Parte 1, Investigación

Sara Nohemi Zavala (carné No. 18893)
Ricardo Antonio Valenzuela (carné No. 18762)
Jose Amado Garcia (carné No. 181469)
Juan Fernando De Leon Quezada (carné No. 17822)
Edgar Andree Toledo Torres (carné No. 18439)

Protocolos de Contraseñas
¿Qué es?

El uso de contraseñas aún es el método de autenticación más común en la red, por eso mismo la protección de estas es de suma importancia para mantener la confidencialidad de quienes las usan.

Los protocolos de contraseña son un método de dos vías que permite autenticar a un usuario, el dispositivo remoto envía el id del usuario y la contraseña que se ingresó, ya el sistema es el que determina si los valores son correctos y delimita si continuar o terminar el proceso.

¿Existen aplicaciones actualmente? ¿Cuáles?

Dentro de las aplicaciones podemos encontrar los siguientes tipos de protocolos:

- OpenID
- OAuth
- OpenID Connect

Como mencionamos anteriormente las contraseñas son el medio de autentificación más común en la red, por lo que se puede observar su uso desde las plataformas más grandes de la red hasta la más pequeña:

- Facebook
- Google
- Youtube
- Entre otros

¿Cómo creen que podrían aplicarlo en un ambiente de trabajo?

A la hora de crear un sistema basado en usuarios se debe tener en consideración obligatoriamente la autenticación por medio de una contraseña. Esto lo podemos realizar nosotros mismos con los conocimientos ya aprendidos o delegarlo a algún proveedor de servicios enfocado a dicha autentificación.

Protocolos basados en contraseñas one-time

¿Qué es?

Contraseña que solo puede ser empleada una vez. Es una técnica que contrarresta la amenaza de un ataque de repetición que utiliza contraseñas capturadas mediante interceptación de las comunicaciones.

¿Existen aplicaciones actualmente? ¿Cuáles?

En ocasiones es la contraseña que se otorga para el primer acceso a un sistema, y que obliga a su cambio una vez validada. En otros casos el ordenador lanza un reto, que está formado por un conjunto aleatorio de caracteres numericos, que el usuario ha de cifrar con un algoritmo y clave solo conocidos por el ordenador y el usuario.

¿Cómo creen que podrían aplicarlo en un ambiente de trabajo?

Al momento de querer interactuar con un usuario y se quiera obtener información de el, se debe verificar que esta sea valida y verdadera. Por ende, en este ambiente se puede aplicar, para verificar la identidad del mismo.

Protocolos de Challenge-response ¿Qué es?

En este tipo de casos tras realizar la conexión el servidor envía al cliente un tipo de “desafío” que debe variar para cada autenticación, este desafío debe ser de forma que solo un cliente legítimo del sistema pueda resolverlos, así comprobando la autenticidad de este.

Esta es una mejora considerable a la seguridad debido a que la contraseña no es pasada directamente entre cliente y servidor, sin embargo se sabe que ambos la conocen.

¿Existen aplicaciones actualmente? ¿Cuáles?

A. CRAM-MD5
B. Secure Remote Password
C. CAPTCHA
D. Protocolo de autenticación por desafío mutuo

¿Cómo creen que podrían aplicarlo en un ambiente de trabajo?

En un sistema la utilización de este protocolo servirá para dos cosas, una ser la autenticación del usuario del sitio, y otra para comprobar que el que este ingresando no sea un bot/robot sino un humano. El ejemplo más común de esto es el uso de captchas, preguntas relacionadas al usuario entre otros.

Bibliografía

- https://es.slideshare.net/cfpdudq/protocoloes-de-seguridad-seguridad-de-contraseas-personales
- https://www.incibe-cert.es/blog/autenticacion-basada-contrasenas
- http://www.tugurium.com/gti/termino.php?Tr=one-time%20password