Acceso seguro a Internet móvil

*Juan Carlos Castro**

Resumen

En el presente documento se explican los procedimientos de autenticación y cifrado que se emplean en las diferentes familias de telefonía móvil conocidas, exponiendo al final la tecnología WAP. Se realiza una comparación de los diferentes mecanismos de seguridad que se pueden emplear en ésta indicando las características, ventajas y desventajas de cada uno de ellos.

Introducción

Todos conocemos el crecimiento que ha experimentado Internet y la telefonía móvil en estos últimos años. Este crecimiento se ha debido en gran parte a la facilidad de uso y en el beneficio que obtienen los usuarios de los diferentes servicios, además de la reducción de precios que ha existido. Esto ha motivado a que los usuarios demanden nuevos servicios a los operadores. El presente documento hace una reseña de las diferentes tecnologías de telefonía móvil (GSM, GPRS y UMTS), explicando la manera en la cual se realiza el proceso de autenticación y cifrado de la comunicación. En la última parte se expone el protocolo WAP que permitirá la navegación de Internet a través de móviles, haciendo énfasis en la seguridad que éste posee. Además, se introducen las diferentes formas de implementación de mecanismos de seguridad en la comunicación, realizando una comparación entre las diferentes alternativas existentes e indicando las características, ventajas y desventajas de cada una de ellas.

GSM

El estándar GSM es el sistema de telefonía móvil más usado alrededor del mundo (51 % del mercado compartido de todos los teléfonos celulares, tanto analógicos como digitales), con más de 215 millones de usuarios en América, Europa, Asia, África y Australia. Este estándar hace uso de un conjunto de algoritmos criptográficos para proporcionar los mecanismos de seguridad del sistema (Autenticación y Confidencialidad). Los algoritmos antes mencionados son [9]:

Tabla 1

A3	Algoritmo de autenticación
A5/1 - A5/2	Algoritmos de cifrado
A8	Algoritmo de generación de clave

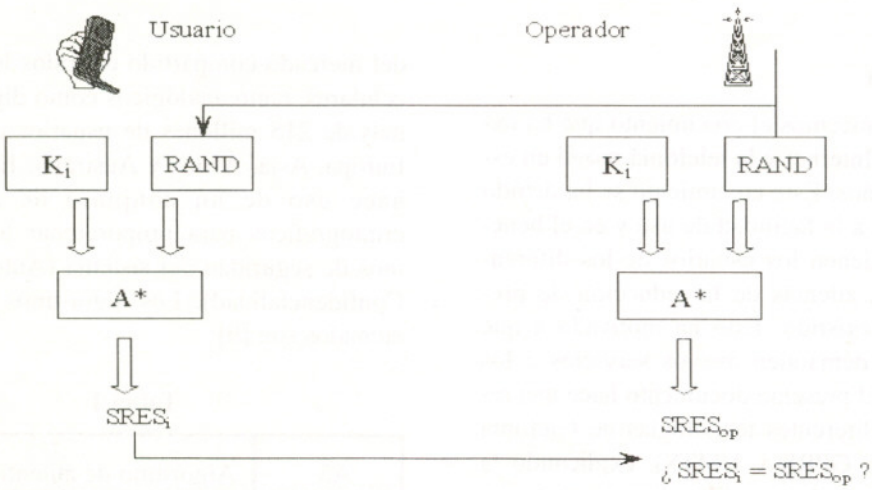
Dichos algoritmos fueron desarrollados de forma secreta; el procedimiento en el cual se describe el proceso de autenticación y generación de claves se muestra en la Figura 1, donde se observa que en ambos procesos el sistema hace uso de una clave secreta (Ki) que servirá como entrada al algoritmo correspondiente (A3 o A8). Dicha clave es conocida únicamente por el SIM (Subscriber Information Module) y el operador. Estas claves son diferentes para el algoritmo autenticación y generación de claves

* Ingeniero en electrónica por la Universidad Don Bosco. Actualmente se encuentra estudiando para su doctorado en Telemática en el Departamento de Matemática Aplicada y Telemática de la Universidad Politécnica de Catalunya. E-mail: jcastro@mat.upc.es

empleando un número secreto aleatorio (RAND) generado por el operador [2].

La mayoría de los proveedores GSM utilizan un algoritmo denominado COMP128 tanto para A3 como para A8. Este algoritmo es criptográficamente débil y no es difícil de romperlo y clonar teléfonos móviles. En Abril de 1998, un grupo de investigación de Berkeley publicó un análisis de COMP128. Este ataque puede ser llevado simultáneamente a cabo sobre tantos teléfonos en un rango de radio tan amplio como canales tenga la estación base con la que se lleva a cabo el delito. Demostrando en esta investigación que todas las implementaciones A8 que se habían examinado, incluyendo las pocas que no usaban COMP128, eran deliberadamente débiles [9].

El procedimiento de cifrado esta basado en la suma OR exclusiva de los bits a transmitir. El algoritmo ocupado para la generación de las secuencias de cifrado y descifrado es secreto y se denomina A5, del cual existen dos versio-



El protocolo A $^+$ se encuentra definido de la siguiente manera:

A3: Autenticación
A8: Generación de la clave de cifrado

Figura 1. Proceso de Autenticación y Generación de claves en GSM

nes: A5/1 y A5/2. Este tiene dos entradas: el Nº de trama (22 bits) y la clave de cifrado KC (64 bits), con estas entradas en algoritmo desarrolla procedimientos matemáticos obteniendo a su salida dos secuencias binarias de 114 bits, una de las cuales se utiliza para cifrar y la otra para descifrar. El procedimiento anteriormente descrito se muestra en la Fig. 2. Entre los meses de Mayo y Agosto de 1999 se analizaron los algoritmos A5/1 y A5/2 encontrándose que los dos algoritmos encargados del cifrado en GSM son imperfectos. El ataque al cual fue sometido el algoritmo A5/1 lo realizaron Alex Biryokov y Adi Shamir [8] y [5] mientras que el ataque al A5/2 fue realizado por Marc Briceno, Ian Goldberg y David Wagner [8]. Ellos encontraron que el A5/2 es el más débil de los dos algoritmos de cifrado ya que éste puede ser roto en tiempo real sin ningún problema, teniendo un factor de trabajo de aproximadamente 216 [9].

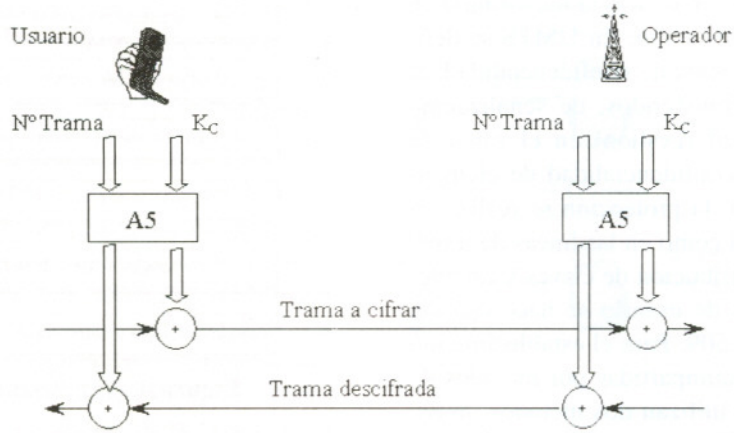


Figura 2. Procedimiento de cifrado y descifrado en GSM

GPRS

GPRS (General Packet Radio Services) es un nuevo conjunto de servicios desarrollado por el ETSI (European Telecommunication Standard Institute) los cuales se añadirán a los actuales que posee GSM. Estas se introducirán durante el año 2000. Básicamente, lo que hace es añadir conmutación de paquetes de datos a todos los niveles de la red GSM: radio, nodos de conmutación, tarificación, etc.[6].

GPRS ofrece funciones de autenticación, control de accesos, confidencialidad de la identidad del usuario y confidencialidad de la información. Mediante la autenticación, se puede confirmar la identidad del abonado, mientras que el control de accesos permite introducir diferentes tipos de restricciones de acceso a abonados al sistema GPRS, siguiendo unos criterios de localización o listas de protección. La confidencialidad de la identidad del usuario, por su parte, garantiza la privacidad de la identidad de los abonados a GPRS. De este modo, se consigue optimizar otras prestaciones de seguridad, como la confidencialidad de la información. Además, impide la realización de rastreos de localización de un determinado abonado móvil mediante escuchas de los cambios de señalización que se producen en el tramo de radio. Finalmente, las funciones de confidencialidad de información de usuario ponen los datos transferidos a salvo de personas, entidades o procesos no autorizados. Para ello, durante la comunicación de radio se protegen determinadas partes de los mensajes [4].

Los algoritmos empleados en el proceso de Autenticación son los mismos que los de GSM (A3 y A8), mientras que el algoritmo utilizado para el cifrado de los datos de usuario ha sido modificado debido a la naturaleza del tráfico de GPRS. Dicho algoritmo, denominado GPRS A5, fue definido por 5 personas en SAGE (Security Advisor Group of Experts) de el ETSI y no se encuentra disponible de forma pública [3]. A GPRS se le denomina como la generación 2.5, ya que es el paso intermedio a los nuevos sistemas de 3ª generación y proporciona a los sistemas actuales disponibilidad y funcionalidad de tercera generación.

UMTS

UMTS (Universal Mobile Telephone System) es el sistema de telefonía móvil de 3ª generación que se encontrará disponible a partir del año 2002. El UMTS será capaz de alcanzar velocidades entre 384 kbps para entornos de redes de banda ancha y 2.0 Mbps para entornos locales. Los mecanismos de seguridad del sistema UMTS se encuentran en la fase de desarrollo. Han sido propuestos diferentes mecanismos para proporcionar autenticación, confidencialidad y generación de claves. Los mecanismos de autenticación y distribución de claves son separados en dos grandes grupos: claves simétricas y claves asimétricas. Las técnicas de claves

asimétricas se emplean de forma mayoritaria en el proceso de autenticación. En UMTS se definen diferentes servicios de confidencialidad de datos de usuario transferidos, de señalización de usuario o de red (gestión) en el canal de señalización y de confidencialidad de elementos de señalización; la protección se realiza en los radioenlaces así como en las líneas de transmisión. Para la distribución de claves y establecimiento de claves de usuario se hace uso del estándar CCITT X.509. Para el establecimiento de claves secretas compartidas por métodos de claves públicas, se utilizan dos métodos: negociación de claves y transporte de claves. En el primero de estos se hace uso de variantes del algoritmo Diffie-Hellman [7].

WAP

El WAP (Wireless Access Protocol) es un sistema completamente nuevo que combina dos tecnologías: Internet y las comunicaciones móviles. El sistema fue realizado por 4 compañías (Nokia, Motorola, Ericsson y Unwired Planet). La Fig. 3 nos muestra el modelo de funcionamiento del sistema WAP, el cual se encuentra definido en [10]. Dicho protocolo proporcionará todos los servicios (Navegación, Correo Electrónico, Comercio Electrónico, etc.) que tiene disponible el usuario con Internet.

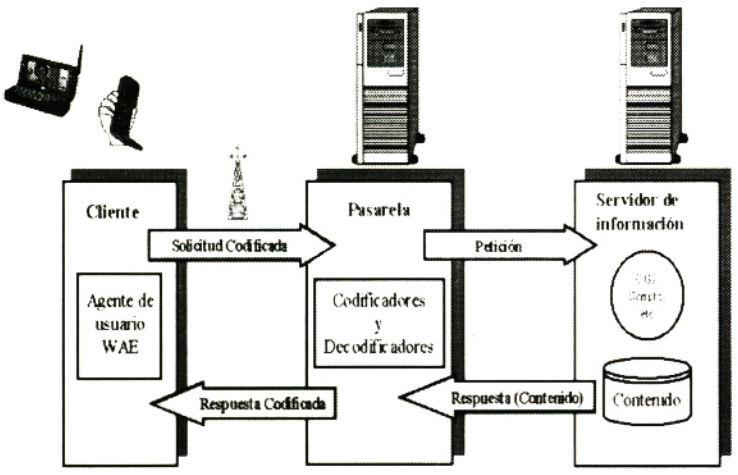


Figura 3. Modelo de funcionamiento de WAP

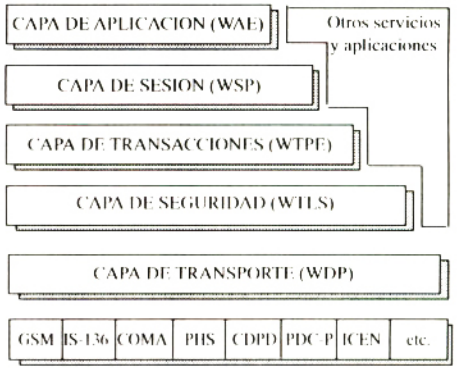


Figura 4. Arquitectura WAP

Cada una de estas capas del modelo de referencia emplea uno o varios protocolos que tienen la función de interpretar la información que recibe de la capa inmediata inferior y adaptarla para que la capa inmediata superior pueda repetir la misma operación y llegar a la capa de aplicación. La capa de transporte viene definida por el protocolo WDP (Wireless Datagram Protocol) que permite hacer uso de las mismas aplicaciones en diferentes tipos de portadoras (distintas frecuencias o distintos protocolos de acceso al medio) o señales de información. En la capa de seguridad se emplea el protocolo WTLS (Wireless Transport Layer Security) el cual es derivado del SSL 3.1, y se basa en el sistema abierto TLS 1.0, proporcionando los elementos de seguridad de confidencialidad, integridad y autenticación. La verificación de la autenticación no-repudio son dadas por una PKI (Public Key Insfraestructure). La capa de transacción esta basada en el WTP (Wireless Transaction Protocol) derivado del TCP. La función principal de esta capa es eliminar los datagramas no utilizados y preparar la información para la capa superior. El WSP (Wireless Session Protocol) es el protocolo que se empleará en la capa de sesión y está preparado para agrupar varias operaciones WTP, siendo encargado también del restablecimiento de las conexiones que excedan el tiempo de vida asignado al iniciar

la conexión. La última capa, la de aplicación, define la interfaz de usuario en el teléfono y hace uso de: Wireless Markup Language (WML), WMLScript y Wireless Telephony Application (WTA).

Al igual que UMTS los mecanismos de seguridad de WAP se encuentran en una etapa de desarrollo, aunque ya existen algunas herramientas que se apoyan en dicho estándar para ofrecer los elementos de confidencialidad, integridad, autenticidad y no-repudio. Así tenemos W/ Secure[11] y Baltimore Telepathy[1] los cuales contienen una implementación de WTLS, existen diferentes forma de implementar dichos mecanismos de seguridad, entre los cuales tenemos:

- Autenticación mutua sobre el interface aire, la cual serviría para establecer parámetros importantes de seguridad.
- Encripción interface aire. Para emplear este tipo de encripción es necesario hacer uso de diferentes claves de control junto con la información de señalización.
- Encripción punto a punto: por medio de este tipo de encripción la aplicación puede verificar las claves de administración sin ningún problema y de esta manera los datos de los cuales hace uso la aplicación nunca serán expuestos fuera de ella.

El protocolo WAP se puede implementar no sólo en una terminal telefónico digital celular con tecnología GSM, D-AMPS o CDMA sino también en los de tercera generación (UMTS) o en los inalámbricos DECT, para ofrecer servicios de datos nuevos o con mejores prestaciones. Algunos de los servicios que ofrecerá WAP son:

- Acceso a la información general disponible en Internet
- Acceso a bases de datos en las Intranets (información corporativa, de administración y gestión)
- Noticias breves
- Banca y Comercio Electrónico

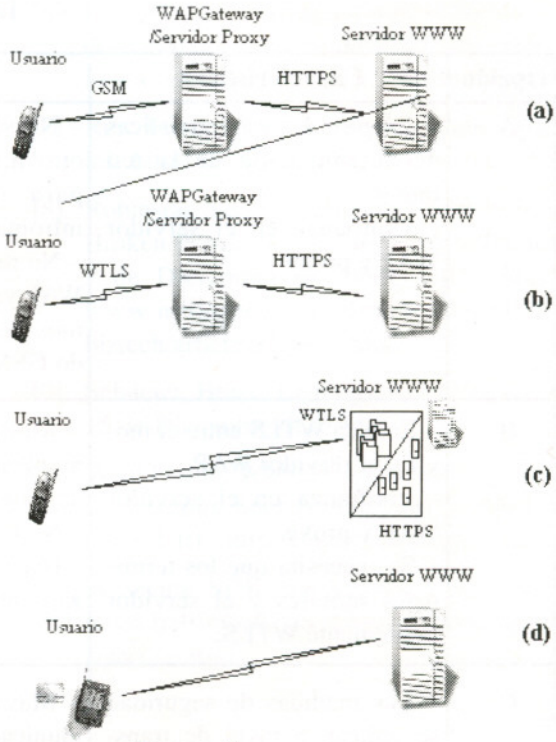


Figura 5

- Directorios (Páginas amarillas, páginas blancas, etc.)
- Juegos y Ocio

Mecanismos de Seguridad

WAP nos ofrece una arquitectura flexible de seguridad, centrándose en proporcionar seguridad entre la conexión que posee un usuario y un servidor WAP, es decir extremo a extremo. Se ha visto que la capa WTLS es la encargada de proporcionar seguridad a WAP, y que dependiendo de los requisitos de seguridad y de las características que posea la red así una aplicación podrá habilitar o deshabilitar las facilidades de WTLS. En la Fig. 5 se muestran diferentes opciones que se puede emplear para obtener el acceso seguro a Internet empleando la red telefónica móvil (ver Tabla 2).

Tabla 2

Opción	Características	Ventajas	Desventajas
A	– Emplea las características de autenticación de la red móvil – Confianza en el servidor WAP y proxy	– No se debe emplear ningún otro método de autenticación para el transporte de la infromación. – No requiere implementación WAP ya que ocupa los algoritmos de autenticación y cifrado GSM.	– Requiere confianza en el servidor WAP y proxy. – Tomar en cuenta las diferentes debilidades encontradas en los algoritmos de autenticación y cifrado de GSM [5] y [8]
B	– Emplea WTLS entre el móvil y el servidor WAP – confianza en el servidor WAP y proxy. – Se necesita que los terminales móviles y el servidor implemente WTLS.	– Mayor seguridad en la comunicación ya que base uso del protocolo WTLS. – No centralizado – Hace uso de una PKI (Public Key Infraestructure).	– Requiere confianza en el servidor WAP y proxy. – Hace uso de certificados, lo cual incrementa los costos.
C	– Las medidas de seguridad se aplican a nivel de transporte empleando seguridad extremo a extremo. – Servidor de Internet debe ofrecer servidor WTKS.	– Mayor seguridad en la comunicación ya que hace uso del protocolo WTLS. – No requiere confianza en el servidor WAP	– Existe una mayor complejidad ya que el servidor de Internet sirve también como servidor WTLS. – Centralizado, es decir toda la carga de trabajo se encuentra sobre el servidor.
D	– Seguridad a nivel de aplicación. – La Aplicación es almacenada en el SIM (subscriber Information Module).	– La mejor solución respecto a seguridad. – Se tiene la facilidad de ofrecer servicios especiales (ej. No repudio)	– La complejidad aumenta ya que ahora la aplicación junto con la infromación del móvil debe ser almacenada en el SIM. – Mayor complejidad en los terminales móviles.

Conclusión

En el presente trabajo se han revisado las diferentes mecanismos de seguridad que podrían emplearse para obtener un acceso seguro a Internet a través de la red telefónica móvil empleando el protocolo WAP, definiendo cuatros opciones de las cuales podemos observar que la opción (a) es la más fácil de implementar ya que se hace uso de los protocolos de autenticación y cifrado actuales de GSM, las opciones (b) y (c) presentan ya el uso del protocolo de WTLS estas presentan el problema que en el caso de aplicaciones como e-comerce será necesario la total confianza de los proveedores de servicios (Bancos, Almacenes, etc.) en los proveedores de servicio. La opción (d) es la mejor solución a nivel de seguridad ya que es basada en una aplicación que se encontrará almacenada en el teléfono móvil teniendo la oportunidad de implementar nuevos servicios.

Referencias

[1] Baltimore Technologies Launches Telepathy - Wireless Security For Mobile Commerce; URL: http://www.baltimore.com/news/press/pr20000111b.html

[2] Franco, J.P., Sarasa L., M.A. Criptografía Digital Prensas Universitarias de Zaragoza, 1º Edición, 1998.

[3] Kari, Hannu H. GPRS security issues. 12 de Febrero de 1999. URL: http://www.cs.hut.fi/~hhk/GPRS/ps/

[4] La conmutación de paquetes llega a GSM GPRS. Nº 86. 1 de Enero de 1995. URL: http://www.idg.es/comunicaciones/mainart.asp?artid=10870

[5] McCullagh, Declan. Cell Phone Crypto Penetrated. 6 de Diciembre de 1999 URL: http://wired.lycos.com/news/politics/0,1283,32900-2,00.html.

[6] Paúl, Daniel. Introducción de GPRS en redes GSM. 19 de Abril de 1999. URL: http://www.telecomid.com/fitxers/1/367.pdf.

[7] Rey, Eugenio. Telecomunicaciones Móviles. Editorial Marcombo, 2ª Edición, 1998.

[8] Robinson, Sara. Researchers Claim to Have Broken Privacy Code for Wireless Phones. 7 de Diciembre de 1999. URL: http://www.nytimes.com/library/tech/99/12/biztech/articles/07code.html

[9] Schneier, Bruce. Criptograma. Número 20. 15 de Diciembre de 1999

[10] WAP Forum. Wireless Application Protocol Architecture Specification. 30 de Abril de 1998. URL: http://www.wapforum.com

[11] W/Secure SDK Whitepaper, URL: http://www.baltimore.com/library/whitepapers/wsecure.html