suplantar la identidad del usuario.

Durante la elaboración del proyecto se ha llevado a cabo:

- Un análisis en profundidad sobre los métodos de autenticación y las tecnologías biométricas, comparadas entre ellas para escoger la más apropiada, combinándola con otras formas de autenticación

- La definición de una jerarquía de perfiles de usuarios con permisos estructurados y adaptables a cualquier vivienda, y que cubra las necesidades de todas las personas que tengan que intervenir en algún momento, sin que esto comprometa la seguridad del sistema.

- Se ha investigado y establecido unos requisitos de seguridad para realizar conexiones seguras al servidor principal del sistema de modo que las órdenes o consultas que se realicen desde dispositivos externos sean cifradas y seguras ante posibles ataques, así como proteger el sistema para que no responda a peticiones desconocidas y evitar la filtración de información.

- Para el control de la vivienda, se han diseñado las interfaces gráficas para la interacción del usuario desde los distintos elementos de control posibles: la cerradura de la puerta principal, el panel o paneles principales de control, o la aplicación para dispositivos móviles para este fin.

Palabras clave: seguridad, usuario, domótica, autenticación, autorización, vivienda inteligente, vpn, firewall, perfiles, permisos, biometría, dispositivo móvil, conexiones seguras, internet de las cosas.

Abstract

In this document, you can find the degree final draft report where applications and security elements that an automated system should use to be able to authenticate users with a negligibe margin of error is described, and, at the same time, it should be easy and comfortable for people who are going to use it, be completely secure for possible attacks from outside or attemmpts to impersonate users.

During the development of the project it has been carried out the following:

- A detailed analysis of the methods of authentication and biometric technologies, compared between them to choose the most appropriate, combining it with other forms of authentication

- The definition of a hierarchy of user profiles with structured and adaptable to any housing permits, which meet the needs of all the people who have to intervene at any time, without compromising system security.

- It has been researched and established security requirements to carry out secure connections to the main server of the system so that orders or inquiries made from external devices are encrypted and secure against possible attacks and protect the system from responding to unknown requests and prevent data leakage.

- To control housing, graphical interfaces for user interaction from the various elements of possible control have been designed: front door lock, the main panel or panels control, or the mobile application for this ending.

Keywords: security, user, home automation, authentication, authorization, smart home, vpn, firewall, profiles, permissions, biometrics, mobile, secure connections, internet of things.

Tabla de contenidos

1 Introducción

El término Internet de las cosas hace referencia a la capacidad que poseen ciertos objetos, tales como smartphones, smartTVs, ordenadores, etcétera, que utilizamos de forma cotidiana, de conectarse entre ellos para ofrecernos nuevas funcionalidades o facilitarnos tareas al tiempo que mantenemos toda nuestra información sincronizada y siempre disponible.

En la sociedad actual, el Internet de las cosas está empezando a tomar relativa importancia en el día a día de la gente, propiciando la integración de la tecnología en la mayor parte de las tareas cotidianas y en todos los elementos con los que interaccionamos. El hogar es uno de los medios más importantes, pues en él pasamos una gran parte de nuestro tiempo, además de ser el lugar donde buscamos el descanso, guarecemos a los que queremos y nos acomodamos según nuestros gustos.

Las viviendas inteligentes están aún un poco lejos de ser algo común, pero ya empiezan a ser y acabarán siendo una realidad. No obstante, antes de que esto pueda llegar a suceder, hay algunos temas importantes que deben mejorarse como es la seguridad.

Con el crecimiento del internet de las cosas, también aumentan los ciberdelitos, aprovechando las vulnerabilidades en el ámbito de la seguridad que estos dispositivos inteligentes aún no han madurado lo suficiente.

Esto plantea un gran reto a la hora de aplicar estas novedades tecnológicas en nuestras viviendas, puesto que la seguridad debe ser muy alta, no dejando puertas traseras en nuestros hogares por culpa de un fallo en el desarrollo del software.

Por otra parte, necesitamos que las personas acepten y quieran disponer de estas nuevas tecnologías en sus hogares, por lo que para ello necesitaremos que su interacción con el sistema sea lo más natural y cómoda posible, para que no suponga un esfuerzo extra por su parte, ni un inconveniente, el disponer de un sistema domótico en su hogar.

Así pues, debemos asegurarnos de que las tareas sean, como mínimo, igual de rápidas y sencillas de llevar a cabo que de forma tradicional.

Para todo esto, hablaremos de los temas importantes a tratar de cara a la implementación de un sistema domótico seguro y fiable, empezando por los conceptos de autenticación y autorización. Mostraremos un estudio sobre los sistemas más seguros para garantizar la identidad de los usuarios junto con una jerarquía de permisos que impidan que cualquier usuario pueda alterar la funcionalidad del sistema.

También introduciremos una serie de herramientas para la seguridad en las conexiones desde cualquier dispositivo al servidor principal para evitar filtrados de datos, vulnerando así todo nuestro sistema.

Por otra parte, mostraremos cómo se interactúa con el sistema desde los distintos puntos posibles, adjuntando imágenes sobre el diseño de la interfaz gráfica y la explicación de su funcionalidad.

Y para finalizar, veremos un resumen de todo el sistema domótico aplicado a una casa, como ejemplo de vivienda domótica.

2 Autenticación

La autenticación es el acto o proceso para el establecimiento o confirmación de algo (o alguien) como real. La autenticación de un objeto puede significar la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad. Todo ello en función de uno o varios factores.

En nuestro caso, la autenticación se refiere a demostrar que la persona que intenta interactuar con el sistema es realmente quien dice ser, pasando posteriormente a permitirle la realización de aquellas acciones en las que tenga permisos.

2.1 Sistemas de autenticación

Con un sistema eficaz de autenticación resolveremos posibles intentos de intrusión en nuestro sistema domótico, dado que restringiremos el uso del mismo únicamente a los usuarios que conozcamos y estén reconocidos por nuestro servidor, con la menor probabilidad de fallo posible.

Hay distintos métodos de autenticación dependiendo de qué se utiliza para la verificación del usuario, dividiéndolos en 3 categorías.

- Sistemas basados en algo conocido:

Utilizan un elemento que conoce la persona a autenticarse, como puede ser, por ejemplo, una contraseña.

Este método es por lo general poco seguro, dado que con frecuencia, con saber algunos detalles acerca del usuario, podríamos dar con la contraseña y suplantar la identidad del auténtico mismo.

- Sistemas basados en algo poseído:

Se utiliza un elemento físico que posee el usuario para autenticarse. Sin ese elemento no se puede acceder, pero este sistema tampoco resulta seguro puesto que bastaría con sustraerlo del usuario para suplantar su identidad.

En estos casos no se garantiza acceso a un usuario sino al "portador de la llave".

Ejemplos de elementos utilizados son: una tarjeta de identidad o una tarjeta inteligente, dispositivos USB tipo e-pass token, que almacena un token de seguridad, tarjetas de coordenadas, smartcards o dongles criptográficos.

- Sistemas basados en una característica física del usuario o un acto involuntario del mismo:

Estos métodos son los más seguros para autenticar a un usuario, dado que muchos de estos se basan en unos elementos no escogidos por las personas, es decir, son únicos y los adquirimos al nacer. Aunque dependiendo de qué característica busquemos identificar, estos sistemas pueden ser más o menos seguros y/o sencillos de llevar a cabo.

2.2 Sistemas de autenticación biométricos

Tras haber explicado brevemente los sistemas de autenticación que existen, resulta obvio que lo más acertado en este caso sea decantarnos por las nuevas tecnologías en cuanto a lecturas biométricas se refieren.

A continuación, se presenta un breve estudio realizado sobre las más comunes, las más fáciles de utilizar y las que garantizan una inferior tasa de falsos positivos, es decir, aquellos casos en los que el sistema pudiera dar por válido a un usuario que realmente no es la persona a la que intentamos identificar.

2.2.1 Características biométricas medibles

Una característica biométrica es un elemento propio de cada persona que nos permite identificarla. Esta característica no solo se basa en elementos físicos de la persona, sino que también se puede referir a su comportamiento u otras aptitudes interiorizadas por la persona y que le caracterizan.

- Caligrafía:

Según estudios, la forma de escribir de las personas dice mucho acerca de cómo somos y qué tendencias tenemos subconscientemente. Por esto no es de extrañar que hayan lectores capaces de reconocer a las personas por esos pequeños detalles como alargar una letras, juntar otras, darle una inclinación hacia la derecha…

Pero este no es un método muy eficiente debido a que hay gente con la habilidad de copiar, con totalidad de detalles, la forma de escribir de cualquier otra persona.

- Reconocimiento de voz:

El detectar la voz de las personas para interactuar con sistemas es algo que hoy en día ya se utiliza mucho, sobretodo en dispositivos móviles. Pero resulta mucho más simple reconocer palabras que identificar a una persona por su registro de voz.

Aparte de ser poco seguro debido a que hay personas con registros muy similares, prácticamente idénticos, esta el problema de la alta variación del registro de voz en la misma persona.

No tenemos la misma voz recién despertados que cuando ya hemos "calentado" las cuerdas vocales, por no hablar de los posibles factores externos que pueden afectar en gran medida el habla de una persona, como la humedad del ambiente, la distorsión de las ondas sonoras por viento fuerte y otros elementos que afecten a las capacidades cognitivas como el alcohol.

- Reconocimiento facial:

A la hora de realizar un reconocimiento facial encontramos dos formas distintas de identificar a la persona:

· **Reconocimiento facial 2D:**

El reconocimiento 2D permite reconocer una cara en cualquier imagen plana, ya sea una foto impresa o sobre una pantalla. Este método puede ser fácilmente vulnerado, dado que con solo acercar una foto del usuario al dispositivo encargado del reconocimiento podremos suplantar su identidad.

· **Reconocimiento facial 3D:**

En este caso, se hace una captura de la profundidad de distintos puntos de la cara del usuario para formar un modelo 3D con mayor detalle y precisión, impidiendo de este modo que una simple foto pueda pasar como válida. Pero, aunque con el uso de un busto del usuario pudiera lograr identificarse como tal, el problema es la complejidad para realizar la captura de los datos biométricos y su posterior comparación, siendo demasiado lento para nuestro sistema.

- Lectura de la huella dactilar:

Este es sin duda la característica más utilizada para cualquier sistema actual de seguridad para identificar a un usuario. Además cuenta con una gran aceptación entre la sociedad y no resulta nada extraño a los usuarios el funcionamiento de esta tecnología.

Pero a pesar de todo, tiene sus contras, como por ejemplo que algunos factores externos pueden hacer muy compleja la identificación y, por tanto, menos efectivo el sistema. La suciedad, por ejemplo, que acumula el trabajador de un taller durante su jornada manipulando grasas y aceites de motor, podría impedirle entrar en su casa al darse el caso de que algún residuo en sus dedos no le permitiera identificarlo.

- Geometría de la mano:

Otra de las tecnologías más utilizadas, aunque con menos conocimiento por parte de la sociedad en general. La geometría de la mano se basa en tomar en detalle la distancia entre ciertos puntos concretos y su posición, para obtener un modelo lo más distintivo posible del usuario. Aunque poco probable, hay personas con geometrías bastante similares, y esto vulnera la seguridad de este tipo de reconocimientos.

- Lectura del iris:

Esta es sin duda, una de las mejores características a tener en cuenta para un sistema de seguridad mediante reconocimiento biométrico. La lectura del iris, aunque no está muy extendida entre la sociedad, es muy precisa y no requiere contacto con ningún dispositivo. Los iris de las personas son únicos, imposibles de falsificar, y prácticamente inalterables a lo largo de la vida de un individuo, lo que lo convierte en una característica altamente fiable.

Ante posibles problemas, como el reconocimiento en espacios poco iluminados, ya se han desarrollado lectores que permiten un buen funcionamiento con poca luz con una alta precisión, además de que existen cámaras que detectan la posición de los ojos y pueden realizar una lectura del iris desde una cierta distancia.

- Escáner de retina:

El escáner de retina ofrece un nivel de seguridad altísimo, pero con un gran inconveniente: es costoso de realizar y muy molesto para la persona que tenga que hacerlo.

Los usuarios de nuestro sistema deberían poder acceder a sus casas sin molestias ni malestares, y este sistema, aunque seguro, no es para nada agradable de usar, así que queda descartado por su complejidad a la hora de obtener un modelo a comparar y su incomodidad para llevar a cabo el escaneo.

- Lectura térmica:

Según varios estudios, la temperatura corporal de las personas dicen mucho acerca de quienes somos, pero esta se puede ver alterada por muchísimos factores, lo que la vuelve imprecisa y por lo tanto inválida.

- Lectura vascular de la mano:

El formato de las venas de la mano es único en cada persona, inalterable con el paso del tiempo, y garantiza con total seguridad la identificación del usuario.

La lectura vascular de la mano es la opción más apropiada para nuestro sistema por su facilidad de uso y su alto grado de seguridad. Además no puede verse afectada por ningún factor externo ni por enfermedades.

Se utilizan haces de luz del espectro infrarrojo, ya que debido a la composición sanguínea ferrosa, la hemoglobina presente en las venas y los capilares de la capa subcutánea absorbe más espectro infrarrojo que los tejidos musculares del cuerpo, permitiendo la obtención de un modelo vascular claro y preciso, sin la necesidad de estar en contacto con ningún dispositivo.

Además, no puede ser falsificable porque no se puede generar ningún modelo similar debido a la necesidad de que el usuario ha de estar vivo y tener, literalmente, sangre corriendo por sus venas, sin contar con que nadie sabe cuál es la distribución de todas las venas y capilares dentro de su mano.

Según estudios realizados, y pruebas de seguridad, la probabilidad de un falso negativo (no reconocer correctamente al usuario) es del 0,01%, mientras que la probabilidad de un falso positivo (reconocer a otra persona como al usuario) es del 0,00001%, prácticamente despreciable y cada vez menor debido a los avances en cuanto a la precisión de estas lecturas.

2.2.2 Factores para la comparación de características biométricas

Existen varios factores a tener en cuenta a la hora de medir la eficacia de una característica biométrica para el sistema de autenticación que deseamos implementar en el servidor de una vivienda domótica.

- Universalidad:

Nos referimos a este factor como la probabilidad de que una persona cualquiera posea esta característica biométrica, sin importar raza, sexo o edad.

Para nuestro caso, y dado que queremos que sea un sistema que pueda usar la mayor cantidad posible de usuarios, necesitaremos que este factor sea alto.

- Unicidad:

La característica debe ser, en la medida de lo posible, única en cada persona, siendo altamente improbable que existan personas que compartan esta característica pudiendo resultar en un falso positivo al identificar la una como la otra ante una lectura biométrica.

Este factor influye directamente en el nivel de seguridad que tendrá nuestro sistema, siendo más seguro cuanto más alta sea esta propiedad.

- Persistencia:

Nos referimos con este factor a la durabilidad que la característica tiene en una persona a lo largo de su vida, entendiendo como tal, si va a variar o no dependiendo de factores externos. Por ejemplo, la voz en las personas depende de muchos factores externos y del estado de salud de la persona. A mayor persistencia de la característica, menor será la probabilidad de fallar al tratar de identificar al usuario correcto.

- Cuantitativa:

La característica biométrica debe poder medirse con unos valores para poderse comparar con los datos almacenados y así identificar al usuario tras la lectura.

Principalmente nos centraremos en si un sistema informatizado puede leer y comparar estas características y con qué facilidad obtiene los datos.

- Eficiencia:

Entendemos en nuestro caso que la eficiencia se basa en la velocidad de lectura y la rapidez en la que es capaz de reconocer correctamente al usuario.

Para mayor comodidad de uso del sistema, esperamos que responda rápido, con el fin de brindar al usuario un método de autenticación más sencillo y rápido que el método tradicional basado en el uso de una llave física.

- Aceptabilidad:

Vivimos en una sociedad en la que las nuevas tecnologías se acogen muy poco a poco y con cierto recelo, por lo que con este factor mediremos el grado de conocimiento y la aceptación que la gente hacia el uso de la característica para su propia identificación.

Este no es un factor extremadamente relevante, dado que esperamos que, tarde o temprano, la gente termina aceptando las nuevas tecnologías, y el objetivo de nuestro proyecto no es ofrecer un negocio redondo, si no una forma cómoda y segura de llevar un control sobre nuestros hogares.

Aún así, esperamos que sea aceptado para que la gente no se vuelva reacia a utilizarlo.

- Vulnerabilidad:

Este sí que es un factor altamente importante, pues si lo que buscamos proteger es el acceso a nuestras viviendas, no podemos permitir que cualquiera pueda hacerlo. Con este valor mediremos si una característica biométrica es fácilmente falsificable, siendo más segura cuanto menos vulnerable sea.

Una vez conocidas la principales características biométricas con las que podemos interactuar con la tecnología actual, y cuáles son los factores relevantes para evaluar si son aptas o no para un sistema en concreto, podemos ver cual es el resultado en una comparación.

De este modo, podemos escoger la que más nos interese para nuestro sistema, argumentando apropiadamente el porqué.

En la siguiente tabla podemos observar a simple vista gracias a la leyenda de colores intuitiva, cuáles son los puntos fuertes de cada característica biométrica y en que aspectos falla, atendiendo para ello cada uno de los factores para la comparación de estas.

	Universal	Unicidad	Persistencia	Cuantitativa	Eficiencia	Aceptabilidad	Vulnerabilidad
Caligrafía	bajo	muy bajo	bajo	medio	muy bajo	muy alto	muy alto
Voz	medio	bajo	muy bajo	medio	bajo	muy alto	alto
Facial 2D	alto	bajo	medio	alto	medio	muy alto	muy alto
Facial 3D	alto	medio	medio	alto	medio	muy alto	medio
Huella dactilar	medio	alto	alto	medio	alto	alto	medio
Geometría de la mano	medio	medio	medio	alto	alto	medio	medio
Iris	alto	alto	muy alto	alto	muy alto	bajo	bajo
Retina	alto	muy alto	muy alto	bajo	alto	muy bajo	muy bajo
Térmica	alto	medio	bajo	medio	medio	bajo	medio
Vascular	alto	muy alto	muy alto	alto	muy alto	alto	muy bajo

Tabla 1: Resumen de la comparación entre las distintas tecnologías biométricas según los factores descritos y atendiendo a la necesidad sobre el sistema.

2.2.3 Autenticación biométrica frente a técnicas tradicionales

Las tecnologías biométricas han surgido como una alternativa y/o complemento a las técnicas de autenticación ya existentes.

Es por esto por lo que resulta posible establecer una comparación directa entre ambas técnicas, aprovechando para destacar los beneficios que resultan del uso del reconocimiento biométrico frente a las técnicas tradicionales, considerando para ello diversos aspectos.

- Secretismo:

Las contraseñas han de memorizarse y evitar que nadie las descubra, y las tarjetas identificativas deben estar a buen recaudo fuera del alcance de terceros.

Sin embargo, con los sistemas de autenticación biométrica el usuario no tiene que preocuparse de que ninguno de estos posibles descuidos pongan en peligro la seguridad de su hogar, sin tener que tomar medidas de protección que dependan exclusivamente de él.

- Posibilidad de robo:

Las tarjetas de identificación y contraseñas pueden ser robadas o descubiertas con mayor o menor facilidad por parte de un tercero, lo que nos hace bastante vulnerables y nos obliga a vigilar mucho nuestros movimientos.

Por contra, robar a una persona uno de sus rasgos biométricos, como hemos visto en el apartado anterior, es extremadamente complejo o incluso imposible, dependiendo de cuál sea.

- Posibilidad de pérdida:

Las contraseñas se pueden olvidar con mayor facilidad actualmente debido a que todos solemos memorizar más de una distinta, y las tarjetas identificativas se pueden perder u olvidar accidentalmente en algún sitio accesible a otras personas.

Los rasgos biométricos permanecen invariables salvo en contadas excepciones y siempre están con el sujeto a quien identifican, sin posibilidad de olvidarse, perderlos o alterarlos accidentalmente.

- Registro inicial y regeneración:

La facilidad con la que se puede generar y enviar una contraseña nueva o obtener una nueva tarjeta de identificación supera con creces la complejidad que supone registrar en un sistema los datos de un rasgo biométrico, ya que requiere de la presencia física del usuario y su plena colaboración.

Hay que señalar que los rasgos biométricos son por definición limitados dado que no hay más que los que tenemos, mientras que la generación de contraseñas es ilimitada, lo cual es una ventaja para las contraseñas.

- Proceso de comparación:

La comparación de dos contraseñas es un proceso rápido y sencillo, al igual que con la identificación de una tarjeta.

Sin embargo, comparar dos rasgos biométricos requiere de mayor capacidad computacional debido a la complejidad de adquirir, procesar y comparar sus datos.

- Comodidad para el usuario:

El usuario ha de memorizar una o múltiples contraseñas, y en el caso de que use una tarjeta de identificación, debe llevarla siempre consigo a todas partes.

Utilizando tecnología biométrica no se necesita hacer ninguno de estos esfuerzos, no podemos dejar de llevar nuestra identidad en nosotros mismos.

- Vulnerabilidad ante el espionaje:

Una discreta vigilancia de nuestra actividad diaria podría servir para obtener nuestra contraseña, o información que facilite su descubrimiento, o robar nuestra tarjeta en momentos puntuales cuando la dejemos desprotegida.

Estos métodos no resultan válidos ante los rasgos biométricos al no poderse robar ni falsificar.

- Vulnerabilidad a un ataque por fuerza bruta:

Las contraseñas tienen una longitud de varios caracteres que dificultan su obtención por fuerza bruta cuanto más largas y con mayor variedad de caracteres contengan. Por su parte, una muestra biométrica emplea cientos de bytes, lo que complica muchísimo los ataques de este tipo.

- Medidas de prevención de ataques:

Los ataques contra sistemas protegidos por contraseña o tarjeta se producen desde hace años porque estos sistemas llevan usándose muchísimo tiempo, y las medidas de prevención contra ellos han ido madurando con el paso del tiempo, tras cada nuevo tipo de ataque recibido, puliendo los posibles agujeros de seguridad.

Por el contrario, los sistemas biométricos son una tecnología mucho más reciente, implicando con ello un historial de ataques reducido. Al ser menos los ataques recibidos, aun no se han perfeccionado del todo los posibles agujeros de seguridad, aunque estos sistemas ofrecen ya de por si una gran seguridad ante ataques.

- Autenticación real del usuario:

La autenticación de los usuarios mediante el uso de una contraseña o tarjeta y su efectividad a la hora de identificarles a ellos mismos, dependen absolutamente de la voluntad del propio usuario a la hora de hacerlas personales e intransferibles, por lo que si así lo quisiera el propietario de las mismas, cualquier otra persona podría identificarse como si del propio usuario se tratase con algo tan sencillo como dejarle la tarjeta o decirle la contraseña. A parte, el hecho de compartir su elemento identificativo, vulneraría de sobremanera la seguridad del sistema.

La característica biométrica está completamente relacionada con el propio usuario puesto que no puede ser prestada ni trasferida por mucho que se desee.

- Coste de implantación:

En el momento de la implantación, el hecho de instaurar un sistema de contraseñas tiene un coste relativamente muy bajo debido a su baja complejidad y su madurez en el mercado.

En cambio, en el caso de implantar un sistema de autenticación basado en muestras biométricas, el coste y la complejidad son superiores y requieren de un sistema más potente que garantice un correcto funcionamiento con un tiempo de respuesta aceptable según las necesidades de los usuarios.

- Coste de mantenimiento:

Aunque parezca un poco contradictorio, el coste de mantenimiento de un sistema de autenticación biométrico, una vez implantado satisfactoriamente, es menor al de un sistema basado en el uso de contraseñas o tarjetas identificativas, ya que no conlleva gastos de gestión asociados a la pérdida u olvido de credenciales.

Aspecto	Biometría	Contraseñas o Tarjetas
Secretismo		
Posibilidad de robo		
Posibilidad de pérdida		
Registro inicial y regeneración		
Proceso de comparación		
Comodidad para el usuario		
Vulnerabilidad espionaje		
Vulnerabilidad fuerza bruta		
Medidas de prevención de ataques		
Autenticación real del usuario		
Coste de implantación		
Coste de mantenimiento		

Tabla 2: Comparación entre los métodos de autenticación según los parámetros anteriormente definidos

Cabe añadir que, a pesar de los múltiples beneficios del uso de la biometría, la sociedad aún es bastante reacia por miedo a la posible violencia que pueda conllevar un ataque para robar tu identidad ante un sistema que requiera a la persona o parte de ella para acceder.

Con el fin de tranquilizar estos pensamientos, dejar claro que un hurto conlleva legalmente un tipo de pena mucho menor que las que pudieran ocasionar los hurtos con agresión para obtener la colaboración del usuario, por lo que este tipo de ataques serían más infrecuentes en la sociedad.

Por último, en nuestro sistema nos hemos decantado por un método más seguro y bastante habitual hoy en día, que se trata de combinar las tecnologías de reconocimiento biométrico con algunos elementos físicos que contengan información sobre el usuario que se ha de identificar, aumentando de forma considerable la seguridad del sistema.

Este uso combinado tiene sus pros y sus contras, pues es más incómodo llevar siempre encima una tarjeta identificativa, pero a la vez nos va a permitir que la autenticación biométrica que ha de llevar a cabo el sistema sea más rápida y requiera menor capacidad de cómputo.

Además, en un futuro se podrían utilizar estas tarjetas para un uso más extenso en los elementos con los que interactuamos a diario, facilitando una centralización de las identificaciones de cada componente al que tengamos que acceder.

3 Autorización

La autorización es una parte del sistema que se encarga de proteger y evitar que los usuarios, identificados o no, puedan acceder a ciertos datos o ejecutar determinadas acciones.

Cabe pues destacar la diferencia entre autorización y autenticación, explicada en el apartado anterior, pues en ocasiones estos conceptos se confunden.

La autorización hace referencia a qué acciones puede ejecutar o a qué datos puede acceder un usuario que ha verificado su identidad, es decir, que se ha autenticado.

La autorización se puede aplicar por cada elemento individual o para grupos de elementos, entendiendo en nuestro caso de la vivienda inteligente, que cada elemento sería la ejecución de una acción.

Lo más apropiado para un sistema con tantas posibles acciones y con nuevas posibilidades con el paso del tiempo es, sin duda, la gestión de grupos de permisos y la elaboración de perfiles de usuarios.

3.1 Niveles de seguridad

Para establecer unos niveles de seguridad en nuestro sistema lo primero que haremos será establecer una serie de criterios en los que basar nuestras decisiones sobre en qué nivel han de estar qué acciones.

La criticidad es el factor que emplearemos para delimitar los distintos niveles, basándonos en la relevancia que puedan tener las acciones a realizar sobre dos elementos clave: la vivienda y los datos de los usuarios.

Dado que lo que se pretende con una casa domótica es que sea más sencilla para el usuario y a la vez mucho más segura que una vivienda tradicional, es obvio que no vamos a dejar que cualquiera pueda realizar acciones que pongan en riesgo esa seguridad que tanto deseamos.

Por otra parte, no todos los usuarios son conscientes de lo que implican ciertas acciones puesto que el sistema puede ser y será utilizado también por los más pequeños de la casa o incluso por invitados.

- Nivel bajo o libre:

Cualquier persona podrá realizar estas acciones debido a su baja repercusión en el entorno domótico. Aquí se incluyen las acciones más elementales como puede ser encender la luz en una habitación.

Estas serán además las únicas acciones que pueda realizar una persona no autenticada ni identificada en la casa. Este tipo de usuarios se les conoce como invitados o anónimos, por su no pertenencia al grupo identificado de usuarios del sistema.

Por otra parte, estos serán los permisos que todo usuario del sistema tendrá por defecto, a excepción de aquellos casos en los que se bloquee el uso del sistema a usuarios sin identificación.

- Nivel medio o selectivo:

Se restringirá el uso de estas acciones a los usuarios identificados de la vivienda, de forma que las personas que no formen parte del hogar, o no sean previamente autorizados, no podrán realizar este tipo de acciones.

Esto es importante para evitar que una persona ajena a nuestra familia pueda, por ejemplo, realizar cambiarnos en la climatización del hogar. Debemos ser permisivos con las visitas y hacer que se sientan confortables, pero hay unos límites que podemos evitar gracias a esta diferencia del nivel de seguridad.

Así dependerá únicamente de los anfitriones el acomodar el ambiente o solicitar a la casa que realice determinadas tareas.

- Nivel alto o restrictivo:

Existen determinadas acciones que no deberían ser realizadas por ningún usuario con ciertas limitaciones en sus capacidades o conocimientos, como sería el caso de un niño pequeño, que por su seguridad habrá acciones que no podrá realizar.

Esto no es una barrera para usuarios discapacitados, nada más lejos de la realidad. Esto es un mecanismo de seguridad para evitar accidentes domésticos como por ejemplo que los niños no puedan encender la cocina, ni abrir las ventanas.

Hay que tener en cuenta que las personas discapacitadas tendrán un mayor control de la casa mediante un sistema domótico que en una casa tradicional, pues dependiendo de sus limitaciones, el sistema se puede adaptar para facilitarle el manejo y acomodarse a sus necesidades.

- Nivel crítico o restringido:

En este nivel se incluyen acciones muy delicadas que puedan poner en riesgo la seguridad o la integridad de la vivienda, como pueda ser la gestión de los usuarios y sus permisos.

El hecho de añadir a un nuevo usuario o de cambiar sus permisos puede afectar seriamente la seguridad, pues estamos confiando en que estos usuarios son aptos para un mayor control de la casa.

Además, también podemos añadir permisos de acceso temporal a la casa, de forma que un usuario pueda abrir la puerta según como el propietario estipule. Este podría ser el caso de una persona que tenga que estar al cuidado de la casa durante unas vacaciones de los propietarios, dándole durante ese periodo de tiempo, autoridad para acceder a la vivienda y realizar un mayor número de acciones.

3.2 Perfiles de usuarios

Una de las opciones más utilizada en los sistemas de seguridad es la asignación y elaboración de perfiles de seguridad para los usuarios.

Cuando un nuevo usuario se añade al sistema, debemos asignarle unos permisos y almacenar sus datos para su identificación.

Si tuviéramos que darle permisos individuales a cada elemento interaccionable de la vivienda sería un trabajo extremadamente tedioso.

Para ello daremos la opción de generar un nuevo usuario a partir de una plantilla o de unos perfiles predeterminados, donde se establecerán diferentes permisos de forma predeterminada y acceso autorizado a según que niveles o elementos de la casa.

Además, no solo existirán los perfiles que se propondrán a continuación, al usuario se le permitirá crear nuevos perfiles y almacenarlos para futuros usos.

- Infantil:

A los niños hay que vigilarlos constantemente para que no hagan cosas que puedan resultar peligrosas para ellos o para la seguridad del hogar, puesto que no tienen percepción del peligro que pueda suponer por ejemplo asomarse a una ventana abierta, encender una chimenea, o abrir la puerta principal a un extraño.

Con un sistema domótico y un perfil apropiado esto puede solucionarse sin tener que estar constantemente detrás de ellos vigilándolos.

Con el perfil infantil dejaremos que disfruten de todos los permisos que puedan tener los padres, exceptuando aquellos que permitan realizar acciones que puedan resultar peligrosas para ellos, como impedir que puedan abrir una ventana, activar algunos electrodomésticos, o incluso por motivos de privacidad, acceder a determinadas habitaciones sin la presencia de un padre o responsable.

Este perfil es el que más variaciones puede presentar, debido a que, según los niños vayan madurando, podrán llevar a cabo más acciones en la casa, por lo que los padres eliminarán determinadas restricciones cuando lo consideren oportuno, lo cual también transmite al niño el concepto de responsabilidad.

- Temporal:

Resulta útil tener alguien disponible para echarnos un ojo a la casa en el momento en que nos sea imposible a nosotros, como sería el caso de un viaje de vacaciones. Confiamos en estas personas y deseamos que puedan acceder a la casa y tener unos permisos superiores a un simple invitado.

Además, con este perfil se puede limitar el uso de la vivienda a un tiempo determinado o a un horario concreto, facilitando así el acceso a la vez que nos evitamos tener que estar pendientes de habilitar el usuario cada día o cada ciertas horas.

Aun así, a este tipo de usuario no se le permitirá cambiar los modos de comportamiento del sistema, que veremos posteriormente.

- Residente:

Una persona adulta que viva en la casa, un hijo que se ha independizado pero aún vuelve a casa, algún familiar cercano… Todos estos posibles usuarios deberán ser capaces de ejecutar todas las acciones que permita la vivienda, pues son responsables y de un nivel de confianza muy elevado.

A diferencia del perfil temporal, estos usuarios no tienen un horario restringido ni un tiempo limitado para realizar acciones en la casa, además de poder cambiar los modos del sistema.

Solo tienen una limitación los miembros con este perfil: no pueden gestionar los usuarios del sistema debido a su directa repercusión en los permisos de estos en el sistema.

- Administrador:

En todos los sistemas, sean del tipo que sean, hay siempre un limitado número de usuarios que pueden tener el control total del sistema, y este no es una excepción. Los usuarios con perfil de administrador podrán ejecutar todo tipo de acciones, pero sobretodo, y lo más importante, serán los únicos con autorización para gestionar los usuarios y sus permisos.

- Invitado:

Si en algún momento vamos a compartir la vivienda con una visita que se va a quedar un tiempo limitado, habrá que darle permisos para realizar prácticamente las mismas acciones que un residente, como si fuera un residente temporal.

Con este perfil cubriríamos los mismos permisos que un residente, pero con una fecha de caducidad, para que cuando termine su estancia en nuestra casa vuelva a ser como cualquier otro visitante en la vivienda.

3.3 Modos de comportamiento del sistema

Con los perfiles de usuarios hemos visto como se puede facilitar la gestión de permisos a la hora de crear un nuevo usuario o de modificar las autorizaciones de otro.

Pero aun así, puede haber momentos en los que se quiera que el sistema sea más flexible o más restrictivo. En estos casos, tener que cambiar uno a uno los permisos de los usuarios para más tarde volver a cambiarlos puede llegar a ser un trabajo insufrible que llevar a cabo.

En nuestro sistema domótico proponemos una serie de estados del sistema, o modos de uso, según lo requiera la situación.

- Modo normal:

El sistema funciona acorde con lo estipulado en los perfiles y los permisos tal y como los tienen asignados.

Es el modo más apropiado a lo largo del día, pues los accesos a la casa seguirán siendo seguros sea cual sea el modo que este activo, y de esta forma tendrán acceso solo los usuarios con acceso autorizado.

- Modo visitas:

Como usuarios residentes, podremos activar este modo para ser más flexibles en caso de tener que recibir visitas, habilitando de este modo que usuarios no identificados puedan realizar determinadas tareas o acciones que no impliquen ninguna alteración del bienestar del hogar.

Algunas restricciones, como impedir que el nivel de volumen de la televisión sea muy elevado, dificultando la conversación entre las persona, se pueden activar en este modo.

- Modo nocturno:

Llega la noche, y al irnos a dormir no vamos a permitir que nadie ajeno a la familia pueda acceder a la casa.

Con la activación de este modo, los usuarios con acceso a la casa que no sean miembros de la familia de la vivienda o tengan la autorización expresa pertinente, no podrán acceder a esta.

Además, se activarán ciertas medidas automáticas para el bienestar del hogar, como evitar que las persianas estén levantadas si hay más luz en el interior de la casa que fuera, con el fin de que no puedan vernos desde casas vecinas, preservando nuestra privacidad.

- Modo seguridad:

Si por algún casual o debido a una necesidad tenemos que ausentarnos de la casa y dejar solos durante un breve periodo de tiempo a nuestros hijos, podremos estar tranquilos activando este modo, pues con él impediremos la ejecución de una gran cantidad de acciones y limitaremos el acceso a la vivienda como si del modo nocturno se tratase.

En algunas viviendas de uso temporal, este sería el modo perfecto a dejar activado al regresar de esas vacaciones que hemos disfrutado en esa casa, pudiendo configurar un cierre más severo del acceso a la vivienda.

Con esta serie de modos, que además podemos automatizar para su cambio automático, brindaremos un manejo más cómodo de la vivienda para que, en cada momento, las personas apropiadas a la situación no se sientan incapaces de realizar ninguna tarea sin solicitarlo a un usuario con más permisos.

A la vez, también nos permite aumentar las restricciones en momentos de necesidad para asegurar la integridad del sistema y, sobretodo, del hogar.

4 Seguridad en las comunicaciones

El servidor principal de nuestro sistema domótico estará ubicado en nuestra casa y toda interacción con él, a través de los paneles de control o de la cerradura de la puerta, tiene un cableado directo que impide que se puedan llevar a cabo ataques a través de Internet, puesto que no es necesario para ninguna interacción en estas conexiones.

El uso de unos dispositivos móviles para el control de la casa conlleva una mayor fragilidad en la seguridad del sistema, que hay que tener en cuenta.

Como estos se conectan al servidor a través de Internet, y en el momento de dar un punto de enlace a nuestro servidor con la gran malla mundial, tenemos que estar preparados ante cualquier ataque que pueda realizarse por ese pequeño agujero.

4.1 Conexión cifrada por OpenVPN

Las conexiones entre los dispositivos y el servidor domótico se han de proteger para impedir que cualquier persona lance órdenes o peticiones de manera que pueda alterar el estado del servidor de la casa.

El uso de una VPN puede ayudarnos con este problema, pues se trata de una tecnología de red que permite una conexión virtual segura de la LAN de nuestro sistema sobre la red pública o sobre Internet, garantizando que la transferencia de datos entre los dispositivos y el servidor sean confidenciales entre ambos.

Para esto se establece una conexión virtual punto a punto, y existen diversas soluciones para generarlas y cifrarlas. En nuestro caso nos decantaremos por el uso de OpenVPN, que se trata de una aplicación software open-source muy completa y utilizada en entornos que requieren un alto grado de seguridad.

OpenVPN nos ofrece 2 modos posibles de autenticación al establecer la conexión virtual: utilizando una clave estática previamente compartida por los extremos, o utilizando un protocolo SSL/TLS.

La ventaja de utilizar el modo de seguridad mediante claves pre-compartidas, frente al modo SSL/TLS, es su facilidad de configuración, ya que los participantes no necesitan manejar ningún certificado y no hace falta la intervención de una autoridad certificadora (CA).

Por el contrario, dichas claves han de estar a buen recaudo, por lo que este modo se considere menos seguro que utilizando el protocolo SSL/TLS y dado que en nuestro sistema buscamos la mayor seguridad posible, nos decantaremos por este último.

Las conexiones con SSL/TLS se llevan a cabo del siguiente modo:

Se establece una sesión SSL bidireccional para que ambos extremos presenten sus propios certificados con el fin de autenticarse, en nuestro caso se trata del dispositivo móvil utilizado hacia el servidor del sistema domótico.

Tras la autenticación de ambos, el servidor se encargará de generar las claves para cada extremos de forma aleatoria y de una duración limitada para la conexión entre ambos:

- Una clave para el cifrado de los mensajes que envíe.
- Una clave para el descifrado de los mensajes que recibe.
- Una clave HMAC para enviar paquetes y garantizar su identidad.
- Una clave HMAC para recibir paquetes con la certeza de conocer al remitente.

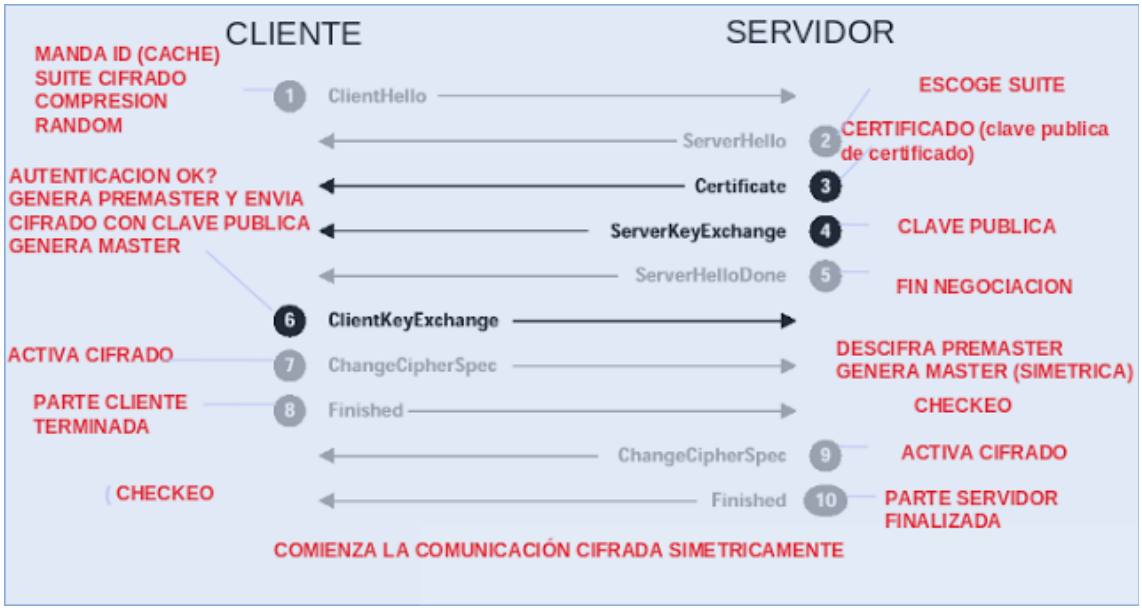

Ilustración 1: Diagrama de intercambio de información durante el proceso de Handshake.

Con las claves disponibles de ambos, se empieza la conexión donde, desde el dispositivo móvil, se cifrarán las ordenes a enviar al servidor con la clave generada para el cifrado de datos, y se cifrará el paquete en el que se enviará con la HMAC para que el servidor domótico pueda autenticarlo.

El servidor, al recibir el paquete y garantizar la identidad del cliente, utilizará su HMAC para la recepción que le permitirá sacar los datos cifrados del paquete y posteriormente, con la clave para el descifrado de datos, descifrar la petición realizada por el usuario al sistema domótico que, tras verificar los datos del usuario y sus permisos, cumplirá su petición si procede.

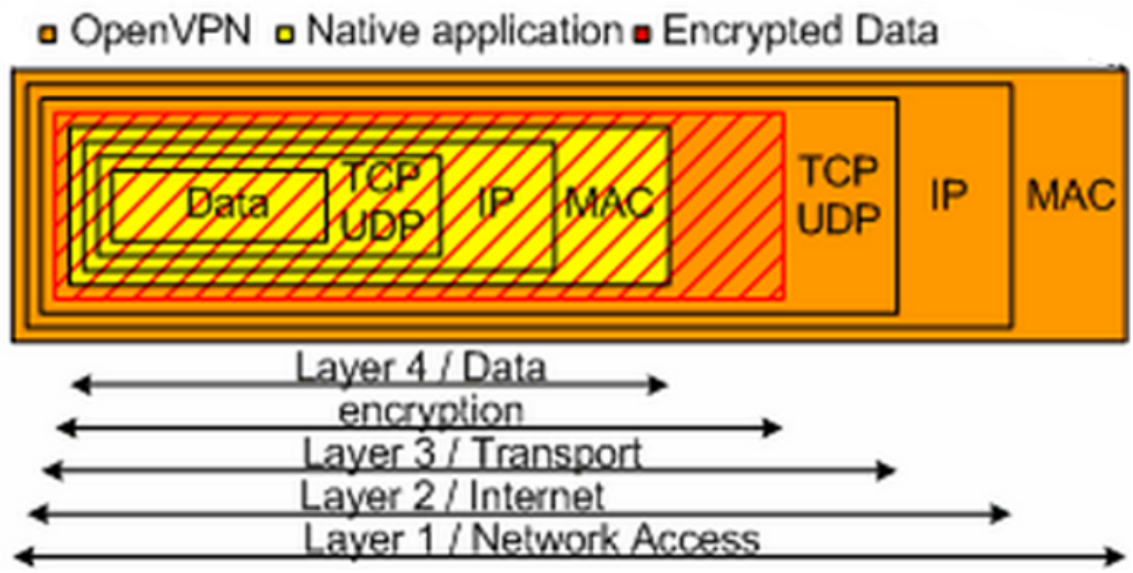

Ilustración 2: Capas de cifrados empleados en el envío de datos de un dispositivo al servidor a través de OpenVPN.

Pasado cierto tiempo, o por petición del usuario, la conexión se cerrará, requiriendo de nuevo la generación de un nuevo conjunto de contraseñas.

Con el fin de aumentar la seguridad, se utilizará una clave pre-compartida para generar un HMAC que autentique los paquetes que forman parte del protocolo de establecimiento Handshake del propio protocolo TLS, pues así se protege a la implementación de un posible desbordamiento de buffer por parte de un atacante, ya que este no podrá iniciar el Handshake de TLS al no haber generado paquetes con la HMAC que se utiliza en ese momento.

Por otra parte, podemos pensar que desde el interior de la casa no habrá ninguna complicación para conectarse al servidor y mandar las ordenes, pues estamos en la misma red local. Pero esto sería un error, pues los datos y paquetes que se envíen deben ir cifrados también. Imaginad por un instante que alguien consiguiera conectarse a nuestra red local wifi y emular la MAC de nuestro dispositivo: podría obtener toda la información que quisiera y realizar las acciones que deseara como si de nosotros mismos se tratara.

Así pues, todas las conexiones realizadas desde dispositivos móviles serán cifradas en todo momento, independientemente de desde donde estemos utilizándolo.

4.2 Control de comunicaciones mediante firewall

Los firewalls son una parte de un sistema diseñado para proteger las conexiones entrantes o salientes, bloqueando aquellas no autorizadas y garantizando aquellas debidamente autorizadas.

Se trata de un bloqueo de los puertos de entrada y de salida hacia el exterior de un servidor, dejando accesibles unos puertos concretos para el envío de datos desde el servidor o para la recepción del exterior, pudiendo añadir reglas para filtrar aún más que tipo de conexión se permitirá en cada puerto concreto y cuando aceptarlas.

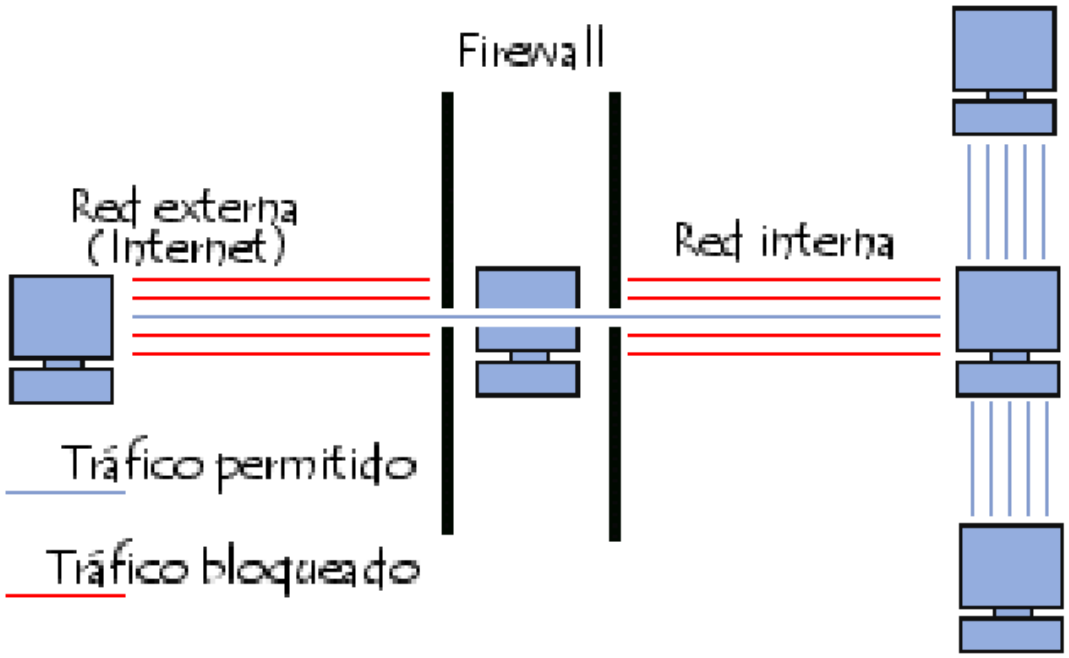

Ilustración 3: Esquema sobre el funcionamiento de un firewall

Los bloqueos y filtrados se pueden llevar a cabo de dos formas opuestas según la política que se desee implementar.

- Política permisiva:

Se permite todo el tráfico a excepción del que se limite de forma explicita. De este modo solo se bloquean conexiones de las que se tenga la certeza que son peligrosas o que vayan en contra del funcionamiento establecido para el servidor.

- Política restrictiva:

Al contrario que con la política permisiva, solo se permiten las conexiones que se haya definido de forma explícita, bloqueando todo tipo de comunicación no autorizada.

En nuestro caso, queremos aislar el servidor para que nada pueda interferir en el funcionamiento de nuestra vivienda inteligente, por lo que emplearemos una política restrictiva, dejando únicamente acceso a aquellas conexiones que tengamos la certeza de que son apropiadas.

4.3 PFSense

Es una de las soluciones software más completas y de código libre que podemos encontrar a la hora de proteger nuestros servidores.

Además de permitirnos una amplia variedad de reglas y opciones de configuración para el firewall, cuenta con el uso de OpenVPN para establecer una conexión virtual segura a través de él, dejando el puerto 1194 a la escucha de peticiones de los dispositivos que desean empezar un HandShake con nuestro servidor.

PFSense cuenta con una cómoda e intuitiva interfaz web para la configuración del mismo, que nos permite todo tipo de ajustes y la posibilidad de añadir nuevos módulos.

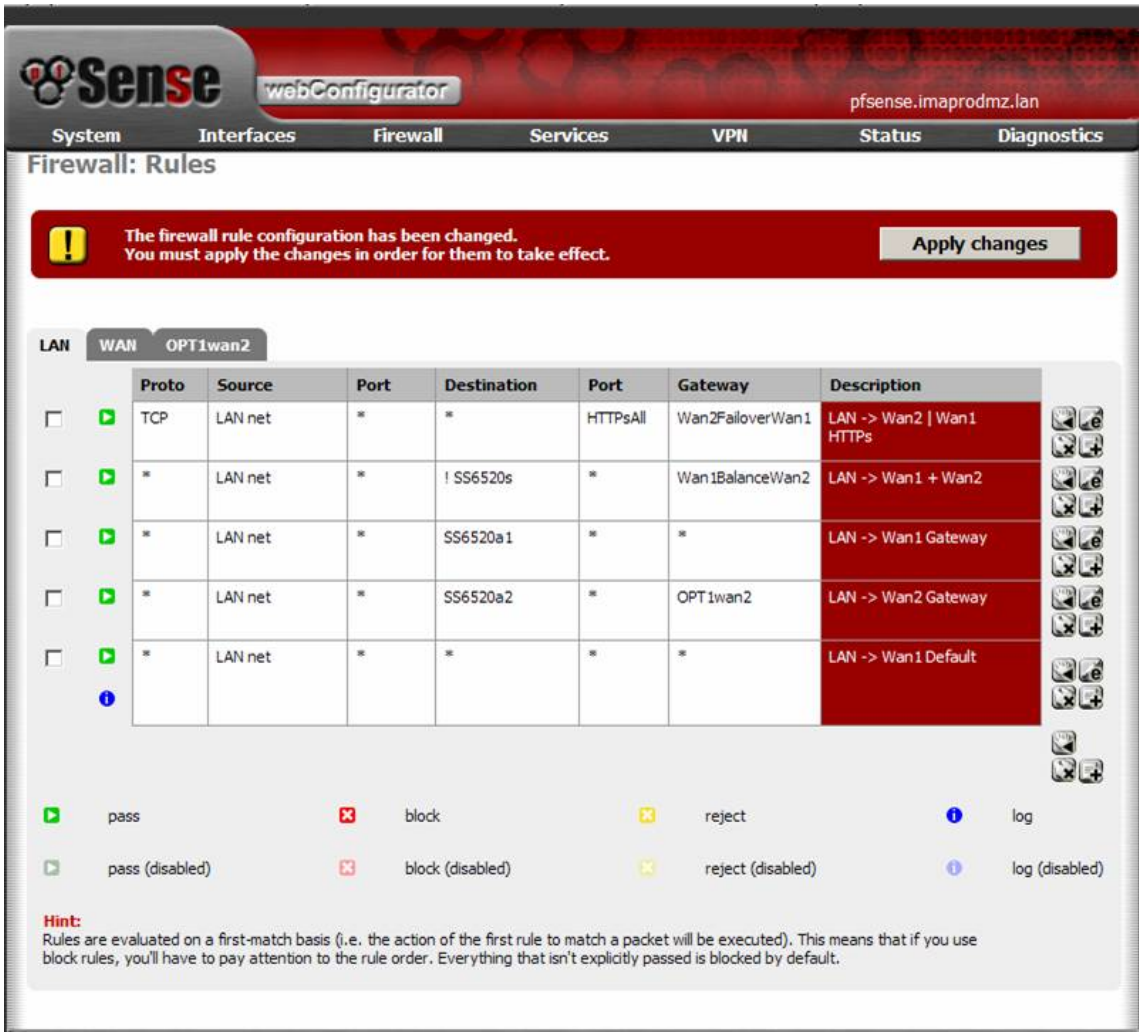

Ilustración 4: Ejemplo de interfaz web de PFSense para la gestión de reglas del firewall

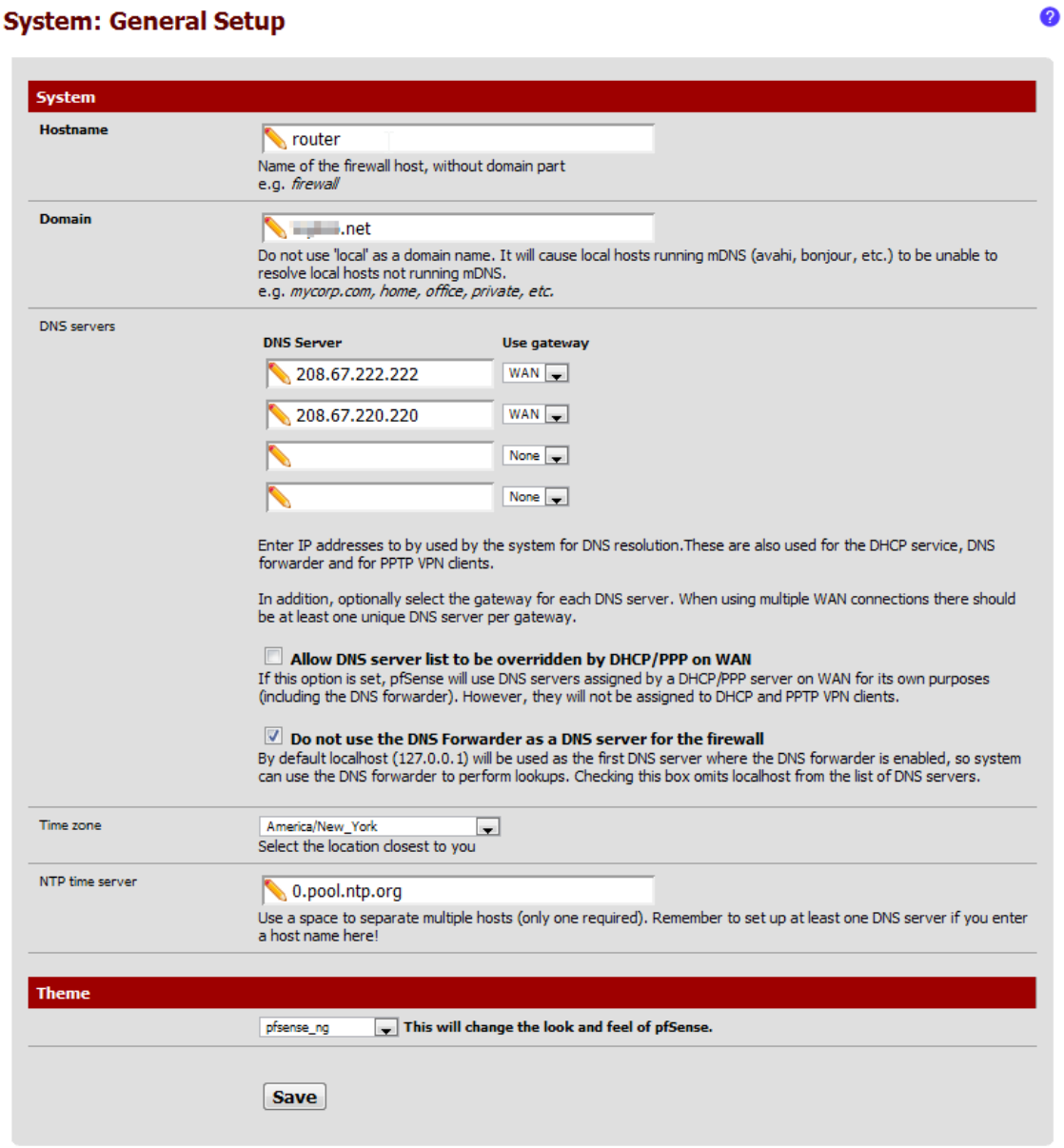

Ilustración 5: Página de configuración de PFSense

Por otra parte, si se desea implementar este sistema domótico en un edificio donde el servidor principal formara parte de la comunidad, fuese más potente y gestionara la seguridad de las viviendas particulares, donde además cada casa tuviera uno de menor potencia que compartiera las características de seguridad del principal, se podría mantener la configuración base del firewall del edificio sincronizada con la del resto de firewalls de cada vivienda concreta gracias al PFSync, que los mantiene sincronizados para que los cambios del principal se reflejen en todos y que no se vulnere la configuración de seguridad del principal desde uno particular.

Sin contar con las opciones que nos brinda para las conexiones OpenVPN, la implementación del firewall (que permite filtrados de IP, restricciones en la conexión, protocolos permitidos…), y la sincronización de varios servidores con la misma configuración, podemos encontrar estas otras funcionalidades que en algunos casos nos podrían ser de utilidad:

- Balanceo de cargas:

En el caso de implementar el sistema en un edificio, se puede utilizar el balanceo de cargas para garantizar a todos los vecinos un servicio óptimo de conectividad, asegurando en todo momento el acceso al servidor en caso de fallo de uno de los particulares.

- Tabla de estado:

Y para verificar que todos los elementos que formen parte de nuestro sistema se mantienen funcionando correctamente, tenemos esta funcionalidad que nos permite monitorizar el estado de los servidores y dispositivos conectados al sistema, informándonos de perdidas de sincronización, fallos de conexión o retrasos en las conexiones.

- Gestión de Autoridades Certificadoras:

PFSense nos permite gestionar nuestras propias CA, que nos facilitará la elaboración y control de las claves pre-compartidas que utilizaremos más adelante en la configuración de los dispositivos que se conectarán a través de OpenVPN.

-Sistema de notificaciones:

Entre sus funcionalidades básicas, podemos encontrar un servicio de notificaciones vía correo o SMTP para mantenernos informados del estado del servidor o de intentos de intrusión.

Por último, si somos novatos en el uso de estas soluciones software para la seguridad de servidores, siempre podemos optar por comprar uno de los componentes que ofrece la web oficial, junto con un servicio de configuración y soporte técnico durante 1 año o 2 incidencias del sistema.

5 Interacción de los usuarios con el sistema domótico

Con todos los conceptos claros y las diversas opciones para la elaboración de un sistema domótico seguro, procedemos a establecer el funcionamiento del nuestro.

Recordar, que facilitar al usuario el uso del mismo es una parte muy importante, además de tener en cuenta que lo que se pretende en una vivienda inteligente es que una vez dentro de la casa, las acciones se puedan ordenar desde dispositivos móviles del usuario.

Las diferentes formas de interactuar el usuario con la casa dependerán del nivel de criticidad de las acciones a realizar y de la ubicación del usuario.

Dispondremos de 3 plataformas distintas para la interacción con el sistema, siendo estas:

- Cerradura con lector biométrico y de tarjeta de identidad de la puerta de entrada, donde la seguridad debe ser máxima y la probabilidad de fallo prácticamente nula.
- El panel de control principal del sistema domótico, del cual dispondremos en la entrada de la casa, siendo posible añadir más en otras zonas de la vivienda a gusto del usuario.
- Uso de dispositivos móviles como smartphones o tablets, conectadas al sistema por VPN, utilizando para ello un protocolo TLS.

5.1 Cerradura con lector biométrico y de tarjetas de identidad

En la puerta de acceso a la casa sucederán las más críticas de todas las interacciones posibles con la vivienda, por lo que el dispositivo incluirá un lector vascular para autenticar al usuario, pero consideramos apropiado añadir también un lector de tarjetas identificativas.

Aunque puede resultar un poco menos cómodo, el uso combinado de la biometría con alguna técnica más tradicional, como las tarjetas identificativas, puede aumentar el nivel de seguridad junto con la velocidad de procesamiento, como hemos comentado anteriormente.

El usuario deberá en primer lugar introducir o acercar la tarjeta al lector, que identificará al usuario. A continuación, se procederá a la lectura vascular de la mano, que el sistema comparará con la del usuario para autenticarlo.

De este modo, al tener el usuario identificado previamente a la lectura biométrica, nos ahorramos tener que cotejar toda la base de datos en busca de unos datos biométricos que coincidan, y simplemente comparando con los asociados a ese usuario bastará.

Ilustración 6: Cerradura de la puerta principal de la vivienda con lector biométrico y de tarjetas identificativas.

El pequeño monitor que tiene a la parte inferior nos indicará cuando el acceso es correcto y cuando esta fallando la autenticación o autorización del usuario, notificando el problema que existe que impide al usuario entrar, ya sea por no reconocerlo o por no disponer de autorización para acceder.

5.2 Panel principal del sistema

En la casa habrá ubicado un panel con otro lector biométrico para la gestión de las tareas más críticas y que requieran un mayor nivel de autoridad, desde el cual también se podrán llevar a cabo todo tipo de tareas dependiendo del usuario tras su autenticación.

Por defecto, este panel nos permitirá de un simple vistazo ver el estado general de la vivienda, intercambiando entre las diferentes plantas que tenga, en el supuesto de que se trate de una casa en lugar de un piso.

Para ello dispondremos de un mapa de la planta, con indicadores básicos como qué luces están encendidas y cuáles no, la temperatura en cada sala, las puertas y/o ventanas que están abiertas, etc.

Obviamente, como no se ha identificado ningún usuario, no se podrá realizar ninguna modificación, a menos que esté habilitado el modo para invitados, donde veremos más adelante que sí podrán realizar cambios básicos sin demasiada importancia.

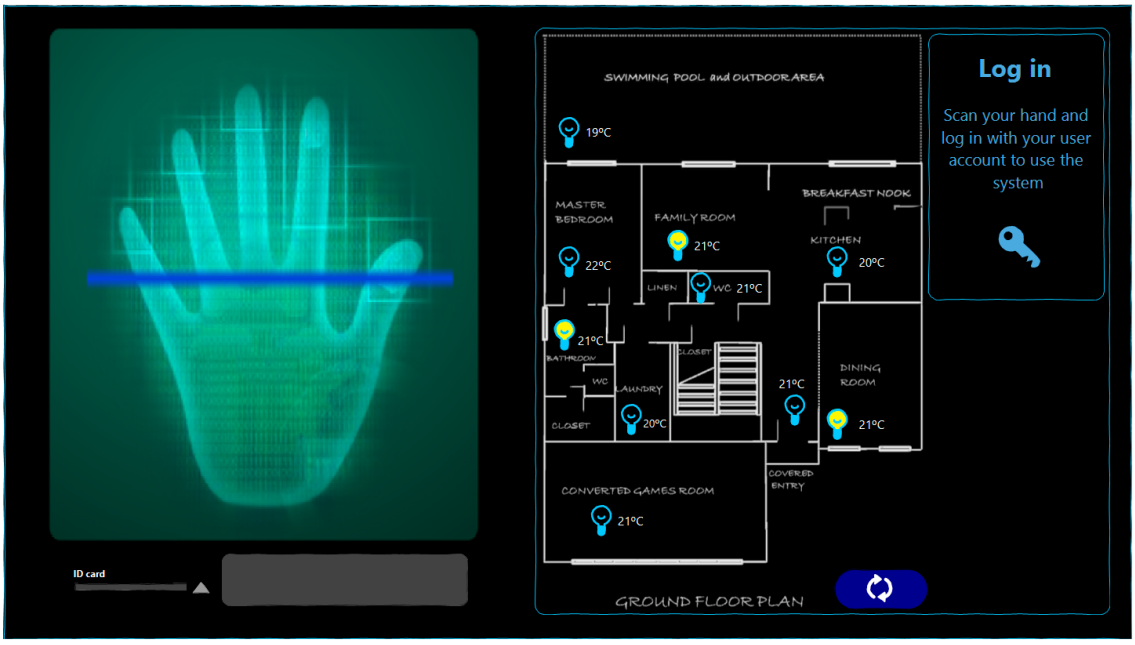

Ilustración 7: Panel principal con la interfaz por defecto, previa a la autenticación de un usuario.

Los usuarios podrán habilitar el panel para realizar todas las tareas que quieran, ya sea desde encender o apagar las luces de las diferentes habitaciones, hasta desplegar el gestor de usuarios y modificar permisos. Todo esto dependiendo de los permisos que tenga el usuario que lo ha habilitado.

La habilitación del panel se puede hacer simplemente pasando la mano por el escáner biométrico. Este detectará al usuario y mostrará aquellas opciones que por su perfil pueda realizar.

Además, al pulsar sobre las distintas habitaciones de la casa, esta se ampliará para poder mostrar acciones más concretas que se puedan realizar en esa sala.

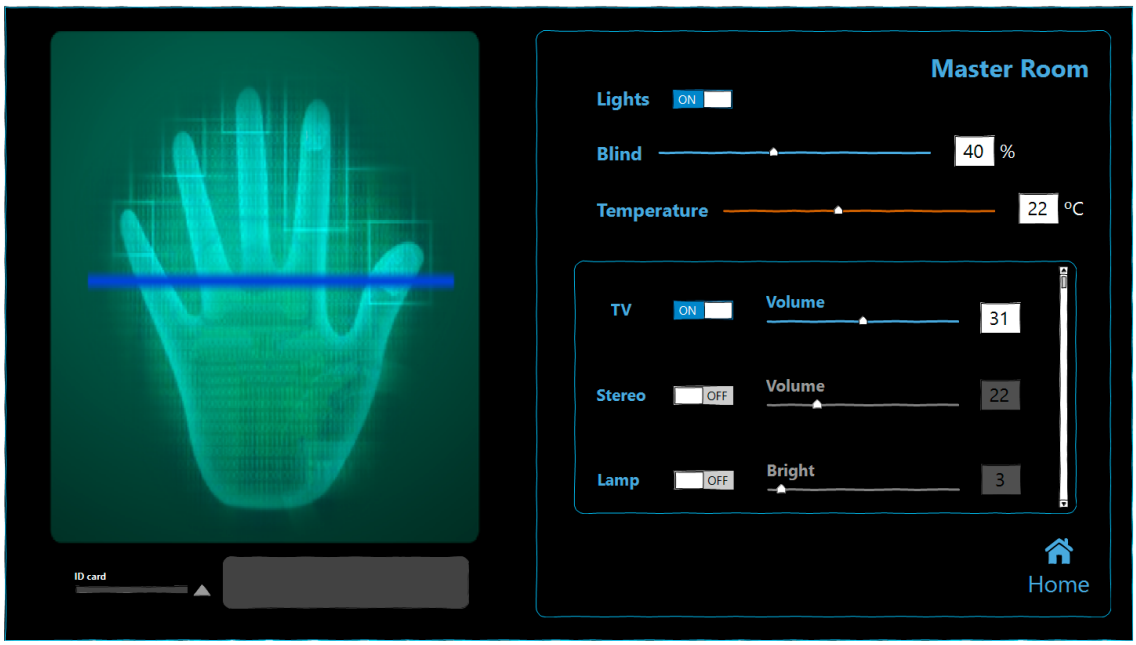

Ilustración 8: Ejemplo de interfaz mostrada al acceder a las acciones de una habitación o sala de la vivienda.

Por ejemplo, si pulsamos sobre la sala de estar, donde tenemos un *home cinema* con su sistema de sonido conectado, podemos seleccionarlo para gestionar el volumen, o si la luz es regulable, ajustar la intensidad de la misma.

Dependiendo de en que sala o habitación accedamos, las funciones irán cambiando, incluso habrá algunas donde solo determinados usuarios puedan realizar cambios en elementos concretos.

5.2.1 Habilitado por invitado, infantil o temporal

Tanto si la persona que intenta habilitar el panel principal es un niño, una persona con acceso temporal a la casa o un invitado que viene a pasar unos días con la familia, en ninguna caso podrán modificar nada del estado del sistema domótico ni de las cuentas de usuario, ni siquiera de las suyas propias.

En todo caso, al habilitar el panel principal uno de estos usuarios, se mostrará la información perteneciente a esta persona.

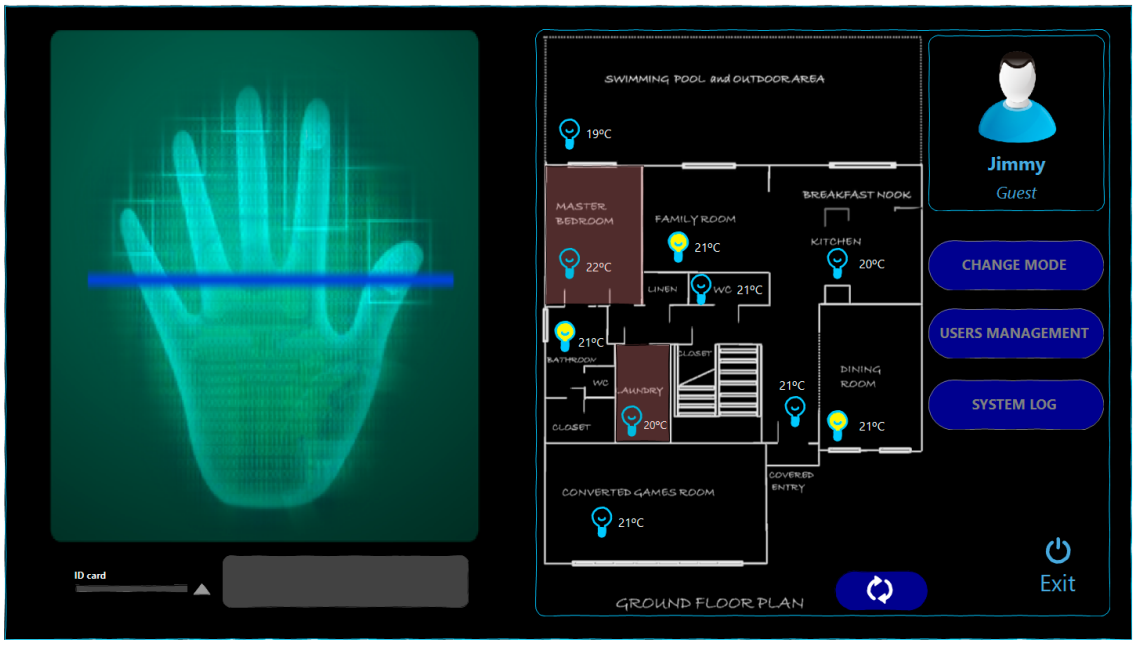

Ilustración 9: Apariencia de la interfaz cuando es habilitado por los usuarios con pocos permisos como los niños o los invitados.

Seguirá siendo posible realizar todas las órdenes y acciones que su perfil les permita ejecutar, aunque en algunas habitaciones de la casa no podrá realizar ningún tipo de modificación.

5.2.2 Habilitado por residente

Por ejemplo, si el hijo mayor, con un perfil de residente, habilita el panel, este mostrará las opciones de modificar el estado de los elementos visibles, de cambiar el modo de funcionamiento del sistema y editar los datos básicos de su cuenta de usuario.

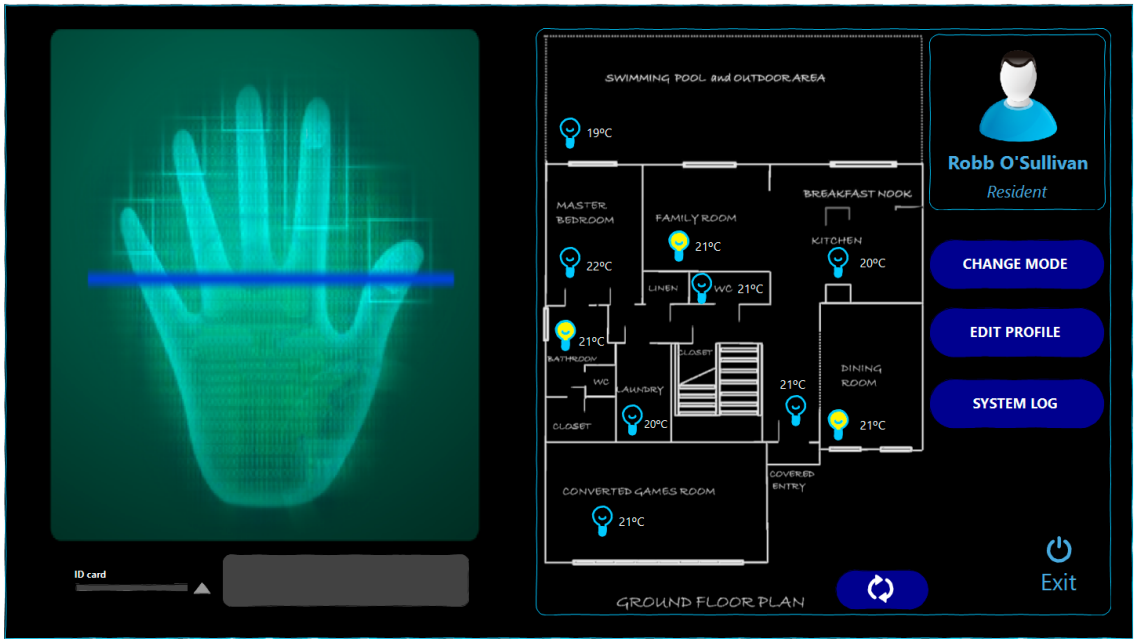

Ilustración 10: Interfaz visible para el control de la vivienda por parte de un residente, junto con las opciones disponibles.

Las limitaciones que un usuario con este tipo de perfil tiene en el panel principal se limitan a aquellas de la gestión de los permisos de los usuarios del sistema y de sus permisos.

Sí que tendrá acceso a todas las acciones sobre la casa, y la posibilidad de cambiar el modo de comportamiento del sistema, así como revisar el log de eventos registrados cuando los usuarios han llevado acabo alguna acción sobre la vivienda.

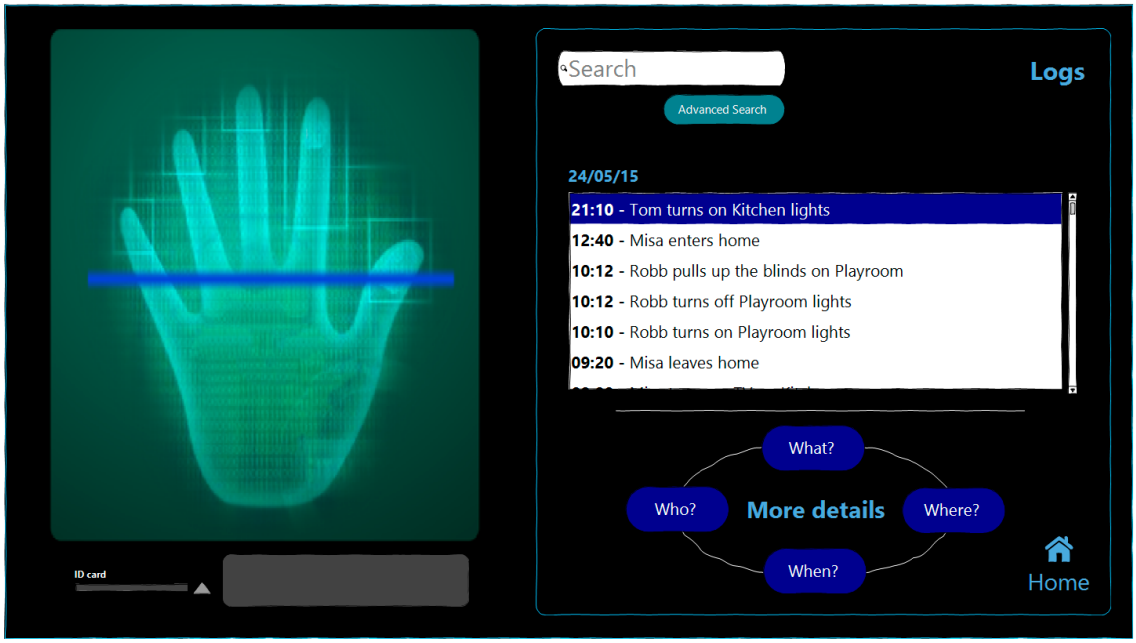

Ilustración 11: Interfaz gráfica empleada para mostrar el registro de eventos del sistema.

Cuando se revise el log del sistema, veremos una lista a modo resumen de todas las acciones llevadas a cabo y la hora en que sucedieron.

Pero además, seleccionando cualquier entrada del registro, podremos escoger que información más detallada queremos ver de ese evento concreto.

Esta interfaz tendrá la misma apariencia para los usuarios administradores, pues los eventos sucedidos en casa pueden ser revisados únicamente por las persona que viven en la casa, y el administrador siempre será uno de ellos.

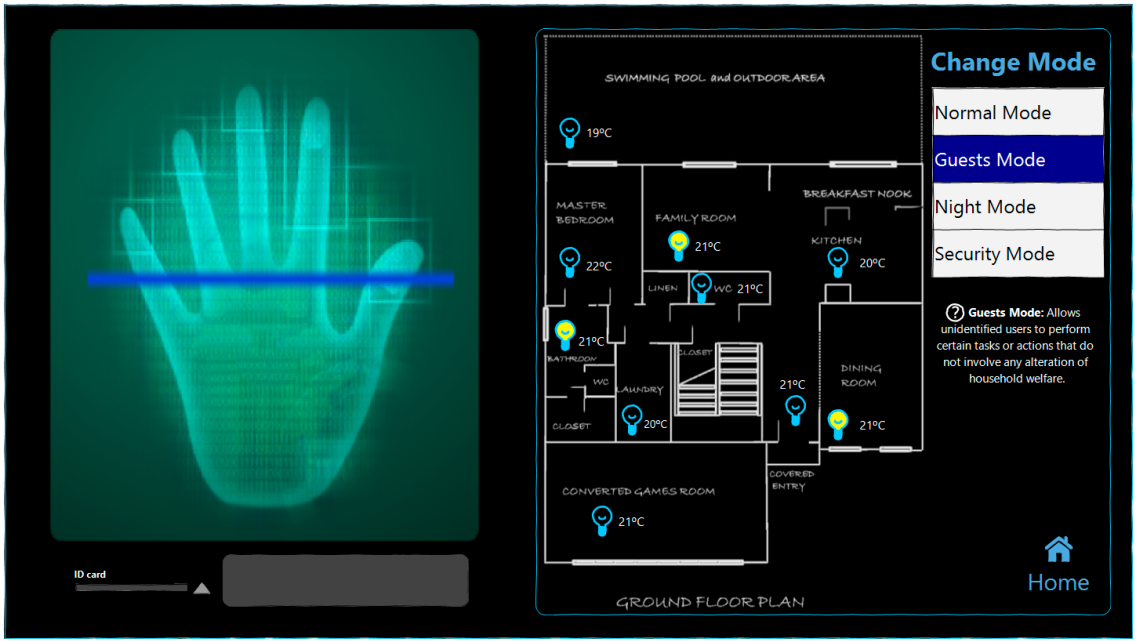

Ilustración 12: Interfaz gráfica que muestra la posibilidad de cambiar el modo de comportamiento del sistema.

El cambio de modo de comportamiento podrá ser llevado a cabo por los residentes, pues los cambios en la seguridad no son críticos y se considera que, al vivir en la casa, obviamente no van a poner en peligro voluntariamente sus pertenencias y sus bienes más preciados.

5.2.3 Habilitado por administrador

El panel mostrará la posibilidad de entrar en el gestor de usuarios, junto con todas las opciones visibles para un residente, cuando un administrador habilite el panel autenticándose.

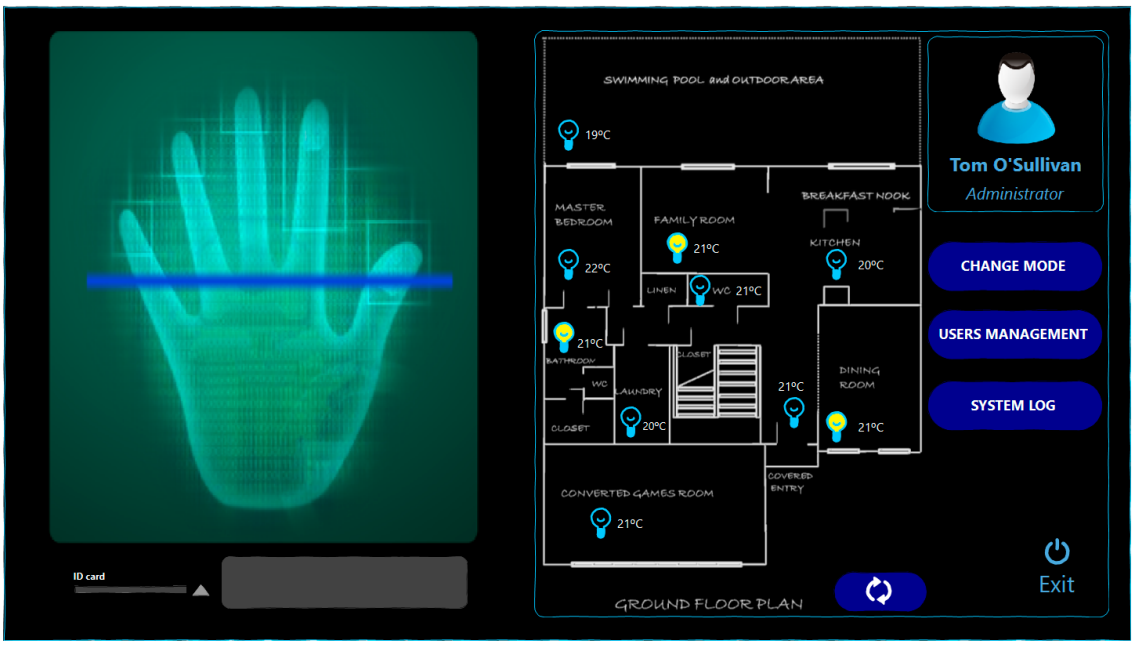

Ilustración 13: Interfaz visible para el control de la vivienda por parte de un administrador del sistema, junto con las opciones disponibles.

En la pantalla de gestión de usuarios, el administrador verá una lista con los nombres de los usuarios y a su lado el perfil completo de estos.

Ilustración 14: Apariencia básica de la interfaz de gestión de usuarios dels sistema.

Se podrá realizar una búsqueda simple por el nombre del usuario, o seleccionar distintos filtros en las opciones de búsqueda avanzada, pudiendo mostrar los usuarios según su perfil, o según fecha del último acceso.

Cuando el administrador tenga seleccionado un usuario, toda la información de este aparecerá visible, con varias opciones pera realizar sobre el perfil:

- Editar datos básicos:

Con el usuario seleccionado, se podrá pasar al modo de edición de los datos básicos como su nombre, su foto o la MAC de su dispositivo. Además, tendremos la opción de volver a almacenar los datos del usuario en una tarjeta identificativa en caso de extravío o de haberla usado para otros usuarios por necesidad.

Ilustración 15: Ejemplo de interfaz gráfica para la edición de datos de un usuario. Las fechas son modificadas automáticamente por el sistema.

En este apartado podremos también inhabilitar/habilitar al usuario si sabemos que durante un tiempo no usará el sistema, por ejemplo por una estancia en el extranjero, pero que volverá a utilizarlo en un futuro próximo.

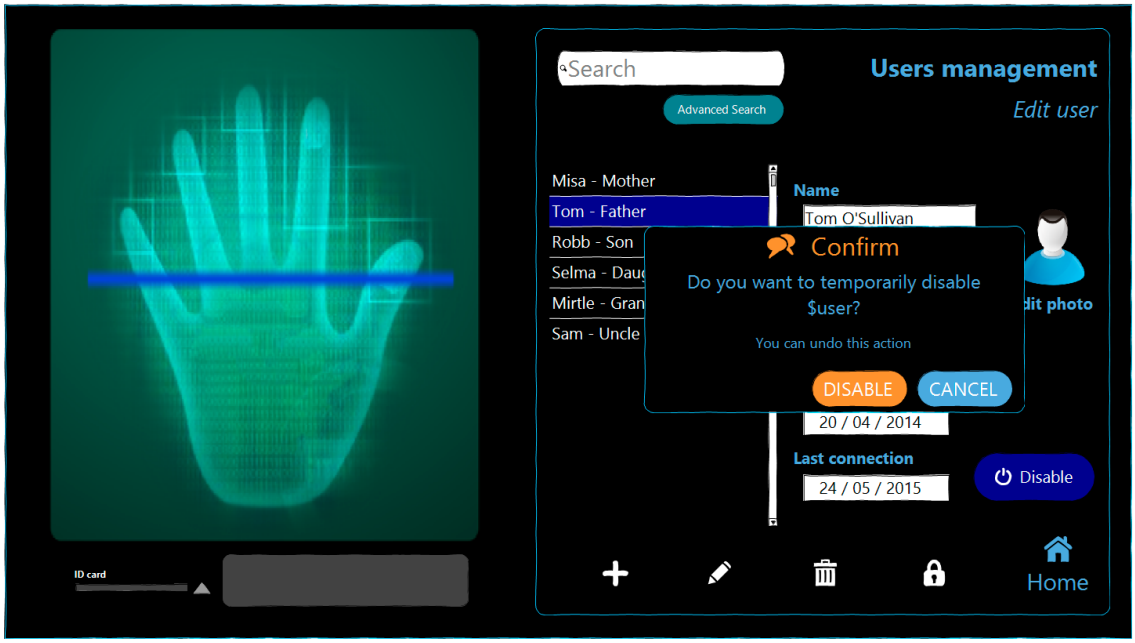

Ilustración 16: Mensaje de confirmación para la inhabilitación del usuario. El usuario podrá ser habilitado en un futuro.

En el momento de habilitarlo también podremos volver a almacenar sus datos en una tarjeta identificativa, pues el sistema nos preguntará por ello.

- Eliminar:

Tras pedir confirmación, el sistema eliminará al usuario del sistema, aunque en los logs de eventos anteriores seguirá apareciendo el nombre del usuario en el momento que se ejecutó debido a que estos no se pueden modificar de ningún modo.

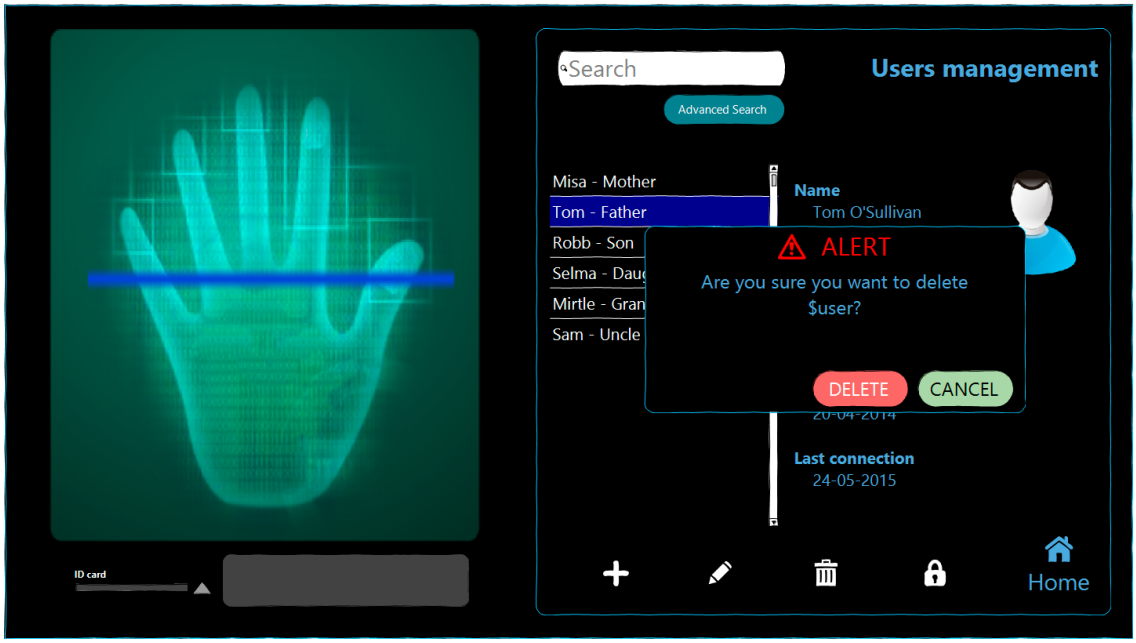

Ilustración 17: Interfaz con el mensaje de confirmación requerida por el administrador para eliminar un usuario completamente.

No quedarán datos del usuario de ningún tipo, eliminando por completo incluso sus datos biométricos.

- Editar permisos:

En este apartado podremos modificar los permisos del usuario seleccionado cambiando su tipo de perfil entre Invitado, Residente o Administrador. Solo para los menores de edad se podrá escoger el perfil Infantil.

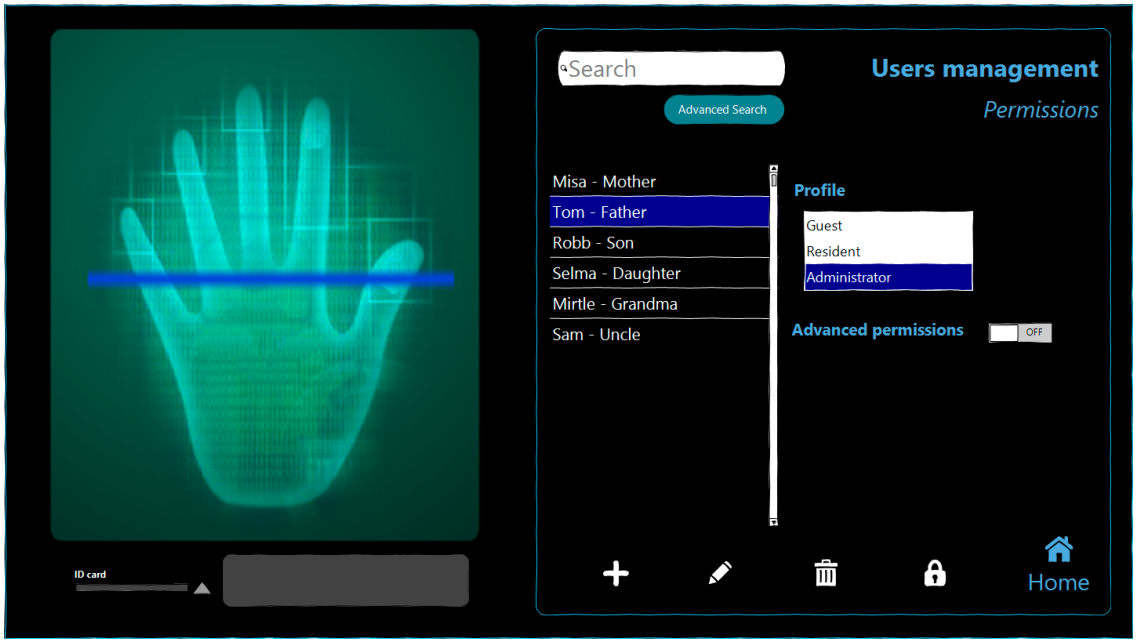

Ilustración 18: Interfaz de cambio de perfil de seguridad para yn usuario. El administrador no se podrá cambiar el perfil a si mismo.

También en este apartado podremos activar la edición de permisos avanzada para editar uno a uno los diferentes permisos de ese usuario, pudiendo otorgarle más o menos de los que su perfil predeterminado le confieren.

Ilustración 19: Interfaz gráfica con la edición de permisos avanzados activada.

- Crear:

Si desea añadir un nuevo usuario al sistema, el administrador tendrá que añadir sus datos básicos y darle unos permisos, pudiendo seleccionar directamente un tipo de perfil predeterminado y modificando a partir de este las autorizaciones.

Ilustración 20: Interfaz gráfica en la que se muestra la pantalla de creación de un nuevo usuario.

En el paso final de este proceso se solicitará que el nuevo usuario ponga la mano en el escáner vascular para registrar sus datos biométricos y que se conecte una tarjeta al lector para grabar los datos del usuario y que pueda utilizarla cuando deba acceder a la casa.

Los permisos del usuario no se harán efectivos hasta que se hayan almacenado correctamente sus datos biométricos y se realice la verificación de los mismos (el usuario deberá volver a pasar la mano por el lector tras su alta para comprobar que la comparación de los datos obtenidos con los almacenados resulta efectiva).

5.3 Dispositivos móviles

El panel de control en los dispositivo móviles será similar al panel central, pero con limitaciones a la hora de gestionar temas de permisos o de gestionar usuarios.

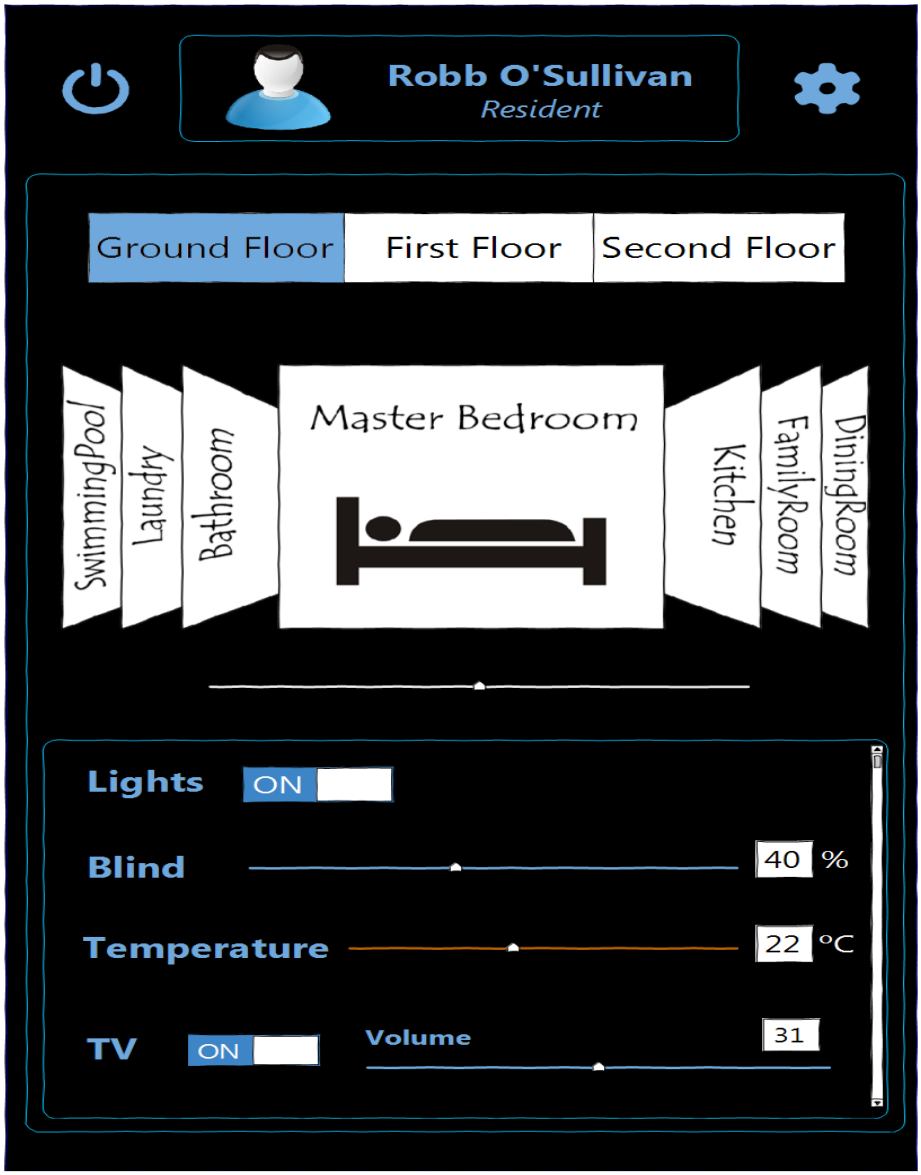

Ilustración 21: Interfaz de interacción con la vivienda domótica desde un dispositivo móvil

Desde el dispositivo móvil podemos realizar las mismas acciones que podríamos realizar desde el panel de control, con nuestro usuario, sobre los elementos de la casa, es decir, podemos regular la temperatura, encender las luces, poner en marcha el televisor…

La autenticación del usuario en este caso se realiza mediante la comprobación de la MAC registrada cuando se creó o se modificó al usuario. Así, sabemos qué partes de la casa tendrá limitadas y si algún tipo de cambio no puede realizarlo.

Como meter un mapa completo de la casa era inviable debido al tamaño reducido de los textos informativos y su imposibilidad de interactuar directamente sobre los elementos, nos hemos decantado por convertirlo en una lista de habitaciones mostrando los controles de las mismas en cada pantalla.

Por otra parte, los dispositivos de personas con un perfil de residente o administrador, recibirán notificaciones cuando se produzca algún cambio, pero como esto podría resultar un tanto molesto debido a la posible cantidad de acciones realizables en un breve periodo de tiempo, los usuarios podrán configurar estas notificaciones para que muestren un resumen cada cierto tiempo, o para consultarlo cuando lo deseen.

Del mismo modo, los administradores recibirán en el momento que suceda, una notificación informando sobre cambios en el modo de comportamiento del sistema, modificaciones sobre los usuarios y/o sus permisos, o accesos a la vivienda.

6 El sistema de seguridad aplicado a una casa

Tras la debida documentación, valoración y pruebas realizadas, se han establecidas unas pautas para poder implementar un sistema domótico en cualquier tipo de vivienda, desde casas particulares hasta edificios con una comunidad de vecinos, además de permitir su uso a todo tipo de usuarios con total seguridad para los mismos.

Veamos cual sería el sistema resultante si lo aplicáramos a una casa particular y lo necesario para llevarlo a cabo.

Ilustración 22: Recuperada en junio de 2015, de: http://gstylemag.zippykid.netdna-cdn.com/wp-content/uploads/2015/01/SmartHome.jpg

6.1 Requisitos hardware

El sistema domótico que hemos diseñado para su implementación ha de incluir un servidor con una potencia de cómputo suficiente para realizar verificaciones de datos biométricos de varios bytes de tamaño. No se requiere una potencia descomunal, pero si un mínimo, que podríamos construir a partir de un equipo informático de gama media.

Por otra parte, se requiere la instalación de dos lectores biométricos para obtener los datos de la persona que desea utilizar el sistema y para autenticar a quien intenta abrir la puerta.

Los dispositivos que se utilicen para el control de la casa de forma remota pueden ser los que se deseen, con conexión a internet como requisito, pues OpenVPN es compatible con los distintos sistemas operativos actuales en el mercado, al igual que PFSense, aunque este solo se instalará en el servidor de la casa.

Con el abaratamiento de los discos duros, aprovechamos para incluir un par de discos de copia de seguridad, por lo que pudiera suceder. De este modo preservaremos la configuración y el funcionamiento del sistema en caso de algún fallo.

Y por último, para evitar que un pequeño corte de luz pueda dejarnos sin control de la casa, añadimos un SAI que nos permita mantener el servidor en marcha en caso de apagón durante algunas horas, a la vez que servirá de protección en caso de subidas de tensión por tormentas u otros factores.

6.2 El servidor domótico

El servidor principal donde se implementará toda la funcionalidad de la casa se protegerá de los posibles ataques desde la red mediante la utilización de la solución software PFSense, que nos brinda un magnífico firewall con una política restrictiva, dejando únicamente los puertos que se necesiten para el envío de información y para la recepción de ordenes.

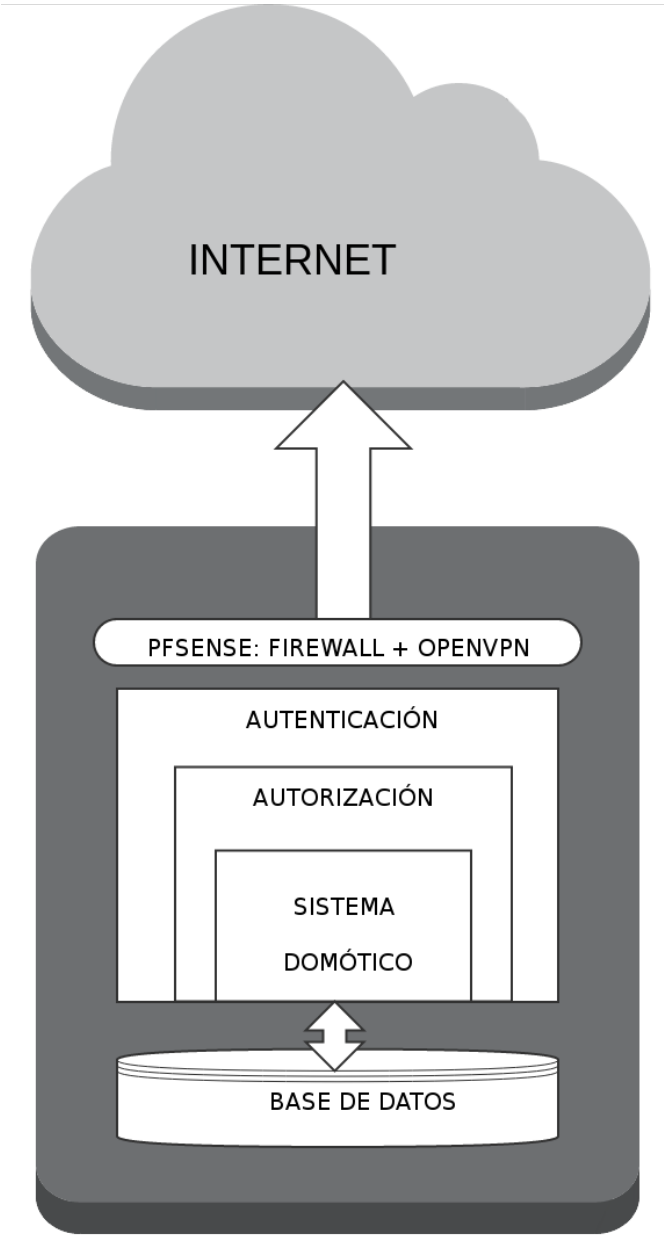

Ilustración 23: Esquema de la arquitectura del sistema domótico del servidor

Además, toda conexión que se realice al servidor estará correctamente cifrada y viajará a través de redes virtuales privadas. La mejor herramienta para implementar una VPN segura y fiable, que además es opensource, es OpenVPN, que se puede incorporar como un módulo más de PFSense.

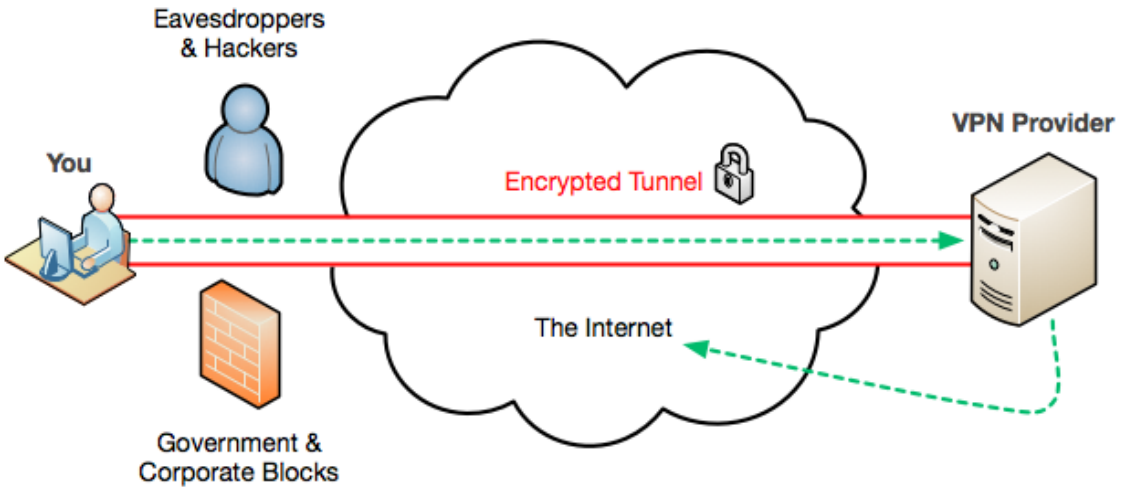

Ilustración 24: Diagrama VPN. Recuperado en junio de 2015, de: http://blog.rastating.com/content/images/2014/11/vpn-diagram.png

OpenVPN se configurará con un protocolo SSL/TLS junto con una clave pre-compartida para la identificación de los paquetes enviados entre los distintos puntos para evitar ataques de DoS, al no intentar procesar ningún paquete que no este cifrado con esa llave. El inconveniente que tenemos con esta solución es que hemos de instalar el software OpenVPN en todos aquellos dispositivos que vayan a conectarse al servidor a través de Internet y compartir de forma segura la clave pre-compartida para identificar los paquetes válidos. Pero considerando que esto se puede llevar a cabo en poco tiempo, y la gran seguridad que ofrece, es más que aceptable.

6.3 Primeros pasos con el panel de control

El lugar más apropiado para instalarlo es en el recibidor de la casa o en la sala principal.

A diferencia de lo que sucede con los dispositivos móviles, en el panel de control se pueden realizar todo tipo de acciones dependiendo del usuario que lo utilice.

Estará cableado con RJ-45 cruzado hasta el servidor principal para evitar retrasos en las comunicaciones y para garantizar una seguridad completa al no estar enlazado a Internet. El sistema tiene una serie de ordenes únicamente realizables a través del panel de control, por lo que se ignoraría cualquier intento de ejecución de esas ordenes que no provenga directamente del cable.

Su funcionalidad ya ha sido descrita en el apartado 5.2, pero para su funcionamiento hay una configuración inicial que sería interesante detallar.

Lo primero de todo será definir al usuario administrador, pues siempre ha de haber uno disponible en el sistema, para poder agregar otros usuarios y cambiar permisos. Para esto se seguirán los pasos que serán los mismos que más adelante seguiremos para añadir a cualquier otro usuario.

Se registra su nombre, apellidos, fecha de nacimiento y, opcionalmente, la dirección MAC de su dispositivo, con el que interactuar posteriormente. Se almacenará la fecha de su alta en el sistema y se solicitará una lectura biométrica de los vasos sanguíneos de su mano, para lo que únicamente deberá posar la mano sobre el lector. Tras obtener los datos de la persona, se solicitará una tarjeta identificativa a introducir en el lector-grabador. Se registrarán los datos para su identificación de forma cifrada en la tarjeta y se pedirá al usuario una prueba de autenticación para verificar que el proceso de registro ha sido correcto.

Al ser el primer usuario en registrase, automáticamente tendrá permisos de control total, pues será el administrador (más adelante, tras definir a otro usuario como administrador, se podrán modificar los permisos del anterior para que deje de serlo).

En el caso de cualquier otro usuario, se podrán escoger entre los perfiles de seguridad, para otorgarle autorización a determinados conjuntos de elementos de forma cómoda y sencilla, y/o pasar a definir los permisos de manera más concreta, detallando que acciones más exactas puede o no realizar.

Una vez creados los usuarios con sus permisos ya podremos pasar al siguiente punto importante para el control de la casa: los dispositivos móviles de los usuarios que nos permitan lanzar las acciones de la vivienda de forma remota.

6.4 Configuración de los dispositivos móviles

Con PFSense, desde el servidor, generamos una clave para almacenar en los dispositivos que deseamos conectar. Esta se tendrá que mantener a buen recaudo en los dispositivos en los que vamos a utilizarla.

Anteriormente, a cada usuario le hemos asignado, de forma opcional, un dispositivo móvil, registrando su MAC en el sistema. Ahora hay que configurar OpenVPN en los smartphones y tablets escogidas para que puedan conectar con total seguridad con el servidor.

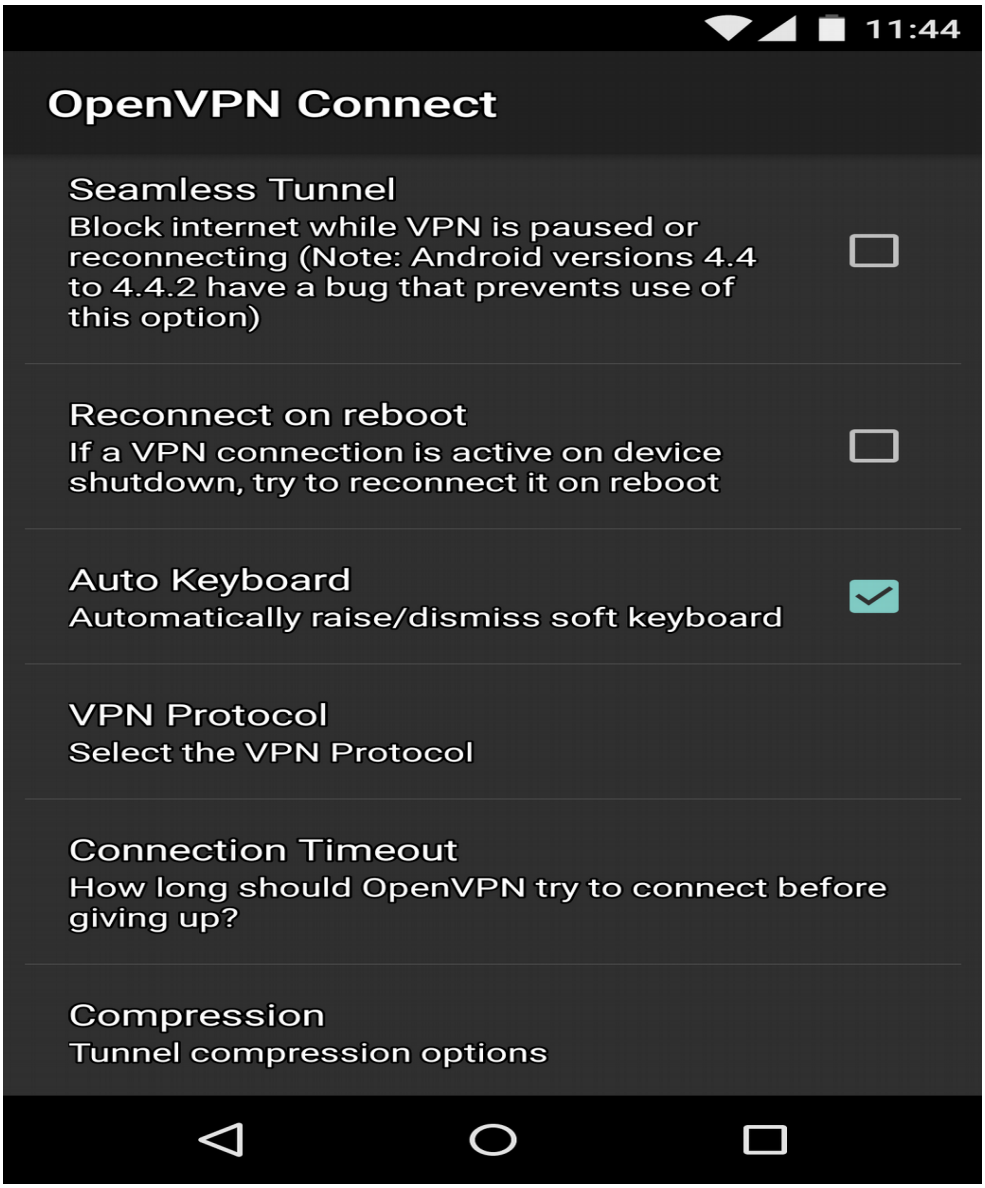

Ilustración 25: Captura con las opciones de OpenVPN y su información detallada

Una vez se ha configurado OpenVPN, que gracias a su interfaz intuitiva y sus explicaciones acerca de cada punto, no cuesta mucho tiempo, podemos optar por añadir un acceso directo para decidir cuando conectar la VPN o dejar que siempre que tengamos el dispositivo desbloqueado se conecte.

Estos pasos solo necesitamos hacerlos una vez, pues al igual que copiamos la clave pre-compartida cada vez que añadimos un nuevo dispositivo al sistema, podemos importar también la configuración de OpenVPN, ahorrándonos la configuración manual.

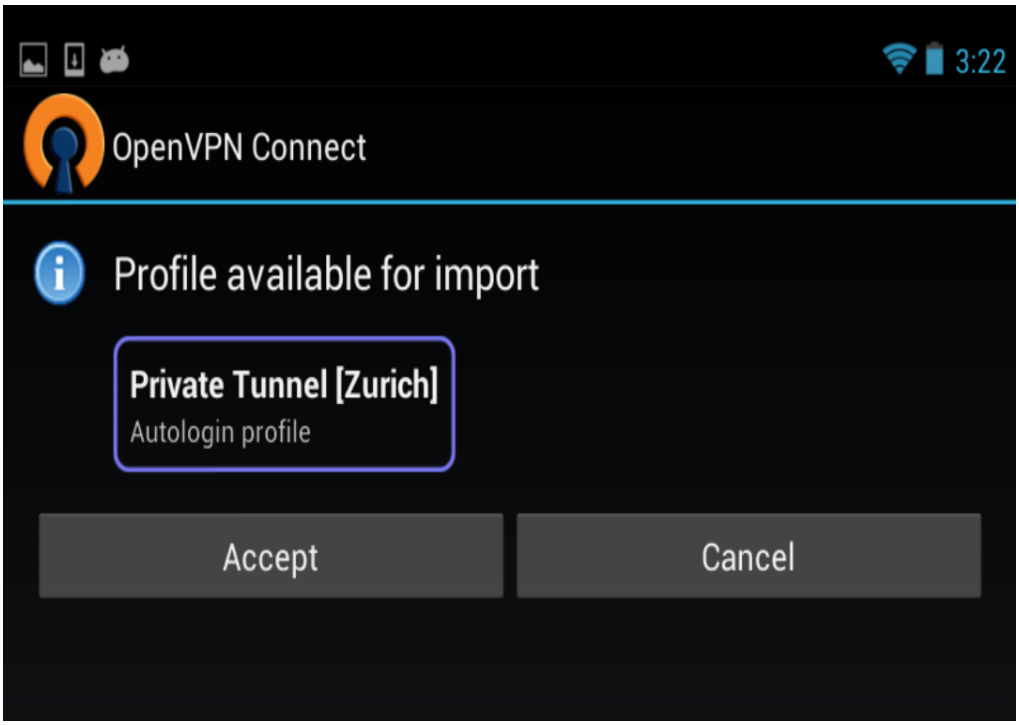

Ilustración 26: Captura sobre la importación de un perfile OpenVPN

El uso de la aplicación en el dispositivo no requiere cuentas de usuarios, pero sí debe configurarse una clave de acceso a la aplicación en forma de patrón u otro método identificativo sencillo, al igual que también debe poder obtener información del aparato para la verificación de la MAC y configurar la ruta a la que ha de conectar para establecer comunicación con el servidor.

Si la VPN no está conectada en el momento de abrir la aplicación o lanzar una orden, esta dará un error al ser imposible conectar con el servidor.

Es por esto que en aquellos dispositivos que vayan a permanecer en la casa, o que dispongan de suficiente capacidad para mantener la conexión, es recomendable dejar que la VPN se establezca automáticamente.

Mantener la conexión VPN siempre disponible no implica que las claves de cifrado no cambien, estas lo seguirán haciendo cada cierto tiempo, por lo que los pasos para mantener la conexión serán similares a los de establecerla por primera vez.

Por suerte, la comunicación no se cortará con un cambio de claves gracias al modo multiventana de OpenVPN, que permite terminar las transferencias de datos mientras en otro proceso en segundo plano realiza el nuevo handshake con el servidor.

Entendemos que el uso de dispositivos móviles es para la comodidad del usuario y para mantener un mejor control sobre la casa, por lo que el uso responsable del mismo ya solo depende de la persona que lo maneja, aunque las funciones más críticas que afecten a la seguridad del sistema nunca serán ejecutadas o alteradas desde otro lugar que no sea el panel de control.

7 Conclusión

Tras todos los estudios realizados y la apropiada documentación para la elaboración de este proyecto, me parece que las casas inteligentes serán una realidad en un futuro bastante cercano, aunque por el momento no será accesible para la mayoría de las personas, pero esto es algo que sucede con todas las nuevas tecnologías.

En tiempos remotos, solo un pequeño porcentaje de la población podía escuchar la radio, ver la televisión o conducir un coche. Pasados unos cuantos años, ese porcentaje ha aumentado drásticamente, sobretodo en los países más desarrollados. Por eso no descarto que en unos años, todas las casas y edificios se construyan pensadas para la domótica.

Con este proyecto espero poder servir de guía para personas que quieran aumentar la seguridad de sus servidores o implementar un sistema domótico en sus casas.

El objetivo más complicado de cumplir de los que me había propuesto es poder mostrar los beneficios de la tecnología a esa parte de la población que teme las innovaciones y la menosprecia prefiriendo los métodos manuales con grandes posibilidades de fallos e imperfecciones porque “así se ha hecho siempre”. Y digo que es el más complicado porque el menor fallo, puede convertir una buena idea en una nueva amenaza para la sociedad con esta mentalidad.

Antes de empezar este proyecto, mis conocimientos sobre seguridad se basaban en considerar segura una autenticación en dos pasos, o verificar las aplicaciones que instalo en mis equipos.

Según iba profundizando en el tema de la seguridad, me doy cuenta de que por mucho que nos esforcemos en mantener seguro un sistema, siempre habrá una mínima opción para romper esa seguridad, por lo que nuestras contribuciones se basarán en protegernos de ataques ya sufridos.

De la experiencia, y sobretodo de los errores, surgen las mejores ideas, las mejores soluciones, los mayores avances en la tecnología, mejorando día a día la seguridad de las personas y procurando preservar el mundo en el que vivimos.

Quizás con mucho esfuerzo, lleguemos a tiempo para ofrecer un futuro prometedor al mundo del mañana y cumplir con las promesas de esos mundos futuristas que tanto nos ofrece la literatura y cinematografía.

8 Bibliografía

8.1 Biometría y tecnologías de autenticación

JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun A. *Handbook of biometrics*. Springer Science & Business Media, 2007.

Griaule Biometrics. (2008). *Understanding biometrics*. Recuperado en marzo de 2015, de:
http://www.griaulebiometrics.com/en-us/book/understanding-biometrics

CNX Anixter. (2013). *Biometría vascular-¿Es el futuro?*. Recuperado en abril de 2015, de:
http://www.anixtersoluciones.com/es/cnx/noticia/95/biometria-vascular-es-el-futuro

Javier Gómez. (24 de septiembre de 2012). *La biometría vascular, un nuevo sistema biométrico.* Dolthink. Recuperado en abril de 2015, de:
http://www.dolthink.com/biometria-vascular-lector-biometrico.html

Crossmatch Technologies. (enero de 2012). *I Scan 2 - Dual Iris Capture Scanner*. Recuperado en abril de 2015, de:
http://www.biometriaaplicada.com/E-STORE/DataSheets/ds-iscan2.pdf

Joaquín Rodríguez Varela. (16 de abril de 2014). *Los nuevos lectores biométricos también pueden ser engañados*. Recuperado en abril de 2015, de:
http://www.welivesecurity.com/la-es/2014/04/16/nuevos-lectores-biometricos-tambien-pueden-ser-enganados/

INTECO. (diciembre de 2011). Estudio sobre las tecnologías biométricas aplicadas a la seguridad. Recuperado en abril de 2015, de:
https://www.incibe.es/file/tGi1Xn2W88xxCP8CLUmW_g

INTECO. (octubre de 2011). Guía sobre las tecnologías biométricas aplicadas a la seguridad. Recuperado en abril de 2015, de:
https://www.incibe.es/file/ncKsGyFaqPdQ7ms3m2eDeA

8.2 VPN - Protocolo TLS

GigaNews. (2015). *Compare los Protocolos de VPN - PPTP vs L2TP vs OpenVPN vs Chameleon*. Recuperado en mayo de 2015, de:
http://es.giganews.com/vyprvpn/compare-vpn-protocols.html

OpenVPN Technologies. (2015). *Documentation*. Recuperado en mayo de 2015, de:
https://openvpn.net/index.php/open-source/documentation.html

Openmaniak. (4 de febrero de 2011). *OpenVPN - Introduction*. Recuperado en mayo de 2015, de:
http://openmaniak.com/openvpn.php

RedesZone. (2014). *OpenVPN: Conéctate a cualquier red de forma segura*. Recuperado en junio de 2015, de:
http://www.redeszone.net/redes/openvpn/

Rafa Morales. (5 de noviembre de 2013). *VPN con el protocolo SSL/TLS y OpenVPN*. TICArte. Recuperado en junio de 2015, de:
http://www.ticarte.com/contenido/vpn-con-el-protocolo-ssl-tls-y-openvpn

TechNet Microsoft. (agosto de 2005). *Requerir cifrado TLS*. Recuperado en mayo de 2015, de:
https://technet.microsoft.com/es-es/library/cc759573.aspx

Carlos Erazo. (marzo de 2009). *Protocolo TLS (Transport Layer Security)*. Monografías. Recuperado en mayo de 2015, de:
http://www.monografias.com/trabajos74/protocolo-tls-transport-layer-security/protocolo-tls-transport-layer-security.shtml

8.3 Firewall - PFSense

PFSense. (16 de enero de 2015). PFSense Documentation. Recuperado en junio de 2015, de:
https://doc.pfsense.org/index.php/Main_Page

Juan Manuel Sanz. (28 de mayo de 2014). PFsense: firewall perimetral (I). Security Artwork. Recuperado en junio de 2015, de:
http://www.securityartwork.es/2014/05/28/pfsense-firewall-perimetral-i/

Juan Manuel Sanz. (10 de julio de 2014). PFsense: firewall perimetral (II). Security Artwork. Recuperado en junio de 2015, de:
http://www.securityartwork.es/2014/07/10/pfsense-firewall-perimetral-ii/

Juan Manuel Sanz. (6 de octubre de 2014). PFsense: firewall perimetral (III). Security Artwork. Recuperado en junio de 2015, de:
http://www.securityartwork.es/2014/10/06/pfsense-firewall-perimetral-iii/

Juan Manuel Sanz. (15 de diciembre de 2014). PFsense: firewall perimetral (IV). Security Artwork. Recuperado en junio de 2015, de: http://www.securityartwork.es/2014/12/15/pfsense-firewall-perimetral-iv/

Juan Manuel Sanz. (18 de febrero de 2015). PFsense: firewall perimetral (V). Security Artwork. Recuperado en junio de 2015, de: http://www.securityartwork.es/2015/02/18/pfsense-firewall-perimetral-v/

Juan Manuel Sanz. (11 de junio de 2015). PFsense: firewall perimetral (VI). Security Artwork. Recuperado en junio de 2015, de: http://www.securityartwork.es/2015/06/11/pfsense-firewall-perimetral-vi/

9 Índice de ilustraciones

10 Índice de Tablas