



## Tarea 3

### Pregunta 1

#### Parte a)

Las malas consecuencias de utilizar este tipo de autenticación pueden provenir de dos fuentes (asumiendo que el canal de comunicación es seguro), el mismo usuario que está creando y usando estas credenciales, y el servicio sobre al cual se accede:

- **Usuarios:** El problema principal va ligado en parte a la naturaleza humana. No somos buenos para recordar una gran cantidad de datos aleatorios, por lo que tendemos a utilizar contraseñas que tienen problemas de seguridad, como los siguientes:
  - No son completamente aleatorias sobre todo el espacio de caracteres. Es difícil recordar una secuencia de caracteres totalmente aleatoria, en la que sus elementos no tienen ninguna correlación entre sí. Se suele optar por contraseñas débiles que por lo general constan de sólo letras y números. También las letras generalmente forman palabras del idioma del usuario, por lo que se reduce aún más el espacio de posibilidades. En la práctica, al intentar obtener una clave por fuerza bruta, es mucho más probable que llegaremos antes a una contraseña correcta si concentramos los caracteres probados en ciertas combinaciones de palabras, a diferencia de probar todos los caracteres posibles.
  - Las contraseñas tienden a ser cortas, debido a que es difícil memorizar strings largos. Por lo tanto, en un ataque de fuerza bruta, se lograría romper mucho más rápido una contraseña corta que una muy larga.
  - Dado que en el último tiempo ha aumentado bastante la cantidad de servicios en línea que se acceden y usan este tipo de autenticación, es común repetir contraseñas entre estos sitios, para no tener que almacenar/recordar una contraseña distinta para cada servicio. Un ejemplo que expondría esta vulnerabilidad sería el caso de que algún servicio es *hackeado* y atacantes obtienen las contraseñas, se prueban los mismos nombres de usuarios y contraseñas en otros servicios que puedan estar usando los usuarios expuestos, para poder acceder a sus cuentas.
  - Si no se recurre a la memoria, entonces las contraseñas se almacenan (en texto plano) en otro lugar físico, como un cuaderno o un *post-it*, elementos que pueden encontrarse expuestos a ser vistos y abusados por otras personas.
- **Servicios:** Pueden incurrir en prácticas pobres y vulnerables para el manejo de credencial:
  - Guardar credenciales en texto plano. Al registrarnos en una aplicación, como usuarios generalmente no tenemos cómo saber las prácticas que usa el servicio al que estamos accediendo para proteger nuestros datos, por lo que como usuario debemos confiar en que se están manejando de manera segura. No usar ningún algoritmo para ocultar las credenciales, deja expuestos los datos del usuario, permitiendo a cualquier persona con acceso al almacenamiento obtener contraseñas.
  - Usar encriptación en lugar de hashing. Debido a que las funciones de encriptación no son *one-way*, existiría forma de obtener la contraseña a partir del string almacenado, dando lugar a una vulnerabilidad. Por ejemplo, un empleado del servicio con suficiente conocimiento de la llave podría acceder a las contraseñas de los usuarios.

- Usar algoritmos que en la actualidad se consideran inseguros. Por ejemplo, si un servicio online, como un banco, tiene almacenadas las contraseñas con una función de hash considerada insegura, como `md5`, si se filtra la base de datos, le será mucho más fácil a los atacantes calcular los hashes y romper contraseñas. Además, si no se utiliza *salting*, las contraseñas quedarían muy expuestas a *rainbow table attacks*.

## Parte b)