ONE TIME PASSWORD

Este documento no pretende ser un curso exhaustivo, en el mejor de los casos, únicamente puede considerarse como un conjunto de notas complementarias en alguna asignatura. Por supuesto, todo documento es susceptible de mejora, cualquier sugerencia o comunicación de error u omisión será bienvenida.

Lamport S-Key

Una primera aproximación para fortalecer protocolos de identificación basados en palabras de acceso consiste en considerar que estas sean de un único uso. Existen distintas aproximaciones para ello, un protocolo interesante en este sentido ses el esquema *S-Key* propuesto por Lamport y basado en el uso de una función unidireccional.

Algoritmo 1 Esquema de identificación S-Key de Lamport

Entrada: Selección, por A, de un valor secreto w_0
Entrada: Una función *hash* h
Entrada: t // # máximo de identificaciones permitido
Entrada: $A \rightarrow B: \ < w = h^t(w_0) >$ // secreto compartido
Entrada: A inicializa el contador de accesos $i = 1$
Entrada: B guarda el valor recibido como $pass_A$ e inicializa el contador de A: $i_A = 1$

1: **Método**
2: $\langle A \rangle: \quad w = h^{t-i}(w_0)$
3: $\langle A \rightarrow B \rangle: \ < A, \ i, \ w >$
4: **Si** $i == i_A$ **y** $h(w) == pass_A$ **entonces**
5: El verificador acepta la identificación
6: $\langle B \rangle: \quad i_A = i$
7: $\langle B \rangle: \quad pass_A = otp$
8: $\langle A \rangle: \quad i++$
9: **FinSi**
10: **FinMétodo.**

Asumimos que el esquema se utiliza para permitir a un usuario A (*claimant*) identificarse frente a un servicio B (*verifier*). En el esquema S-Key las partes acuerdan una función resumen h y un umbral t del número de identificaciones permitido. Además, A establece un *secreto inicial* w_0 que utiliza para obtener el *secreto compartido* con B como:

$$w = h^t(w_0) = \underbrace{h(h(\ldots h(w_0)))}_{t \ veces}$$

El secreto compartido es transmitido inicialmente de forma segura y es actualizado junto con el contador de accesos autorizados después de cada identificación correcta. Alcanzado el umbral t fijado a priori el sistema necesita la reinicialización de los valores de partida. El esquema se describe en el Algoritmo 1

En el protocolo, en cada intento de identificación el usuario prepara un password componiendo la función resumen sobre el secreto inicial (que únicamente conoce él) un número de veces tal que únicamente falte un resumen para obtener el secreto compartido. El contador de identificaciones se mantiene: por parte del usuario para obtener la siguiente palabra de acceso, y por parte del servidor para proceder a la reiniciación de los parámetros al alcanzar el umbral de identificaciones fijado a priori.

Seguridad

La seguridad del sistema recae en la dificultad de invertir una función unidireccional o en el de encontrar un mensaje con el mismo resumen que un valor hash dado.

El esquema es sensible a un ataque de un adversario activo que suplante al servidor e intercepte el secreto compartido de inicialización del protocolo. Este inconveniente puede evitarse estableciendo los parámetros iniciales del esquema únicamente después de un proceso de identificación mutua de las partes. En determinadas *condiciones de carrera* (situaciones en las que el servicio queda a la espera de recibir parte del paquete de identificación) el esquema puede ser sensible si el servidor queda a la espera de recibir determinado número de bits y el atacante es capaz de probar cualquier combinación de estos.

Originalmente el sistema consideraba resúmenes de 64 bits que eran convertidos en una cadena de palabras. Pese a ser de fácil actualización, actualmente este esquema ha caído en desuso.