

Aplicación para asignar una clave inalámbrica de forma aleatoria con elementos de seguridad al administrador de RED.

Área: Tecnología.

(25 de Junio del 2022)

Santiago Guarín. Autor, Daniela Larrotta. Autora
POLITECNICO INTERNACIONAL

Resumen – Innova soluciones tiene un problema en el área de tecnología ya que sus administradores de red no tienen el sistema de seguridad adecuado para la plataforma. Este trabajo presenta el desarrollo de nuestra aplicación para la asignación de claves alfanuméricas aleatorias para mejorar el sistema de seguridad del administrar de red. La aplicación arrojo resultados positivos ya que logramos reducir los intentos de robo a la red y nos contribuyó a una mejor accesibilidad a la plataforma

El documento se centra en la explicación del desarrollo de la aplicación inicialmente se hizo una investigación sobre el tipo de redes para ver cual nos convenía mejor, ya que teníamos la idea empezamos a general el código que nos iba a arrojar la contraseña alfanumérica, ya que una vez se tiene todo el código se hace la interface a la plataforma para que cada administrador del área de tecnología de la empresa genere su nueva contraseña para que pueda acceder al sistema.

I. INTRODUCCION

La tecnología inalámbrica, ha experimentado un gran salto de velocidad transmisión, pero no compite con el uso o aprovechamiento de la red alámbrica Fibra óptica pero cubre bien la necesidad Movimiento y comunicación del usuario. Entre los tipos de redes de la tecnología incluyen redes de corto alcance llamado WAPN como el alcance utilizado por los equipos que llevan bluetooth, también se encuentra la red de área local (WLAN) como wi-fi y aplicaciones de LAN. Las redes tienen el objetivo de intercambiar la información la comunicación por vía aérea, como medio de transporte lo que lo convierte en una red muy débil.

Las redes inalámbricas de área local se presentan como la 0mejor alternativa que hay para la conexión a internet constituye un complemento de las redes cableadas tipo ETHERNET

Ya que las redes inalámbricas trasmiten datos se pueden interceptar fácilmente, a menos que se implementen medidas de seguridad, La seguridad equivale al cableado (WEP) esa es una calve estática con una clave hexadecimal de 64 0 128 bits, permite que las computadoras en una red intercambien mensajes codificados mientras ocultan a los ladrones el contenido del mensaje. Esta es la clave que se utiliza para para conectarse en una red de seguridad inalámbrica habilitada

Para más elementos de seguridad surgieron más medidas de seguridad como las claves WPA incluye comprobaciones integrales de los mensajes predeterminados si un atacante había capturado o alterado los datos, Las claves WPA utilizan 256 bits ya que tuvo un aumento significativos sobre las claves de 128 bits utilizadas en el sistema WEP se empezaron a explotar los elementos hasta que llevo a crear las claves WPA2



WPA2 es una versión mejorada de WPA Y WPA2 se basa en el mecanismo de red de seguridad robusta y funciona en 2 modos

- Modo personal: Es un código compartido y se usa sobre todo en espacios domésticos
- Modo Empresarial: Se utilizan sobre todo en organizaciones y empresas

El protocolo CCMP se basa en el algoritmo estándar de cifrado avanzado (AES), el cual proporciona una verificación de la autenticidad e integridad de los mensajes. CCMP es más resistente y confiable que el protocolo de integridad de clave temporal.

Para realizar el desarrollo de la aplicación de la asignación de clave aleatoria, se realizó una pequeña investigación donde identificamos el pro y los encontramos de cada tipo de conexiones. Ya por otro lado la conexión (WEP) es el sistema que estamos buscando ya que proporciona una clave a todo el sistema autorizado. A continuación, presentamos una parte del código en NetBeans Java, que fue el programa usado para realizar esta aplicación:

```
private void ButtonClaveActionPerformed(java.awt.event.ActionEvent evt) {
    // Se crea botón para guardar información e iniciar sesión con la clave aleatoria

    int longitud = 14;
    System.out.println(generateRandomPassword(longitud));

    String claveGenerada = generateRandomPassword(longitud);
    JLabelEtiqueta.setText(claveGenerada);
}

// Se crea el método de generar random password, para clave aleatoria y se conecta con el botón
public static String generateRandomPassword(int longitud)
{
    // Caracteres para generar la clave aleatoria (0-9, a-z, A-Z)
    final String caracteres = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*";

    SecureRandom aleatorio = new SecureRandom();
    StringBuilder sb = new StringBuilder();

    // Se crea un ciclo para poder generar la clave aleatoriamente con random
    for (int i = 0; i < longitud; i++)
    {
        int randomIndex = aleatorio.nextInt(caracteres.length());
        sb.append(caracteres.charAt(randomIndex));
    }

    return sb.toString();
}
```

Seguidamente se hizo el diseño de la plataforma para generar nuestro objetivo y poder cumplir con el requisito de la empresa, donde incluimos el logo, los campos necesarios para llenar la información, y el botón para generar clave aleatoria.

En la siguiente imagen evidenciamos el resultado del diseño de la interfaz:



II. CONCLUSIÓN

La creación de una interfaz para la generación de contraseñas es una gran protección al sistema de la empresa Innova ya que ayuda a no ser vulnerado versátilmente.

Adicionalmente, nos ayuda a proteger nuestros datos, Una contraseña segura es la principal barrera que impide que te hackeen la mayoría de tus cuentas en línea. Sin prácticas actualizadas, es probable que estés utilizando contraseñas que los estafadores cibernéticos pueden adivinar fácilmente en cuestión de horas.

III. REFERENCIAS

- [1] Sergio De Luz <https://www.redeszone.net/2012/02/14/generador-de-claves-wpa-y-wpa2-en-java/J>, 14 Febrero del 2012.
- [2] Pablo J - <https://www.puro-geek.com/2021/01/27/crear-un-generador-de-contrasenas-al-azar-proyecto-java-para-principiantes/>