

Servidor de gestion de llaves criptográficas e identidades para redes inalámbricas

PROBLEMA

Las redes inalámbricas forman parte de las tecnologías más usadas en la actualidad y se ha visto afectada en diferentes aspectos. Aún más en su seguridad, la cual se ha convertido en un blanco para personas que desean introducirse en una red y extraer información para cometer actos delictivos como es la extorción o suplantación de identidad. Las herramientas usadas para realizar este tipo de acciones son fácilmente accesibles incluso a través de plataformas comerciales ampliamente conocidas solo para ser descargadas sin mayor complejidad, lo que resulta en convertir este problema en mas grave aún.

OBJECTIVO GENERAL

Desarrollar un sistema de seguridad gestionado mediante un Daemon que permita la administración y distribución de credenciales de usuario y de red.

PROPUESTA

Implementación de un sistema que actualiza de manera dinámica la clave de red y de forma transparente para los usuarios por medio de unas luminarias. Se configurará un sistema de autenticación y encriptación de credenciales de usuarios y clave de red administrable a través de una interfaz. web

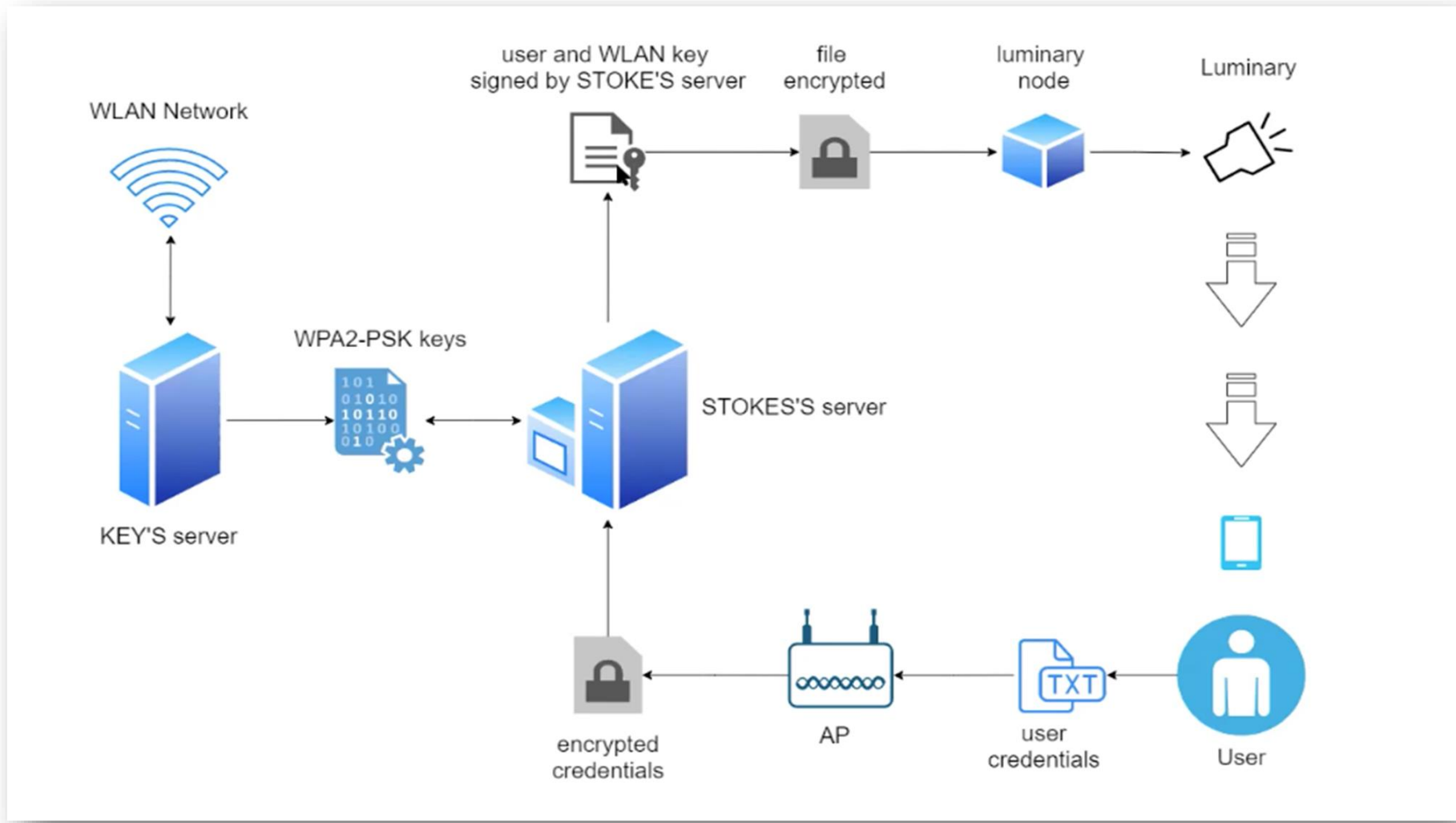


Figure 3: Diagrama esquemático de la propuesta

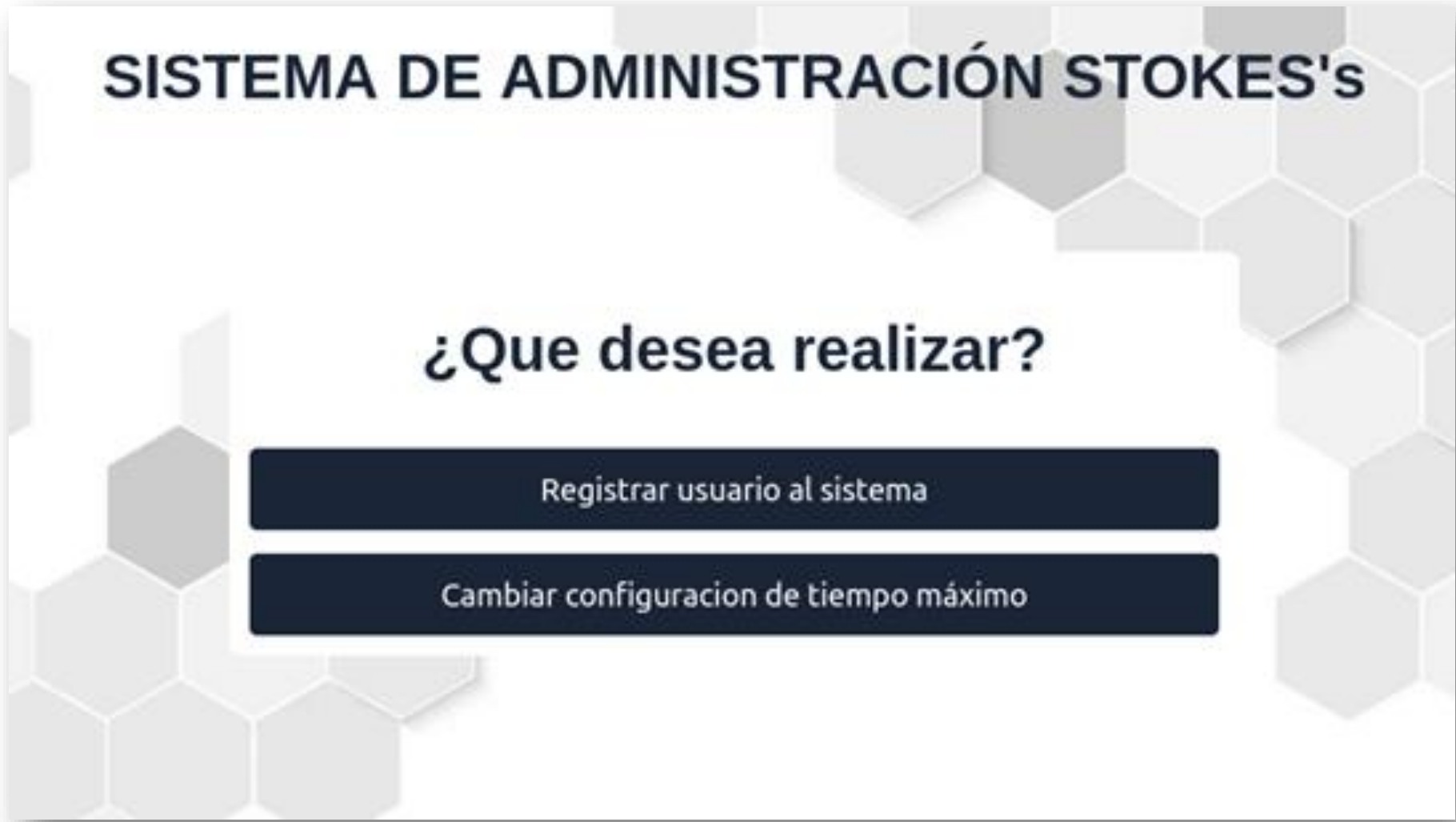


Figure 4: Ventana de configuración del sistema

RESULTADOS

Con el Daemon en ejecución, un usuario registrado en el sistema envía sus credenciales a un dispositivo conectado a la red, esta información es reenviada a nuestro servidor donde se realizará la verificación de los datos. Posteriormente, se envía la contraseña wifi encriptada en un archivo de texto .gpg hacia a las luminarias junto con el usuario que desea conectarse, garantizando así el uso exclusivo de la red. Adicionalmente la contraseña se actualizará cada 5 minutos y se enviará de manera automática a todos los usuarios que se encuentren conectados

```
Validando credenciales ingresadas :
-----
Credenciales validas, usuario detectado en el sistema STOKES: joscent
Conexion establecida para 'joscent' al sistema STOKES
Disponible hasta las 12:25:31 del 29/08/2021
enviando datos a luminarias

Verificando estados de conexión de usuarios registrados :
-----
- Usuario | Estado -
-----
- ibaquerizo Desconectado
- jj Desconectado
- joscent Conectado
se añade el usuario 'joscent' al txt
- Josmart Desconectado
- jp Desconectado
-----
Realizando firma digital %%%%%%%%%%%
Encriptando clave de red actualizada %%%%%%%%%%
Enviando datos a luminarias %%%%%%%%%%%
```

Figure 5: Salida del consola del servidor STOKES

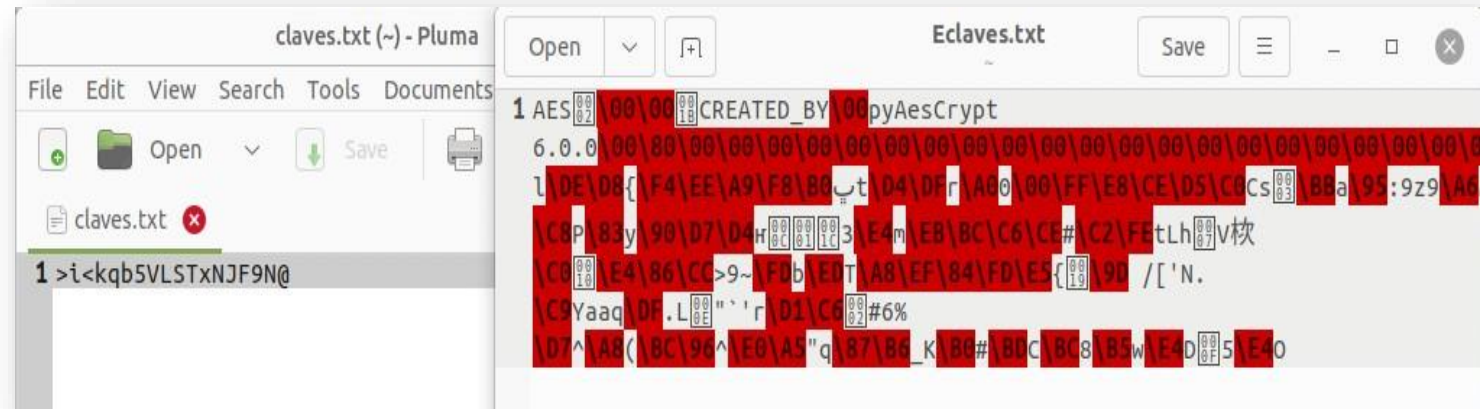


Figure 6: Clave de red encriptada en el servidor STOKES

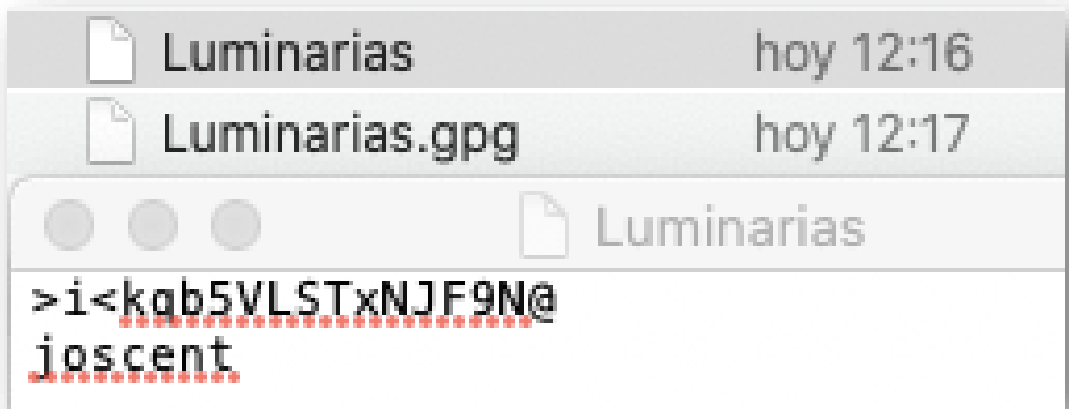


Figure 7: Archivo descriptado dentro de las luminarias

CONCLUSIONES

- Se demostró la viabilidad de desarrollar un sistema de seguridad para redes inalámbricas integrable con otras tecnologías y gestionado por un Daemon codificado dentro de un servidor.
- Se estableció y configuró las características básicas del servicio a través de interfaces de entorno grafico para la base de datos para su administración por parte del personal o departamento designado dentro de la empresa.
- Al configurar un servidor de gestión de claves se automatiza la actualización de la contraseña Wi-Fi. De esta manera se minimiza la supervisión humana, permitiendo que se destine ese tiempo a otras actividades designadas dentro de la empresa o departamento donde se implemente el servicio.