REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 13. No. 2, mayo-agosto, 2014, p. 62-82 ISSN 1729-3804

ANÁLISIS Y PROPUESTA DE UN PROTOCOLO DE AUTENTICACIÓN ROBUSTA MEDIANTE ONE TIME PASSWORDS, USANDO TARJETAS INTELIGENTES, PARA REDES DIGITALESEN EL HOGAR

Sandor Ernesto Tuñón Andrés

Facultad de Informática,Electrónica y Comunicaciones, Universidad de Panamá, Ciudad Panamá, Panamá
sandoret@citicup.org

RESUMEN

En este trabajo, se realiza un análisis de la seguridad de un protocolo de autenticación robusta usando tarjetas inteligentes para redes digitales en el hogar, propuesto por *Vaidya et al.*. Este tipo de redes ha ido creciendo en aplicaciones para el confort y la atención médica a distancia entre otras opciones. En estos entornos delicados, no siempre se puede garantizar la seguridad de los canales de comunicación, por lo que se requiere de otras alternativas que brinden un alto nivel de seguridad. Los actuales mecanismos de autenticación robusta usando *one time passwords* vienen a ser una solución factible para ello. Teniendo en cuenta que normalmente en este tipo de redes intervienen clientes inalámbricos, se han venido desarrollando una serie de protocolos basándose en operaciones criptográficas ligeras, como es el caso del protocolo analizado en este trabajo. Estas operaciones usadas son preferentemente las operaciones *hash* y *XOR*. Las *cadenas de hash* han sido el mecanismo preferido en ente tipo de esquemas, sin embargo, suelen implicar un alto número de operaciones para, al menos, una de las partes involucradas, lo cual atenta contra la eficiencia computacional. Teniendo en cuenta que los protocolos de seguridad son bastante sutiles, cualquier protocolo planteado debe ser sometido a una extensa revisión y análisis en busca de vulnerabilidades. En el presente trabajo no sólo se analizan algunas vulnerabilidades del protocolo de *Vaidya et al,* sino que se proponen mejoras al mismo tanto para resolver las vulnerabilidades de seguridad como para mejorar la eficiencia computacional del mismo.
PALABRAS CLAVES:autenticación robusta, cadenas de hash, tarjetas inteligentes, *one time passwords*, redes digitales en el hogar.

ABSTRACT

In this paper, an analysis of the security of a robust authentication protocol using smart cards for digital home networks, proposed by Vaidya et al.. This type of network has been growing for comfort applications and remote medical care and more. In these sensitive environments, cannot always guarantee the security of the communication channels, so that alternatives are needed to provide a high level of security. The current strong authentication mechanisms using one time passwords come to be a feasible solution for this. Since normally involved such networks wireless clients, have been developing a series of protocols based on lightweight cryptographic operations, such as protocol analyzed in this paper. These operations are preferably used hash and XOR operations. Hash chains have been the

preferred mechanism being such schemes, however, often involve a high number of operations for at least one of the parties involved, which hampers the computational efficiency. Given that security protocols are quite subtle, any proposed protocol shall be subjected to an extensive review and analysis for vulnerabilities. This paper not only discusses some protocol vulnerabilities Vaidya et al, but at the same improvements are proposed to solve both security vulnerabilities and to improve the computational efficiency of the same.

KEYWORDS: strong authentication, hash chains, smart cards, one time passwords, digital home networks.

INTRODUCCIÓN

El desarrollo que se ha alcanzado en la protección de la información hoy en día, no hubiera sido posible sin el uso indispensable de la Criptografía. En la actualidad se han logrado enormes avances en esta rama de las ciencias, haciendo uso de bases matemáticas y los enromes avances tecnológicos existentes. El acelerado avance de las tecnologías ha permitido diversas estrategias para la protección de la información y la seguridad informática. Sin embargo aunque en la actualidad la información se puede proteger mucho mejor de aquellos que carecen de conocimientos suficientes o no disponen de los recursos apropiados para romper los métodos de protección debemos darnos cuenta de que la tecnología existe y se desarrolla tanto para quienes necesitan proteger la información, como para aquellos que pretenden romper los mecanismos de seguridad existentes. De este modo, podríamos decir que este tema ha sido y será siempre, una lucha incesable entre aquellos que trabajan en función de crear nuevos mecanismos y estrategias para la protección de la información, y aquellos que se esfuerzan por buscar sus vulnerabilidades y tratan de violar los mismos, con el respaldo de una tecnología equivalente.

Debido al crecimiento exponencial de los usuarios de Internet, y los dispositivos inalámbricos conectados en todo momento a la gran red de redes, la computación ubicua ha tomado un papel importante en el progreso de las tecnologías y las redes de hoy día. Las redes domésticas avanzadas permiten conectividad a los usuarios del hogar a través de Internet, para el acceso y el control de dispositivos digitales interconectados entre sí y asociados a la vida en el hogar.

De este modo, las redes digitales en el hogar son una de las tecnologías representativas del fenómeno de la computación ubicua. Este tipo de redes se dedican fundamentalmente al confort, ocio y cuidado de la salud de los moradores del hogar; aunque también han sido validadas para proteger lugares y para optimizar procesos como el consumo de energía. Aún cuando las redes digitales proveen conveniencias a los usuarios residenciales, proveyendo servicios de valor agregado; las características heterogéneas de las mismas, y lo delicado del ambiente, hacen que resulte un desafío importante la protección de la privacidad y confidencialidad de la información que se transmite. En la mayoría de los casos es deseable que los usuarios legítimos puedan realizar el acceso remoto a distintos servicios que estas redes brindan. Sin embargo, a no ser que estas redes estén bien protegidas, usuarios ilegítimos podrían conseguir acceso a estos servicios, poniendo en riesgo la seguridad del hogar.

Así, la autenticación de usuarios es uno de los mecanismos de seguridad más importantes requeridos en las redes digitales para el hogar, el cual ha generado creciente interés de la comunidad científica. Los mecanismos de autenticación robusta actualmente existentes, en particular los mecanismos de autenticación mediante doble factor, vienen a proporcionar una solución viable para la seguridad de las redes digitales en el hogar. A pesar de ello la sutileza que implican los protocolos de seguridad informática requiere la constante revisión y perfeccionamiento de los mecanismos que se van planteando, a fin de cumplir cada vez mejor las exigencias de seguridad de cada momento.

Los métodos de autenticación robusta para el acceso remoto han sido extensamente desarrollados; y la autenticación por medio de contraseñas sigue siendo visto como uno de los métodos más simples y

convenientes, por sus notables beneficios en cuanto al costo de implementación y su facilidad de uso. Para prevenir los ataques que se basan en la interceptación de información transmitida por la red (eavesdroping attack), muchos de los esquemas de autenticación modernos se han basado en las contraseñas de una sola vez (One Time Passwords - OTPs). Las contraseñas de una sola vez, en combinación con las tarjetas inteligentes, son una de las formas más simples y populares de autenticación de doble factor para el acceso seguro a las redes. Este tipo de soluciones ha sido ampliamente adoptado debido a su bajo costo computacional y su conveniente portabilidad.

Dada la creciente presencia de los dispositivos inalámbricos en las redes, para los cuales es importante el ahorro de consumo energético, se ha generado una tendencia a producir protocolos más ligeros para los entornos en los que puedan intervenir este tipo de equipos. Actualmente existen mecanismos bastante eficientes y seguros de OTPs, como lo son el HOTP y otros, que se pueden aplicar en estos escenarios.

A pesar de las ventajas de estos esquemas, investigaciones tales como [2] y[3], indican que algunos métodos sofisticados pueden extraer secretos y valores de verificación de las tarjetas inteligentes. Por lo tanto, la debilidad de los esquemas de autenticación usando tarjetas inteligentes se debe fundamentalmente al hecho de que la información guardada en dicha tarjeta puede ser utilizada por un adversario para construir un mensaje válido de autenticación que le permita acceder ilegalmente al sistema, suplantando al usuario legítimo, aun sin el conocimiento de la contraseña. Esta es una problemática que no tiene una solución sencilla. Sin embargo, recientemente Vaidya et al. [1] han propuesto un esquema de autenticación robusta para redes residenciales usando tarjetas inteligentes, basado en el algoritmo HOTP. En el protocolo propuesto, los autores han evitado la sincronización de tiempo y el uso de verificadores de contraseña en el servidor de autenticación. Estos afirman además que, a diferencia de los anteriores, el protocolo es seguro contra ataques con robo de la tarjeta inteligente. Este esquema planteado incurre en costos computacionales algo más elevados que esquemas precedentes, para brindar más seguridad.

El objetivo de este trabajo es mostrar cómo el esquema de Vaidya et al. es inseguro contra ataques de verificación de contraseñas (password guessing) con pérdida de la tarjeta inteligente, y proponer modificaciones al mismo para solucionar esta vulnerabilidad. Además de ello, proponemos modificaciones a la fase de solicitud de acceso al servicio con el objetivo de mejorar el rendimiento computacional del protocolo. También identificamos otras posibles vulnerabilidades del protocolo mencionado que por el momento no serán resueltas en este trabajo.

Breve preámbulo teórico

En esta sección presentamos brevemente algunos elementos básicos, importantes para la mejor compresión de los planteamientos y análisis que se realizan en el presente trabajo. Estos son: la arquitectura de red sobre la cual se soporta el esquema de autenticación robusta objetivo de estudio; y el algoritmo HOTP, en el cual se basa el protocolo que responde al esquema, del cual depende en parte la seguridad y el rendimiento del mismo.

Arquitectura de red de las redes digitales para el hogar.

Las redes digitales para el hogar constituyen un nuevo paradigma de redes de área local, que permite la integración de diferentes servicios asociados con dispositivos y equipos del hogar, usando un sistema

común de comunicaciones. Las mismas están orientadas a proporcionar beneficios desde los puntos de vista del confort, la operatividad de funciones del hogar, el consumo energético, la seguridad, entre otros, con un alto grado de funcionalidad [4]. Estas redes permiten a sus usuarios realizar acceso remoto utilizando algún dispositivo personal para controlar sus aparatos electrodomésticos, o acceder a recursos de almacenamiento disponibles en una red personal. Así por ejemplo, una persona ocupada podrá ejecutar ciertas tareas sin tener que esperar a llegar a su casa [5]. Una red digital típica para el hogar, contiene un punto de acceso a la red (home gateway), electrodomésticos, ordenadores, dispositivos móviles, un servidor remoto de autenticación (IAS) y un proveedor de servicios (ver Figura 1). Dispositivos inalámbricos y móviles son utilizados por los usuarios residenciales, para conectarse al punto de acceso de la red y controlar los aparatos electrodomésticos.

El punto de acceso a la red digital en el hogar (HG) desempeña un papel esencial en la estructura y la seguridad de la red. Por un lado, proporciona conectividad interna a los diferentes terminales de red en el hogar, interconecta con la red pública y las subredes de la red doméstica, e implementa la administración remota. Por otro lado, permite a los usuarios utilizar los servicios de valor añadido brindados por los proveedores de servicios de Internet. También proporciona funciones de los servicios de seguridad, así como a la autenticación de usuarios para el acceso a los servicios de la red digital.

En la mayoría de las aplicaciones de redes digitales para el hogar existe un servidor de autenticación integrado (IAS) fuera de la red doméstica, que administra algunas funciones del punto de acceso, autentica a los usuarios, otorga privilegios, y ofrece controles de contabilidad. Por último, el proveedor de servicios puede suministrar muchas clases de servicios, de valor añadido a la red digital para el disfrute de los usuarios. La figura.1 muestra la arquitectura general de las redes domésticas.

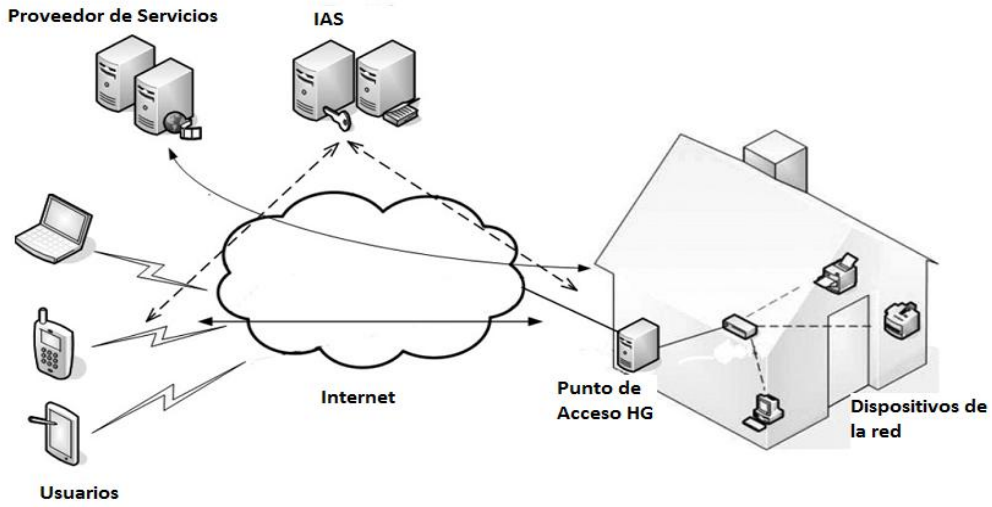

Figura 1: Arquitectura de una red digital en el hogar, (adaptada de [1]).

HOTP: algoritmo de one-time password basado en HMAC

HOTP es un algoritmo de bajo costo para la generación de OTPs, basado en HMAC, que ha sido propuesto por la OATH (initiative for Open AuTHentication). El mismo se encuentra descrito en el RCF

4226 del IETF [6]. Sus características convenientes han provocado que este sea últimamente bastante usado en los protocolos actuales de autenticación robusta.

Se basa en un contador ascendente y una clave simétrica para la generación de los valores OTP. El contador es usado en sustitución del mensaje correspondiente en el algoritmo HMAC, mientras que la clave simétrica es conocida solo para el cliente y el servidor implicados. Normalmente la función hash segura SHA-1 es usada para obtener los valores del algoritmo HMAC, pero esta podría ser reemplazada por cualquier otra función hash con requerimientos de seguridad mejores, en caso de que exista una disponible y sea deseable.

Al algoritmo opera de la siguiente forma. Inicialmente, la función generadora de SHA-1 es inicializada a partir del secreto compartido. A continuación, se calcula el valor hash del contador y se le aplica un truncamiento dinámico para extraer solo ciertos bytes de esta cadena de salida del HMAC. Finalmente de esta cadena resultante se extrae el resto módulo, donde es el número de dígitos deseados en el resultado final, para ser usados como OTP. El proceso de cálculo indicado puede ser expresado por medio de la fórmula:

$$HOTP(K, C) = Trunc\big(HMAC - SHA1(K, C)\big)_n$$

donde representa la función de truncamiento que convierte la salida de $HMAC - SHA1$ en un valor de OTP; mientras K y C representan la clave secreta compartida y el contador ascendente respectivamente.Para el correcto funcionamiento del algoritmo, tanto el cliente como el servidor involucrados en este deben generar el mismo valor de OTP, partiendo del hecho de que ambos mantengan el mismo valor del contador de forma sincronizada.

TRABAJOS RELACIONADOS

El primer esquema de autenticación mediante contraseñas de un solo uso (OTPs) fue inicialmente introducido por Lamport [7] a través de la idea de las cadenas de hash. A partir de entonces los mecanismos basados en OTPs se ha convertido en uno de los métodos más ampliamente usados en la autenticación robusta. Dos de los principales objetivos de seguridad que se persiguen con el uso de OTPs son el brindar protección contra los ataques de eavesdropping y replay attack. La evolución de este tipo de métodos ha conducido a esquemas cada vez más sofisticados, que requieren la utilización de algún dispositivo con cierta capacidad de almacenamiento que sea capaz de realizar operaciones criptográficas. Así se obtiene lo que es llamado autenticación robusta de doble factor, donde son necesarios dos factores distintos para realizar la autenticación en un entorno dado; en este caso algo conocido como puede ser una contraseña o un número PIN, y una posesión con características particulares. Uno de los dispositivos más factibles para este tipo de uso son las tarjetas inteligentes, por su bajo costo y fácil portabilidad. El hecho de que estas tarjetas puedan ser dedicadas al manejo de credenciales de autenticación e información de usuario, y no estén siempre conectadas a una red, puede verse como una ventaja desde el punto de vista de la seguridad informática. Debido a ello, los esquemas de autenticación remota de usuarios basados en contraseñas usando tarjetas inteligentes han sido ampliamente desarrollados, [8-10]. En muchos de los casos se suelen almacenar parámetros de autenticación o verificadores de contraseña por parte del servidor de autenticación y/o en la tarjeta inteligente entregada al usuario.

El primer mecanismo en darle uso exitoso a la idea de las contraseñas de una sola vez basadas en cadenas hash fue el S/KEY [11]. Luego, en el 2002, Yeh et al. [12] propusieron un esquema de autenticación mediante OTPs usando tarjetas inteligentes, que constituye una mejora del mecanismo S/KEY. Este incorpora un desafío en forma de número aleatorio para proporcionar autenticación mutua y ofrecer así protección contra ataques de tipo server spoofing. Sin embargo Tsuji y Shimizu [13] luego demostraron que este esquema es vulnerable a ataques con robo de verificador (stolen-verifier attacks). En el 2005, Lee y Chen [14] propusieron una mejoría al mecanismo de Yeh el al. para soportar este tipo de ataques sin degradar la eficiencia del mecanismo original.

Este tipo de esquemas de autenticación comienza entonces a ser introducido en los modelos de redes residenciales como mecanismos para el control de acceso. Jo y Youn [15] propusieron un protocolo seguro de autenticación para redes residenciales que emplea un mecanismo three-way challenge-response handshake para lograr autenticación mutua. You y Jung propusieron un protocolo ligero de autenticación para redes digitales en el hogar, basado en el esquema de Lee-Chen [14]. Las mejoras añadidas en este protocolo, permiten resistir un tipo de ataque sofisticado denominado “the compromise of pass session keys via stolen passwords”. Jeong et al. propusieron un esquema de autenticación de usuarios basado en OTPs usando tarjetas inteligentes, para redes residenciales [16], el cual ofrece protección contra el acceso ilegal a los servicios de estas redes y limita el acceso innecesario de usuarios legítimos a los servicios de la red. Sin embargo, en este esquema el servidor almacena un verificador de la contraseña, y es susceptible a ataques de enmascaramiento (masquerading attack) si el adversario se hace con el verificador. Kim y Chung en [17] han propuesto modificaciones al esquema de Yoon y Yoo [18] que brinda protección contra la fuga de contraseñas y ataques de suplantación de identidad; por sobre los beneficios del esquema de Yoon y Yoo. A pesar de todos los esfuerzos hasta este punto, estos esquemas aún poseen una serie de fallas de seguridad, incluyendo el hecho de que son vulnerables contra los ataques con robo de la tarjeta inteligente.

Recientemente Vaidya et al. propusieron recientemente un esquema de autenticación de usuarios basado en contraseñas fuertes para proveer acceso remoto seguro en el escenario de las redes digitales en el hogar; el cual usa el mecanismo de OTP basado en HMAC, conocido como HOTP, y la técnica de las cadenas de hash, junto con una tarjeta inteligente. Dicho esquema está concebido no solo para resistir los ataques con pérdida de la tarjeta inteligente, sino además para proporcionar autenticación mutua, evitar la sincronización basada en tiempo y descartar el uso de verificadores de contraseña en el servidor remoto.

En el artículo que introduce dicho esquema se realiza una verificación formal del mismo y un análisis en función de la seguridad y los requerimientos funcionales del esquema. A pesar de ello,Kim et al. muestran en [19] que el protocolo planteado por Vaidya et al. es inseguro contra la verificación de contraseñas con pérdida de la tarjeta inteligente y que este tampoco cumple la propiedad de forward secrecy con pérdida de la tarjeta. Kim et al. proponen modificaciones al protocolo de Vaidya et al. para resolver estas dos vulnerabilidades; sin embargo no queda claro que la segunda de estas se resuelva con su propuesta, la cual además incrementa ligeramente el costo computacional del protocolo original, que ya era notablemente costoso para este tipo de escenarios donde participan dispositivos inalámbricos.

Descripción general del Protocolo de Vaidya et al.

Como se vio en la arquitectura de red, en este esquema intervienen tres tipos de entes principales: el/los cliente/s, un punto de acceso a la red residencial (Home Gateway - HG) y un servidor de autenticación (IAS). Este último funciona como una tercera parte de confianza para los dos primeros entes. El mismo se encargará de manejar permisos de inicio de sesión para que los usuarios puedan acceder a los servicios de la red en el hogar a través del HG; a su vez IAS mantendrá una clave secreta compartida con el HG.

El protocolo propuesto por Vaidya et al. para este esquema, consiste en cuatro fases en su totalidad: fase de registro, fase de autenticación e inicio de sesión, fase de solicitud de servicios y fase de cambio de contraseña.Durante la fase de registro el usuario escoge su propia contraseña y recibe su tarjeta inteligenteSC. En la etapa de autenticación e inicio de sesión se realiza una autenticación mutua entre el servidor y el cliente basándose en el algoritmo HOTP. En esta etapa el usuario y el servidor acuerdan una clave de sesión única para cada vez. El servidor IAS le otorga al usuario, un tiqueteTKG para autenticarse con el HG y acceder a los servicios de la red. Los mensajes intercambiados en el último paso de inicio de sesión y el primer paso de la solicitud de servicios, se envían encriptados usando cifrado de clave simétrica.

Hay tres secretos fijos, los cuales constituyen la base de la seguridad del protocolo, en conjunto con la tarjeta inteligente. Estos son: la contraseña de usuario PW, una clave secreta “x” del servidor IAS y una clave secreta K compartida entre el servidor IAS y el cliente U. La clave secreta compartida K no es almacenada por ninguno de los que intervienen en el proceso. El cliente U es autenticado sobre la base de su tarjeta inteligente y su contraseña PW. El dispositivo del usuario U puede obtener K a partir del valor correcto de PW y unos valores criptográficos almacenados en su tarjeta SC. El servidor IAS puede obtener K a partir de su clave secreta “x” y dos valores enviados por el cliente.

Existe un mecanismo de sincronía U-IAS: un contador ascendente controla los valores generados por el algoritmo HOTP. Los valores de HOTP dependen de K y PW, y se usan para: autenticar al usuario U en el primera inicio de sesión, y obtener una clave para dicha sesión combinando el valor de HOTP con un número aleatorio generado por IAS.

La clave de sesión es utilizada para cifrar la respuesta de autenticación (AuthResp) de IAS y le permite al servidor autenticarse con U. Durante el último paso de la fase de inicio de inicio de sesión, el usuario recibe un tiquete (TKG) para el proceso de autenticación mutua con HG y el acceso a los servicios.TKG está encriptado usando una clave secreta pre-compartida entre IAS y HG. Este tiquete TKG es enviado por el usuario al HG en la fase inicial de solicitud de servicios. Tanto AuthResp como TKG contienen información simétrica compartida por U y HG para inicializar y recorrer la cadena de hash que usarán para la autenticación mutua. Cada sesión tiene un tiempo de expiración , después del cual es necesario volver a la fase de inicio de sesión para recibir una clave de sesión y un tiquete nuevo para acceder nuevamente a los servicios de la red.

El proceso de autenticación mutua U-HG para el acceso a servicios se realiza usando el esquema tradicional de las cadenas de hash y un valor criptográfico que depende de la clave de sesión y un contador descendente. La cadena de hash es computada a un valor que depende de la clave de sesión y una semilla aleatoria compartida entre U y HG.

Desglose detallado del Protocolo de Vaidya et al.

A continuación se muestra el protocolo de Vaidya et al. [1] de forma detallada, con el objetivo de poder analizar posteriormente los pasos que conducen a vulnerabilidades y que ello permita proponer modificaciones válidas para mejorarlo.

Tabla 1: Aclaración de las notaciones usadas en el esquema de Vaidya et al.

Símbolo	Descripción
ID_c	*Identificador del usuario*
ID_{IAS}	*Identificador del servidor IAS*
ID_{SC}	*Identificador de la tarjeta inteligente (SC)*
PW	*Contraseña de usuario*
x	*Clave secreta mantenida por*
$F(\cdot), h(\cdot)$	*Funciones hash seguras*
$F^n(S)$	*Función hash anidada n-veces aplicada a S*
$H^i(K,C)$	*i-ésimo valor de HOTP con los parámetros K y C*
C_X	*Contador de 8-bytes, factor de cambio (moving factor)* $X = C$ *– cliente,* S *– servidor,* M *– máximo permitido*
K	*Secreto compartido entre el cliente y el servidor*
K_i, S_K	*Claves de sesión*
K_{IAS-HG}	*Clave simétrica entre IAS y HG*
N	*Número de accesos permitidos*
S	*Semilla aleatoria*
$E_{K_X}(M)$	*Cifrado simétrico con la clave* K_X
T_{exp}	*Tiempo de expiración para el tiquete de autenticación*
$\oplus$	*Operación XOR*
$\|$	*Operación de concatenación*

Fase de Registro - R:

Paso R1. U escoge los valores ID_C y PW, y los envía a al servidor IAS por un canal seguro de comunicaciones.

Paso R2. IAS realiza las siguientes operaciones:

Genera un secreto K

Calcula $\begin{cases} v_T = h\,(ID_c \oplus x)\ \oplus h(PW)\ \oplus K \\ g_T = h(ID_c \parallel x \parallel K) \oplus h(ID_c \parallel PW) \\ k_T = K \oplus H\big(PW \oplus H(PW)\big) \end{cases}$

Almacena ID_c e ID_{sc} en su base de datos de usuarios

Escribe $\{ID_c, ID_{SC}, h(\cdot), v_T, g_T, k_T, C_M\}$ en la tarjeta inteligente

Paso R3. La autoridad en cargada del IAS hace llegar la tarjeta inteligente SC al usuario U por una vía segura.

Fase de Autenticación e Inicio de Sesión - LA:

Paso LA1. El usuario U su tarjeta inteligente en su terminal o en un lector asociado a su dispositivo personal, e ingresa los valores ID_C y PW .

Paso LA2. La tarjeta SC actúa del siguiente modo:

Verifica ID_C. Si ID_C es idéntico al ID_C almacenado por la tarjeta SC , ésta continuará con el procedimiento para iniciar sesión; de lo contrario, el proceso se interrumpirá.

Obtiene los valores $\begin{cases} K = k_T \oplus h\big(PW \oplus h(PW)\big) \\ h\,(ID_c \oplus x) = v_T \oplus h(PW) \oplus K \end{cases}$

Calcula $\begin{cases} u_1 = h(PW \oplus h(PW)) \oplus K \\ u_2 = h(ID_c \oplus x) \oplus h(ID_c \parallel PW) \oplus h(K) \end{cases}$

Genera el valor actual de $HOTP\ H^i(K, C_C) = HOTP(K, C_C, h(ID_c \parallel PW))$

Incrementa su contador en $C_C \coloneqq C_C + 1$

Calcula $G = h\big(u_T \oplus g_T\big) \oplus H^i(K, C_C)$

Paso LA3. U le envía $\{ID_C, u_T, a_T, G\}$ al servidor IAS

Paso LA4. IAS procede de la siguiente manera al recibo de la información:

Verifica ID_C . Si ID_C no es un identificador de usuario válido, esta continuará con el procedimiento la verificación de identidad y autenticación, de lo contrario, la solicitud de inicio de sesión será rechazada.

Obtiene $\begin{cases} K = u_T \oplus h(ID_c \oplus x) \\ h(ID_C \parallel PW) = a_T \oplus h(ID_{SC} \parallel K) \end{cases}$

Calcula $g_T^{'} = h(ID_c \parallel x \parallel K) \oplus h(ID_c \parallel PW)$

Obtiene $H^i(K, C_C) = h(u_T \oplus g_T^{'}) \oplus G$

Genera $HOTP\ H^i(K, C_S) = HOTP(K, C_S, h(ID_c \parallel PW))$

Compara los valores $H^i(K, C_C) = H^i(K, C_S)$ y si estos coinciden, entonces IAS incrementa su contador $C_S \coloneqq C_S + 1$

Obtiene $K_i = H^i(K, C_S)$

Genera un número aleatorio Na y con el calcula $S_K = h(K_i \parallel N_a)$

Calcula $A_S = h(S_K \parallel ID_C)$

Cifra $E_{K_i}(ID_C, ID_{IAS}, N_a, A_S, N, S)$, $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, N_a, K_i, N, S, T_{exp})$

Paso LA5. IAS envía una respuesta de autenticación $AuthResp = E_{K_i}(ID_C, ID_{IAS}, N_a, A_S, N, S)$ y un tiquete de autenticación $TKG = E_{K_{IAS-HG}}(ID_C, ID_{IAS}, N_a, K_i, N, S, T_{exp})$, al usuario U.

Paso LA6. U opera de la siguiente forma:

Descifra $E_{K_i}(ID_C, ID_{IAS}, N_a, A_S, N, S)$ usando$K_i^{'} = H^i(K, C_C)$

Obtiene $S_K^{'} = h(K_i^{'} \| N_a)$

Calcula $A_S^{'} = h(S_K^{'} \| ID_C)$

Finalmente chequea si $A_S - A_S^{'}$, en caso de que coincidan da por válido el $AuthResp$ y autentica positivamente al servidor IAS.

Para acceder a los servicios de la red, los usuarios una vez autenticados pueden solicitarlos al punto de acceso HG,. lo que se describe a continuación.

Fase de Solicitud de Acceso al Servicio - SR:

Paso SR1. El usuario U calcula el valor de OTP inicial $P_0 = F^N(S_K \oplus S)$ de una cadena de hash y lo almacena para su uso posterior.

Paso SR2. Cuando el usuario requiere acceder a servicios dentro de la red digital en el hogar, éste envía al punto de acceso HG el par de valores $ID_C, E_{K_{IAS-HG}}(ID_C, ID_{IAS}, N_a, K_i, N, S, T_{exp})$

Paso SR3. Al recibir el par de valores de la solicitud el punto de acceso HG actúa del siguiente modo:

Descifra $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, N_a, K_i, N, S, T_{exp})$ usando la clave K_{IAS-HG}

Verifica el valor IDc recibido con el valor obtenido al descifrar el TKG si estos coinciden continúa con el procedimiento; de lo contrario, niega de inmediato el acceso al servicio.

Verifica T_{exp} para ver si ha expirado la sesión

Obtiene $S_K = h(K_i \| N_a)$, lo cual es realizado solo una vez por sesión

Calcula $P_0 = F^N(S_K \oplus S)$

Inicializa un contador decreciente C:=N, si es la primera solicitud de la sesión y en otro caso, sólo disminuye su valor actual en 1,C:=C -1

Calcula $R = h(S \oplus C \oplus S_K))$ y $PP = P_0 \oplus h(S_K)$

Paso SR4. HG envía los valores C,R,PP al usuario U para ser autenticado por éste

Paso SR5. El usuario U realiza las siguientes operaciones:

Calcula $R' = h(S \oplus C \oplus S_K)$ y $PP^{'} = P_0 \oplus h(S_K)$

Verifica que se cumpla $R^{'} = R$, $PP^{'} = PP$ y si estos pares de valores coinciden procede a

calcular $P_i = F^{(N-i)}(S_K \oplus S)$, en la *i-ésima* solicitud de servicios

Guarda el valor de C

Reemplaza P_{i-1} por P_i

Paso SR6. U le envía

Paso SR7. HG actúa como sigue:

Obtiene P_i del mensaje recibido

Verifica que se cumple $F(P_i) = F\left(F^{(N-i)}(S_K \oplus S)\right) = F^{(N-i+1)}(S_K \oplus S) = P_{i-1}$

Si finalmente es cierto que $F(P_i) = P_{i-1}$, HG reemplaza P_{i-1} por P_i y da acceso al usuario U al servicio solicitado.

Dado que la fase cambio de contraseña no es objetivo de análisis en este trabajo, no la incluiremos en este desarrollo. En la misma se utiliza un procedimiento parecido al de la fase de inicio de sesión, en el cual se le exige al usuario que entre su identificador, su contraseña actual y la nueva contraseña, una vez introducida la tarjeta inteligente en su terminal. Sobre la base de la contraseña actual, se realiza un proceso de autenticación mutua entre el usuario y el servidor IAS y luego se usa la contraseña nueva para actualizar los valores existentes en la tarjeta inteligente en base a esta contraseña.

Análisis de la seguridad y funcionalidad del protocolo de vaidya

Análisis de seguridad del protocolo

Los autores de [1] afirman que el protocolo es resistente a una lista considerable de ataques, entre ellos algunos sofisticados. Aunque en el trabajo donde es planteado el protocolo se realiza una verificación formal del mismo, esto se hace sobre la base de una ejecución exitosa del protocolo, lo cual no constituye una prueba exhaustiva que permita descartar las innumerables formas en que un adversario pueda intervenir con éxito en dicho protocolo.

Para un breve análisis de seguridad del esquema en cuestión se debe establecer con qué tipo de atacantes se supone que se va a lidiar. En estos casos es realista y conveniente asumir que el atacante tiene el control sobre los canales de comunicación, por lo que puede interceptar todo tipo de mensajes en cualquier dirección, y que puede modificar cualquier mensaje recibido e intentar establecer comunicaciones con cualquiera de las partes. Bajo estos supuestos, Kim et al. han probado en [19], que el protocolo planteado por Vaidya et al. es inseguro contra la verificación de contraseñas con pérdida de la tarjeta inteligente (password guessing attack with lost smart card) y no cumple la propiedad de forward secrecycon pérdida de la tarjeta inteligente.

Verificación de contraseñas con pérdida de la tarjeta inteligente: Este ataque consiste en tratar de obtener la contraseña de un usuario de un sistema, a partir de información almacenada en la tarjeta inteligente, y haciendo uso de cualquier tipo de información recopilada por el atacante, que haya sido capturada por él durante las comunicaciones entre las partes principales del protocolo. Este tipo de ataque suele llevarse a cabo probando posibles valores de contraseñas de una lista dada como puede ser un diccionario.

Ataque de verificación de contraseñas con pérdida de la tarjeta inteligente contra Vaidya et al.:

Paso1: El atacante intercepta los mensajes de una sesión del usuario durante la fase de autenticación e inicio de sesión y logra hacerse con la tarjeta inteligente del usuario de forma ilegal.

Paso2: El atacante ha almacenado el valor fijo $u_T = K \oplus h(ID_c \oplus x)$ obtenido de las comunicaciones interceptadas y logra extraer el valor $v_T = h\,(ID_c \oplus x)\ \oplus h(PW)\ \oplus K$ almacenado en la tarjeta inteligente.

Paso3: El atacante escoge una contraseña candidata PW' de un diccionario y procede a calcular $u'_T = v_T \oplus h(PW') = h\,(ID_c \oplus x)\ \oplus h(PW)\ \oplus K \oplus h(PW') = h\,(ID_c \oplus x) \oplus K \oplus h(PW) \oplus h(PW')$. Nótese que se cumple $u'_T = u_T \iff h(PW) \oplus h(PW')$por lo que, de cumplirse esta igualdad el atacante sabrá que habrá encontrado la contraseña, ya que la función hash usada $h(\cdot)$ es una función segura y de ser $PW' \neq PW$ se habría encontrado una colisión.

Paso4: Si el valor u'_T calculado con la contraseña candidata no coincide con el valor u_T original, el atacante repite el proceso con otro valor del diccionario hasta encontrar la contraseña correcta o agotar el diccionario completo.

Kim et al. [19] resuelven el problema introduciendo una valor adicional $\boldsymbol{K_n} = \boldsymbol{K} \oplus h(K)$ y cambiando el valor de u_T original por $u_T = \boldsymbol{K_n} \oplus\ h(ID_c \oplus x)$. Además de ello, introducen otras operaciones basadas en la teoría de cuerpos algebraicos y en la irreversibilidad computacional del logaritmo discreto, para intentar dotar su propuesta de la propiedad de forward secrecy con pérdida de la tarjeta inteligente, que como ellos mismos prueban, no se cumple en el protocolo de Vaidya et al. Esta última propiedad brinda protección contra el comprometimiento de claves de sesión, en caso de que el atacante tenga en su posesión la tarjeta inteligente y además conozca la clave secreta privada del servidor remoto. Estas exigencias son bastante altas, y los ataques que rompen la propiedad mencionada son inusuales, por lo que ello requiere del adversario. El protocolo propuesto por Kim et al. [19] incurre en costos adicionales de comunicación y cómputo, por encima del protocolo de Vaidya et al. con tal de resolver estas dos vulnerabilidades.

Análisis de funcionalidad del protocolo.

El protocolo propuesto por Vaidya et al. [1] es bastante funcional, ya que posee las siguientes características: la contraseña es de elección libre por parte del usuario, no se almacena una tabla de verificación de contraseñas en el servidor remoto, no se usa sincronización de tiempo, provee autenticación mutua en todas las etapas, se usa una clave de sesión única para cada vez y existe un proceso de cambio de contraseña con autenticación mutua.

A pesar de todo ello, el protocolo incurre en mayor costo computacional que los esquemas representativos anteriores. En el artículo [1] los autores comparan el costo computacional con otros tres esquemas representativos [15],[16] y [17], pero no incluyen las operaciones hash como resultado de

recorrer la cadena de hash usada en la fase de solicitud de acceso a los servicios. Esta cadena de hash se recorre en orden descendiente de la cantidad de hash anidados, por lo que se incurre, al comienzo de la fase, en un mayor número de operaciones. En esta parte hemos visto una oportunidad para reemplazar esta cadena de hash por otro mecanismo que abarate el costo computacional del esquema en su totalidad, sin sacrificar la seguridad del mismo.

El Protocolo modificado

En esta sección se presentan modificaciones el protocolo de Vaidya et al. [1]. Los cabios introducidos tienen el objetivo de simplificar ligeramente la complejidad del protocolo, resolver la vulnerabilidad al ataque de verificación de contraseñas con pérdida de la tarjeta inteligente y mejorar el rendimiento computacional de protocolos en la fase de solicitud de acceso al servicio, sin sacrificar en absoluto la seguridad inicialmente brindada por el mismo.

Fase de Registro modificada

Paso R1. $\boxed{\text{U}}$ escoge ID_C , PW y se lo envía y se lo envía a $\boxed{\text{IAS}}$ por una vía segura.

Paso R2.$\boxed{\text{IAS}}$ realiza las siguientes operaciones:

Genera un secreto K

Calcula$\begin{cases} u_1 = h\big(PW \oplus h(PW)\big) \oplus K \\ u_2 = h(ID_C \oplus X) \oplus h\big(ID_C \parallel PW \oplus h(K)\big) \end{cases}$

Almacena ID_C , ID_{SC}

Escribe$\{ID_C,\ ID_{SC},\ h(\cdot),\ u_1, u_2, C_M\}$en la $\boxed{SC}$

Paso R3. La autoridad en cargada del $\boxed{\text{IAS}}$ hace llegar la tarjeta inteligente SC al usuario $\boxed{U}$ por una vía segura

Fase de Autenticación e Inicio de Sesión Modificada

Paso LA1. El usuario $\boxed{U}$ inserta su tarjeta inteligente en su terminal o en un lector asociado a su dispositivo personal, e ingresa los valores ID_C y PW.

Paso LA2. La tarjeta $\boxed{SC}$ actúa del siguiente modo:

Verifica ID_C. Si ID_C es idéntico al ID_C almacenado por la tarjeta $\boxed{SC}$, esta continuará con el procedimiento para iniciar sesión, de lo contrario el proceso se interrumpirá.

Obtiene los valores$\begin{cases} K = h\big(PW \oplus h(PW)\big) \oplus u_1 \\ h(ID_C \oplus X) = h(K \oplus h(ID_C \parallel PW) \oplus u_2 \end{cases}$

Calcula $\begin{cases} s_1 = K \oplus h(ID_C \oplus X) \\ s_2 = h(ID_C \parallel PW) \oplus h(ID_{SC}) \parallel K) \end{cases}$

Genera el valor actual de $HOTP\ H^i(K, C_C) = HOTP\big(K, C_C, h(ID_c \parallel PW)\big)$

Incrementa su contador en 1: $C_C \coloneqq C_C + 1$

Calcula $G = h(u_2 \parallel s_2) \oplus H^i(K, C_C)$

Paso LA3. $\boxed{U}$ le envía $\{ID_C, s_1, s_2, G\}$ al servidor $\boxed{\text{IAS}}$

Paso LA4. IAS procede de la siguiente manera al recibo de las información:

Verifica ID_C. Si ID_C no es un identificador de usuario válido, esta continuará con el procedimiento la verificación de identidad y autenticación, de lo contrario, la solicitud de inicio de sesión será rechazada.

Obtiene $\begin{cases} K = h(ID_C \oplus x) \oplus s_1 \\ h(ID_C \parallel PW) = s_2 \oplus h(ID_{SC} \parallel K) \end{cases}$

Calcula $u_2 = h(ID_C \oplus x) \oplus h(ID_C \parallel K) \oplus h(K)$

Obtiene $H^i(K, C_C) = h(u_2 \parallel s_2) \oplus G$

Genera $HOTP\ H^i(K, C_S) = HOTP\big(K, C_S, h(ID_c \parallel PW)\big)$

Compara los valores $H^i(K, C_C) = H^i(K, C_S)$, y si estos coinciden entonces $\boxed{\text{IAS}}$ incrementa su contador $C_S \coloneqq C_S + 1$

Obtiene $K_i = H^i(K, C_S)$

Genera dos números aleatorios S y E_1

Calcula $S_{k_i} = h(K_i \oplus S)$

Cifra $\begin{cases} E_{K_{IAS-HG}}\big(ID_C, ID_{IAS}, S_{k_i}, E_1, N, T_{exp}\big) = TKG \\ E_{K_i}(ID_C, ID_{IAS}, h(TKG), E_1) = AuthResp \end{cases}$

Paso LA5. $\boxed{\text{IAS}}$ envía una respuesta de autenticación $AuthResp$ y un hash del tiquete de autenticación TKG al usuario $\boxed{U}$.

Paso LA6. $\boxed{U}$ opera de la siguiente forma:

Descifra $E_{K_i}(ID_C, ID_{IAS}, h(TKG), E_1)$ usando $K_i^{'} = H^i(K, C_C)$

Calcula $h(TKG)$ usando el valor TKG que ha recibido y lo verifica con el valor $h(TKG)$ descifrado

En caso de que coincidan, da por válido el $AuthResp$ y autentica positivamente al servidor $\boxed{\text{IAS}}$.

Fase de Solicitud de Acceso al Servicio Modificada

En esta etapa se usa una sincronización basada en una secuencia que debe ser mantenida simultáneamente por el usuario U y el punto de acceso HG, combinada con un nonce aleatorio A_n que funciona como desafío. Cada valor E_{n+1} dependerá de los valores anteriores E_n y A_n , a partir de una fórmula recurrente. El subíndice indica el número de la sesión que se ejecuta actualmente. Este mecanismo reemplaza a la cadena de hash de esta fase en esquema de Vaidya et al.

Paso SR1. Cuando el usuario $\boxed{U}$ requiere acceder a servicios dentro de la red digital en el hogar, este envía al punto de acceso $\boxed{HG}$ el par de valoresID_C, $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, N_a, K_i, N, S, T_{exp})$

Paso SR2. El punto de acceso $\boxed{HG}$ actúa del siguiente modo al recibir el par de valores de la solicitud:

Descifra $E_{K_{IAS-HG}}(ID_C, ID_{IAS}, S_{k_i}, E_1, N, T_{exp})$ usando la clave K_{IAS-HG}

Verifica el valor ID_C recibido con el valor obtenido al descifrar el TKG, si estos coinciden entonces continúa con el procedimiento, de lo niega de inmediato el acceso al servicio

Verifica T_{exp} para ver si ha expirado la sesión

Guarda los valores $ID_C, ID_{IAS}, N_a, K_i, N, S, T_{exp}$

Inicializa un contador decreciente $C \coloneqq N$, si es la primera solicitud de la sesión y en otro caso solo disminuye su valor actual en 1, $C \coloneqq C - 1$

Genera A_n aleatorio

Calcula $h(S_{k_i})$ y lo almacena para usos posteriores

Calcula $A_n \oplus h(S_{k_i})$, $h(A_n \parallel E_n)$

Paso SR3. $\boxed{HG}$ envía los valores $A_n \oplus h(S_{k_i})$, $h(A_n \parallel E_n)$ al usuario $\boxed{U}$ para ser autenticado por este

Paso SR4. El usuario $\boxed{U}$ realiza las siguientes operaciones

Obtiene $A_n = A_n \oplus h(S_{k_i}) \oplus h(S_{k_i})$ utilizando el valor de la clave S_{k_i} conocida

Calcula $h(A_n \parallel E_n)$a partir de su propio valor de estado E_n

Compara el valor que ha obtenido del cálculo, con el valor $h(A_n \parallel E_n)$recibido de $\boxed{HG}$

Si coinciden entonces reemplaza su valor secuencial E_n por $E_{n+1} = h((A_n \oplus E_n) \parallel S_{k_i})$

Paso SR6. $\boxed{U}$ le envía $h(E_{n+1}) \oplus h(S_{k_i})$ a $\boxed{HG}$

Paso SR7. $\boxed{HG}$ actúa como sigue:

Obtiene $h(E_{n+1})$ a partir de S_{k_i}

Calcula E_{n+1}a partir de su valor secuencial actual E_n y el aleatorio A_n

Compara $h(E_{n+1})$ obtenido con $h(E_{n+1})$ calculado y si estos valores coinciden da acceso al usuario $\boxed{U}$ al servicio solicitado

Comparación entre el protocolo modofocado y el protocolo original.

La primera modificación importante que se ha hecho al protocolo de Vaidya et al. [1], es cambiar algunos de los valores que son almacenados en la tarjeta inteligente en la fase de registro. En este caso ya no se almacenan los tres valores $v_T = h\ (ID_c \oplus x)\ \oplus h(PW)\ \oplus K$,

$g_T = h(ID_c \parallel x \parallel K) \oplus h(ID_c \parallel PW)$ y$k_T = K \oplus H\big(PW \oplus H(PW)\big)$, sino sólo el par de valores $u_1 = h(PW \oplus h(PW)) \oplus K$ y $u_2 = h(ID_c \oplus x) \oplus h(ID_c \parallel PW) \oplus h(K)$. Nótese que el conjunto de valores que se almacena en la tarjeta inteligente están orientados a combinar criptográficamente los secretos para que cada una de las partes pueda obtener la clave secreta compartida K, pero de forma tal que la combinación de los valores internos no revele dicha clave. La modificación propuesta sigue cumpliendo dicha propiedad y reduce la información almacenada en la tarjeta inteligente. Los valores u_T y a_T enviados al servidor IAS en el último paso de la etapa de autenticación e inicio de sesión, no se han cambiado en el protocolo modificado; aunque sí hemos utilizado una notación diferente para los mismos. Sin embargo, los cambios introducidos a los valores iniciales son suficientes para eliminar la vulnerabilidad al ataque de verificación de contraseñas con pérdida de la tarjeta inteligente, ya que en este caso no es posible combinar ningún valor enviado en claro, con ningún otro almacenado en la tarjeta inteligente, para obtener un verificador de la contraseña, o para obtener K.

En el protocolo modificado se reducen ligeramente la cantidad de operaciones realizadas en la etapa de autenticación e inicio de sesión. Las modificaciones más relevantes que se han hecho a esta fase consisten en el cambio de los valores de la respuesta de autenticación y el tiquete para el acceso a los servicios, del par de valores $AuthResp = E_{K_i}(ID_C, ID_{IAS}, N_a, A_S, N, S)$,
$TKG = E_{K_{IAS-HG}}(ID_C, ID_{IAS}, N_a, K_i, N, S, T_{exp})$ al par $AuthResp = E_{K_i}(ID_C, ID_{IAS}, h(TKG), E_1)$,

$TKG = E_{K_{IAS-HG}}\big(ID_C, ID_{IAS}, S_K, E_1, N, T_{exp}\big)$, con ello se reduce la cantidad de información a cifrar y transmitir en el último paso de esta etapa y, hasta cierto punto, se proporciona integridad al valor TKG enviado en claro.

Por último en la fase de solicitud de acceso al servicio, se ha reemplazado la cadena de hash por un mecanismo de sincronización basada en una secuencia $E_n$antenida simultáneamente por el usuario U y el punto de acceso HG. Esta secuencia es combinada con un nonce aleatorio $A_n$que funciona como desafío y aporta cierta incertidumbre al proceso de cambio de la secuencia. Así cada próximo valor E_{n+1} se obtiene en función de los valores anteriores E_n y A_n utilizando una función hash segura. A diferencia de la cadena de hash, en la cual el número de operaciones hash requeridas depende de la posición de la cadena en la que se encuentren sincronizados el cliente y el servidor, en la secuencia utilizada se requiere una cantidad fija de operaciones hash en todo momento.

Puede ser comprobado que con la sustitución de la cadena de hash por nuestra sincronización secuencial, durante la fase de solicitud de servicios, en el protocolo modificado se realizan $\frac{N(N-5)}{2}$ operaciones hash menos que en el protocolo original, hasta que expira la sesión. Esto para un valor de N= 50 arroja una diferencia de 1125 operaciones hash.

Por otra parte el mecanismo basado en el valor secuencial es seguro, ya que este nunca es enviado en claro en el proceso de autenticación, y una vez conocido E_n no es posible obtener E_{n+1} si no se conoce el valor aleatorio An, que es enviado de forma cifrada usando una ronda de la operación XOR con $h(S_{k_i})$ que es un valor secreto dependiente de la clave de sesión. Además de lo planteado, se puede afirmar que las modificaciones realizadas no comprometen el nivel de seguridad ya proporcionado por el protocolo de Vaidya et al. ya que solo afectan cuestiones muy particulares, y no los principios esenciales de su funcionamiento.

Finalmente señalemos que aunque no hemos incluido las modificaciones pertinentes que requeriría la fase de cambio de contraseña del protocolo de Vaidya et al. [1], para nuestra propuesta estas son bastante naturales, y consistirían simplemente en actualizar los valores usados en la fase de registro por los introducidos en la fase de registro modificada.

CONCLUSIONES Y TRABAJOS FUTUROS

En este trabajo se ha hecho una revisión del protocolo recientemente planteado por Vaidya et al. [1] y se ha mostrado cómo este no es, en efecto, seguro contra los ataques con robo de tarjeta inteligente, tal y como afirmaban sus autores. Los protocolos de autenticación robusta mediante one time password usando tarjetas inteligentes de hoy día son considerablemente complejos; y aunque se hace importante brindar protección en los mismos contra ataques cada vez más sofisticados, esto no es una cuestión nada sencilla. En particular, el interés por brindar protección contra los ataques con pérdida de la tarjeta inteligente ha ido en aumento; y a pesar de ello, la mayoría de los protocolos representativos propuestos hasta el momento han fallado en proporcionar una solución adecuada para este tipo de vulnerabilidades. En el presente artículo se han realizado modificaciones puntuales al protocolo de Vaidya et al. para corregir la vulnerabilidad del mismo contra el ataque verificación de contraseñas con pérdida de la tarjeta inteligente, y se ha logrado mejorar la eficiencia computacional del protocolo original, cambiando la cadena de hash de la fase de solicitud de acceso al servicio por un mecanismo de sincronización secuencial. Con todo ello se ha obtenido un protocolo más eficiente y seguro que el protocolo de Vaidya et al., el cual había sido propuesto por sus autores como el protocolo más seguro de autenticación robusta mediante one time password usando tarjetas inteligentes, en comparación con otros protocolos representativos de este mismo tipo.

Aunque se han dado argumentos para la comprobación de la seguridad de la propuesta realizada en este trabajo, es necesaria la corroboración de dichas afirmaciones por medio de métodos más formales. De este modo se invita a aquellos investigadores que trabajan en esta área a revisar exhaustivamente esta nueva propuesta y adicionar nuevas modificaciones que ayuden a resolver otras vulnerabilidades no resueltas del protocolo de Vaidya et al. [1] En este sentido está orientado actualmente la continuación de este trabajo para momentos futuros.

RECONOCIMIENTOS

Este trabajo ha sido auspiciado por la “Secretaría Nacional de Ciencia, Tecnología e Innovación” (SENACYT), de la república de Panamá, en el marco del “Programa de la Maestría en Ciencias de Ingeniería de Sistemas de Comunicación con énfasis en Redes de Datos”, como parte de la investigación del autor para concluir su trabajo de diploma.

Es importante señalar que este trabajo no hubiera sido posible sin la amable colaboración del director del “Grupo de Análisis Seguridad y Sistemas” (GASS) de la Universidad Complutense de Madrid, Dr. Javier García Villalva, que me recibió durante dos meses de intenso trabajo guiado por él en su grupo, el cual ha permitió llevar a un estado maduro la presente investigación. Del mismo modo se agradece a todos los compañeros del mismo grupo que han participado en el proceso de análisis y discusiones progresivas de la investigación, impulsando el avance de la misma con sus valiosos comentarios y sugerencias.

REFERENCIAS

1. VAIDYA, Binod; HYUK PARK, Jong; YEO, Sang-Soo;J.P.C. RODRIGUES, Joel."Robust one-time password authentication scheme using smart card for home network environment". Computer Communications, 2011, vol 34, pp. 326 336.

2. KOCHER, P.; JAFFE, J.; JUN, B.B.. "Differential power analysis". Proceedings of Advances in Cryptology (CRYPTO'99), 1999, pp. 388397.

3. MESSERGES, T.S.; DABBISH, E.A.; SLOAN, R.H.; "Examining smart-card security under the threat of power analysis attacks". IEEE Transactions on Computers, 2002, vol 51, núm. 5, pp. 541552.

4. Raisul Alam, Muhammad; Ibne Reaz, Mamun; Mohd Ali, Alauddin; "A Review of Smart Homes: Past, Present, and Future". IEEE Transactions on Systems. Man, and Cybernetics, 2011.

5. Chan, Marie;EstEve, Daniel; Escriba, Christophe; Campo, Eric. "A review of smart homes: Present state and future challenges".Computer Methods and Programs in Biomedicine, 2008, vol 91, pp. 5581.

6. M'Raihi, D. et al.. "HOTP: An HMAC-Based One-Time Password Algorithm", Request for Comments: 4226 , diciembre 2005. Disponible en Web: http://tools.ietf.org/html/rfc4226.

7. Lamport, L.. "Password authentication with insecure communication". Communications of the ACM 24, 1981, vol 11, pp. 770772.

8. Lee, S.W.; Kim; H.S.; Yoo, K.Y.. "Improved efficient remote user authentication scheme using smart cards". IEEE Transactions on Consumer Electronics, 2004, vol 50, núm. 2, pp. 565567.

9. YOon, E.J.; Ryu, E.K.; Yoo, K.Y.. "An improvement of Hwang-Lee-Tang's simple remote user authentication schemes". Computers & Security, 2005, vol 24, pp. 5056.

10. Hsing, H.S.; Shin, W.K.. "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication using smart cards". Computer Communications, 2009,vol 32, pp. 649652.

11. Haller, N.M.. "The S/KEY one-time password system". Proceedings of the Internet Society Symposium on Network and Distributed System Security, 1994, pp. 151158.

12. Yeh, T.C.; Shen, H.Y.; Hwang, J.J.. "A secure one-time password authentication scheme using smart cards". IEICE Transaction on Communications, 2002, vol 85, núm. 11, pp. 25152518.

13. Tsuji, T.; Shimizu, A.. "One-time password authentication protocol against theft attacks". IEICE Transactions on Communications, 2002, vol 87, núm. 3, pp. 523529.

14. Lee, N.Y.; Chen, J.C.. "Improvement of one-time password authentication scheme using smart card". IEICE Transaction on Communications, 2005, vol 88 núm. 9, pp.37653769.

15. Jo, H.S.; Youn, H.Y.. "A Secure User Authentication Protocol Based on One-Time-Password for Home Network". Computational Science and Its Applications ICCSA 2005, 2005, pp. 519528.

16. Jeong, J.; Chung, M.Y.; Choo, H.. "Integrated OTP-based user authentication scheme using smart cards in home networks". Proceedings of the 41st Annual Hawaii International Conference on System Sciences, 2008.

17. Kim, S.K.; Chung, M.G.. "More secure remote user authentication scheme". Computer Communications, 2009,vol 32, pp. 10181021.

18. Yoon, E.J.; Yoo, K.Y.. "More efficient and secure remote user authentication scheme with smart cards". Proceedings of 11th International Conference on Parallel and Distributed System, 2005, vol 2, pp. 7377.

19. KIM, Hyun Jung; KIM, Hyun Sung. "AUTH HOTP - HOTP Based Authentication Scheme over Home Network Environment". ICCSA 2011, Part III, LNCS 6784, 2011, pp. 622637.