Paola Martín Sánchez

Consulta 2 – Student 2

Introducción

Contexto: En una red interna de una entidad se intenta preservar la integridad de la información transmitida entre empleados y los diferentes servidores de la entidad. Para ello se usan por cada empleado diferentes claves.

Consulta: El cliente nos solicita que le indiquemos la solución tecnológica para entregar lo más seguro y eficiente posible las claves anteriores a cada uno de los empleados que se incorporen a la entidad. Y en caso de posible ataque a dichas claves, cómo se podrían cambiar dichas claves de forma segura y eficiente.

Exponer soluciones

Una de las soluciones posibles sería usar MAC (lenguaje de programación para garantizar la integridad en la transmisión). Esto nos garantizaría la integridad en la transmisión de claves entre los empleados.

Sin embargo, nosotros recomendaríamos otra solución alternativa, que sería usar un MAC basado en funciones hash (HMAC). HMAC es un mecanismo de autenticación criptográfico que utiliza una función hash para garantizar la integridad y autenticidad de un mensaje. Por tanto, HMAC combina el "message authentication code" (MAC) con el resultado de una función hash. Es una forma de ampliar el uso de las funciones hash ya que el resultado no depende solo del hash del mensaje sino de otro parámetro que puede ser la clave secreta del usuario.

Además, para cambiar las claves de los empleados de forma segura y eficiente, podríamos usar autenticación del emisor/receptor del mensaje con claves suficientemente robusta para evitar posible replicación.

Esta anterior opción estaría bien pero nosotros recomendamos que además, la autenticación de los empleados sea de doble factor, ya que esto añade más seguridad a la autenticación.

Recomendamos, además, una política de cambio de claves fuerte y periódico.

Valorar las soluciones

Tanto para usar MAC como para usar HMAC, necesitaríamos un presupuesto para desarrollar el software e implementarlo en el software de la empresa. Sin embargo, HMAC presenta más ventajas que MAC en cuanto a seguridad.

La autenticación de doble factor nos ofrecería una mayor seguridad frente a la autenticación sin doble factor ante posibles replicaciones o suplantaciones de identidad en la autenticación.

Cómo solventar el problema

Nosotros recomendamos usar HMAC para garantizar la integridad y autenticidad de las claves proporcionadas a los empleados, ya que presenta más ventajas que MAC.

Para cambiar las claves de los empleados, nos decantaríamos por usar autenticación de doble factor, con claves robustas que eviten posibles replicaciones.

Además, recomendamos a la empresa que realice un cambio de claves periódico para asegurar la seguridad.

Referencias

Tema 2. Integridad de la Información. (I) Integridad en el almacenamiento y las transmisiones

https://justcryptography.com/funciones-hash-criptograficas-y-hmac/