Seguridad en Protocolos de Comunicación: Eventos

1st Alejandro Padrón-Godínez
Instrumentación. Científica e Industrial, ICAT- Coordinación de Óptica
UNAM - INAOE
Circuito Exterior S/N CDMX - Tonantzintla, Puebla - México
apadron@inaoep.mx

***Resumen*—En este trabajo presento el diseño e implementación de protocolos de comunicación con el uso técnicas criptográficas, construyendo supuestos eventos donde puede haber vulnerabilidades. Una vez identificado el evento propuesto se pueden diseñar los pasos a seguir en cada caso, además de aplicar los servicios y mecanismos que nos ayudarán a salvar dificultades ante ataques.**

***Palabras Clave*—criptografía, protocolos, servicios y mecanismos de seguridad**

I. Introducción

Los protocolos no deben ser vistos solo como una serie de pasos a seguir como si fuera un recetario, esto no funciona. Los protocolos son una serie de pasos a seguir por varias entidades con tareas individuales para su implementación. Las tareas que deben de realizar las entidades son desde generar claves hasta implementar algoritmos criptográficos en *hardware* o *software* (mecanismos de seguridad) y muchos otros como verificación de datos recibidos. El protocolo debe ser completado; debe haber una acción determinada para cada situación posible. El propósito de los Protocolos.- en la vida cotidiana, hay protocolos informales para casi todo: pedir mercancías por teléfono, jugar al poker, votar en una elección. Nadie piensa mucho acerca de ellos, han evolucionado con el tiempo y digamos todo el mundo sabe cómo usarlos, funcionan razonablemente bien. En estos días, la interacción humana ocurre por redes informáticas en lugar de cara a cara. Las computadoras necesitan protocolos formales para hacer las mismas cosas que la gente hace sin pensar. Muchos protocolos cara a cara se llevan a cabo en presencia del pueblo por ejemplo las votaciones, para garantizar la equidad y la seguridad [1]. Por otro lado la finalidad de la criptografía es resolver problemas de seguridad como no repudio, autenticación, integridad y confidencialidad. En realidad, ese es el punto principal que buscan los computólogos — algo que mucha gente tiende a olvidar. Cualquiera puede aprender todo sobre algoritmos criptográficos y técnicas, pero éstos son de carácter académico al menos que puedan resolver un problema real. Por esta razón vamos a estudiar algunos eventos propuestos para implementar la seguridad en protocolos de comunicación.

II. Seguridad Informática

Las comunicaciones se limitaban a un acceso a la red federal de microondas, en ese entonces como ahora para lograr enlaces seguros se han desarrollado más y mejores protocolos de comunicación segura rápida y eficiente lo que nos lleva a pensar en el desarrollo de esta valiosa herramienta como un valor agregado. Existen diversos protocolos de comunicación que se manejan indistintamente en diferentes medios de comunicación, pero sin la seguridad que se requiere, ya que se pude alterar, borrar y/o modificar la información, o que simplemente no lleguen a su destino [2].

PASPA-DGAPA-UNAM beca de doctorado.

II-A. Lenguaje común: definiciones

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la mejor manera posible. Además que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas dentro de los límites de su autorización [3].

II-B. Servicios de Seguridad

En la actualidad hablamos de seis servicios de seguridad que se manejan para el intercambio de información mediante un protocolo de comunicación: confidencialidad, integridad, autenticidad, disponibilidad, no repudio y control de acceso. No es posible implementarlos todos pero si se pueden implementar algunos gracias a los mecanismos de seguridad que han sido desarrollados hasta ahora. Además no todas las aplicaciones o comunicaciones requieren necesariamente los mismos servicios de seguridad. Los servicios hacen que se resuelvan ciertos problemas del protocolo o que se produzca cierto resultado [4]. Los servicios de seguridad responden a varias incógnitas que se han propuesto en la comunicación y transmisión de información a través de canales que son promiscuos e inseguros, ver la Figura(1).

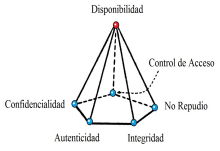

Figura 1. Piramide pentagonal de los servicios de seguridad.

III. Construcción de Protocolos

Un protocolo de comunicación o de red es un acuerdo entre dos o más partes para realizar una tarea específica, una serie de pasos bien definidos y todas las partes involucradas

conocen estos pasos y están de acuerdo en seguirlos. Además un protocolo define claramente lo que cada parte gana o expone con su ejecución. Existen varios tipos de protocolos entre los cuales se mencionan los arbitrados, los adjudicados y los autoimplementados [1].

III-A. Implementación de protocolos

Los protocolos son reglas de comunicación que permiten el flujo de información entre computadoras distintas que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás. Para ello, es necesario que ambas ”hablen” el mismo idioma, por tal sentido, el protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet, es necesario que tenga instalado este protocolo de comunicación. Pueden estar implementados bien en *hardware* (tarjetas de red), *software* (drivers), o una combinación de ambos.

III-A1. Protocolos Arbitrados: Están basados en una tercera parte confiable: el árbitro no tiene ningún tipo y forma de preferencia por ninguna de las partes, en la vida real es el papel que debe jugar un juez. Este tipo de protocolo es poco práctico, por la dificultad de tener una tercera parte confiable y neutral. Objetivo: Alice y Bob hacen compra/venta de un auto usando a S como árbitro.

- 1) A entrega los papeles y las llaves del auto a S
- 2) B entrega el cheque a A.
- 3) A deposita en cheque en el banco
- 4) Si el cheque es bueno, S entrega los papeles y las llaves del auto a B. Si el cheque es malo, S regresa los papeles y las llaves del auto a A. Desde luego, en caso de que el cheque sea malo, A tiene que mostrar pruebas de ello a S.

III-A2. Protocolos Adjudicados: Estos son una variante de los arbitrados y están basados en una tercera parte confiable, pero esta parte no siempre se requiere. Si todas las partes respetan el protocolo, el resultado se logra sin ayuda de la tercera parte denominada adjudicador o tercero en discordia. Si una de las partes involucradas piensa o cree que las otras partes hacen trampa: se invoca al adjudicador como ayuda y el adjudicador analiza la disputa y las reglas además dice quién está actuando bien y qué es lo que se debe hacer. Juzgar la disputa no siempre es sencillo: dependen de la calidad de las evidencias y es tarea del protocolo producir buenas evidencias. Mismo objetivo anterior:

- 1) A entrega llaves y papeles del auto a B.
- 2) B entrega el cheque a A.
- 3) Si el cheque no es bueno, o si los papeles son falsos, A y B comparecen ante un juez y ambos presentan sus evidencias.
- 4) El juez dictamina las evidencias y la parte que engaña es penalizada.

III-A3. Protocolos Autoimplementados: Son los mejores protocolos, se diseñan de tal manera que hacen virtualmente imposible el engaño. No requieren ni árbitro ni juez y garantizan que si cualquier participante engaña, el engaño es descubierto de inmediato por el otro u otros participantes. Propiedades Típicas:

- Detección de la conexión física sobre la que se realiza la conexión (cableada o sin cables)
- Pasos necesarios para comenzar a comunicarse (Handshaking)
- Negociación de las características de la conexión.
- Cómo se inicia y cómo termina un mensaje.
- Formato de los mensajes.
- Qué hacer con los mensajes erróneos o corruptos (corrección de errores)
- Cómo detectar la pérdida inesperada de la conexión, y qué hacer en ese caso.
- Terminación de la sesión de conexión.
- Estrategias para asegurar la seguridad (autenticación, cifrado).

Esta propiedad del protocolo es la que implementaremos en algunos eventos de este trabajo mediante servicios de seguridad y se puede realizar la comprobación de las secuencias pseudoaleatorias utilizando los postulados de Golomb [5].

IV. Circunstancias en donde implementar los protocolos

Ahora se debe analizar el escenario donde se debe establecer la comunicación y qué tipo de servicio de seguridad será necesario implementar en el diseño del protocolo. Para esto veamos primero unos simples desarrollos para entender la notación a utilizar. Partimos de un sistema de comunicación entre Alice y Bob como comúnmente se muestra en la Figura (2), donde también hay un guardián del canal de comunicación.

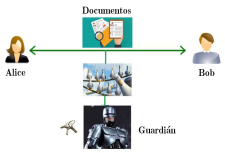

Figura 2. Esquema de comunicación entre dos partes, guardián y mensaje.

- Luego si las claves $K_A = K_B$ entonces se usará criptografía simétrica de clave secreta o criptografía clásica convencional.
- Si las claves $K_A \neq K_B$ entonces se usará criptografía asimétrica de clave pública.
- Si no hay llave entonces se usarán las funciones Hash o huellas digitales del mensaje.

Ahora denotando la nomenclatura a emplear:

- m: mensaje a transmitir
- m’: mensaje recibido a comparar
- A: Alice
- B: Bob
- I: Wendy (atacante o interceptor del mensaje)
- H: Función Hash
- K_a: clave de Alice
- K_b: clave de Bob
- K_{ab}: clave común de Alice y Bob

- vh: valor Hash
- K_a^{pub}: clave pública de Alice
- K_a^{priv}: clave privada de Alice
- K_b^{pub}: clave pública de Bob
- K_b^{priv}: clave privada de Bob
- E: algoritmo de cifrado
- D: algoritmo de descifrado
- C: criptograma
- F: firma digital

AES: algoritmo criptográfico simétrico (Advanced Encryption Standar) NIST, FIPS-197", (2001) [b6].
CBC: modo de operación (cipher block chaining). NIST Special Publication 800-38ª, (2001) [7].
RSA: algoritmo criptográfico asimétrico. Rivest R. et Al., (1978) [8].
MAC: código para autenticación de mensaje. Barak Boaz, (2006) [9].
Algoritmo de Diffie and Hellman para el acuerdo de clave, (1975) [10].

IV-A. Primer Evento

Alice y Bob desean acordar una llave secreta K_s para poder enviarse mensajes cifrados con un "protocolo autoimplementado" garantizando una autenticación unilateral. Un protocolo autoimplementado se diseña de tal manera que se hace virtualmente imposible el engaño y no requieren ni árbitro ni juez. Garantiza que si cualquier participante engaña, el engaño es descubierto de inmediato por el otro u otros participantes. Con esto se implementará el servicio de confidencialidad en el protocolo. Establecido el evento en que se debe desarrollar el protocolo de comunicación sus pasos a seguir serán:

- 1. A: genera la llave secreta K_s.
- 2. A: convierte la llave secreta K_s en una secuencia binaria.
- 3. A: usa criptografía asimétrica para cifrar la llave secreta K_s firmada de acuerdo a: $E_{K_B^{pub}}(E_{K_A^{priv}}(K_s)) = E_{K_B^{pub}}(firma) = C_1$
- 4. A: cifra con la llave secreta K_s un mensaje y obtiene: $E_{K_s}(m_A) = C_2$
- 5. A: envía a B los resultados de C_1 y C_2.
- 6. B: descifra C_1 de acuerdo a: $D_{K_B^{priv}}(C_1) = (firma)$
- 7. B: verifica la firma mediante: $D_{K_A^{pub}}(D_{K_A^{priv}}(K_s)) = D_{K_A^{pub}}(firma) = K_s$
- 8. B: descifra C_2 con la llave secreta y obtiene el mensaje que A le envío: $D_{K_s}(C_2) = m_A$

Este protocolo funciona y es confiable porque nadie más que A y B conocen la llave secreta K_s. Por tanto, nadie más puede leer el mensaje *m* y se acuerda de manera segura la llave.

IV-B. Segundo Evento

En este evento se emplearán los términos de Capa de Conexión Segura (por sus siglas en inglés *Secure Locker Layer*), que es un protocolo criptográfico empleado para realizar conexiones seguras entre un cliente y un servidor. Las suposiciones de este evento son las siguientes:

SLL: genera y distribuye claves de sesión.
SLL: es confiable, emplea criptografía simétrica, caso particular el algoritmo AES-256 bits.
SLL: tiene claves simétricas con Alice (K_{sA}) y clave con Bob (K_{sB}).
Objetivo.- Alice y Bob acuerdan claves K_s a través del servidor de claves.

- 1. A envía SLL: $E_{K_{sA}}$ (requeridas por A, B)=C
- 2. SLL: genera K_s
- 3. SSL: $E_{K_{s_A}} = C_A$
- 4. SLL: $E_{K_{s_B}(K_s)} = C_B$
- 5. SLL envía A: C_A, C_B
- 6. SLL: $D_{K_{s_B}}(C_A) = K_s$
- 7. A envía B: C_B
- 8. B: $D_{K_{s_B}}(C_B) = K_s$

Si agregamos Autenticación mutua con Hand Shake y Verificación de la Integridad tendremos al siguiente protocolo:

- 1. A envía SLL: $E_{K_{sA}}$ (requeridas por A, B)=C
- 2. SLL: genera K_s
- 3. SLL: $E_{K_{sA}}(K_s) = C_A$
- 4. SLL: $E_{K_{sA}^{CBC}}(K_{sB}) = C_{MAC-256}^A$
- 5. SLL: $E_{K_{sB}}(K_s) = C_B$
- 6. SLL: $E_{K_{sB}^{CBC}}(K_{sA}) = C_{MAC-256}^B$
- 7. SLL envía A: $(C_A, C_B, C_{MAC-256}^A, C_{MAC-256}^B)$
- 8. A: $D_{K_{sA}}(C_A) = K_s$
- 9. A: $D_{K_{sA}^{CBC}}(C_{MAC-256}^A) = K_{s_B}$
- 10. A: $D_{K_{sB}}(C_B) = K_s$
- 11. A envía B: $(C_A, C_B, C_{MAC-64}^A, C_{MAC-256}^B)$
- 12. B: $D_{K_{sB}}(C_B) = K_s$
- 13. B: $D_{K_{sB}^{CBC}}(C_{MAC-256}^B) = K_{s_A}$
- 14. B: $D_{K_{sA}}(C_A) = K_s$
- 15. B: $D_{K_s}(K_{sB}) = C_1$
- 16. B envía A: C_1
- 17. A: $D_{K_s}(C_1) = K_{s_B}$

IV-C. Tercer Evento

Veamos las suposiciones para este caso:
- Alice tiene el documento que desea transmitir.
- Se usará el algoritmo RSA para firmar y verificar (criptografía asimétrica).
- Todas las claves K están certificadas.
- Todas las partes tienen sus propias parejas de claves (púbica y privada).
- AC: Autoridad Certificadora, es confiable además verifica todas las firmas.

Objetivo.- A, B y C deben firmar el documento *m* y AC debe verificar todas y cada una de las firmas.

- 1. A: $F_{K_A}^{priv}(m) = s_A$
- 2. A envía $B : (s_A, m)$
- 3. B: $F_{K_B}^{priv}(m) = s_B$
- 4. B envía C: (s_A, s_B, m)
- 5. C: $F_{K_C}^{priv}(m) = s_C$
- 6. C: envía AC: (s_A, s_B, s_C, m)
- 7. AC:$v_{K_A}^{pub}(S_A) = m$, $v_{K_B}^{pub}(S_B) = m$, $v_{K_C}^{pub}(S_C) = m$.

Si se agregará Confidencialidad y Verificación de la Integridad el protocolo quedaría como:

- 1. A: $H_A(m) = vh_A$
- 2. A: $E^{pub}_{K_{AC}}(F^{priv}_{K_A}(m, vh_A)) = s^{H_A(m)}_A$
- 3. A envía B ($s^{H_A(m)}_A, m$)
- 4. B: $H_B(m) = vh_B$
- 5. B: $E^{pub}_{K_{AC}}(F^{priv}_{K_B}(m, vh_B)) = s^{H_B(m)}_B$
- 6. B envía C:($s^{H_A(m)}_A, s^{H_B(m)}_B, m$)
- 7. C: $H_C(m) = vh_C$
- 8. C: $E^{pub}_{K_{AC}}(F^{priv}_{K_C}(m, vh_C)) = s^{H_C(m)}_C$
- 9. C envía AC:($s^{H_A(m)}_A, s^{H_B(m)}_B, s^{H_C(m)}_C, m$)
- 10. AC: $D^{priv}_{K_{AC}}(v^{pub}_{K_A}(s^{H_A(m)}_A)) = m, vh_A$
  AC: $H_A(m) = vh'_A$
  AC: $vh_A = vh'_A$
- 11. AC: $D^{priv}_{K_{AC}}(v^{pub}_{K_B}(s^{H_B(m)}_B)) = m, vh_B$
  AC: $H_B(m) = vh'_B$
  AC: $vh_B = vh'_B$
- 12. A$D^{priv}_{K_{AC}}(v^{pub}_{K_C}(s^{H_C(m)}_C)) = m, vh_C$
  AC: $H_C(m) = vh'_C$
  AC: $vh_C = vh'_C$

Ahora se le agrega la fecha y la hora al protocolo:

- 1. A:$F^{priv}_{K_A}(m) = s^m_A$
- 2. A:$F^{priv}_{K_A}(TS_A) = s^{TS_A}_A$
- 3. A envía B: ($s^m_A, s^{TS_A}_A, m$)
- 4. B:$F^{priv}_{K_B}(m) = s^m_B$
- 5. B:$F^{priv}_{K_B}(TS_B) = s^{TS_B}_B$
- 6. B envía C: ($s^m_A, s^{TS_A}_A, s^m_B, s^{TS_B}_B, m$)
- 7. C: $F^{priv}_{K_C}(m) = s^m_C$
- 8. C: $F^{priv}_{K_C}(TS_C) = s^{TS_C}_C$
- 9. C envía AC:($s^m_A, s^{TS_A}_A, s^m_B, s^{TS_B}_B, s^m_C, s^{TS_B}_B, s^m_C$, $s^{TS_C}_C, m$)
- 10. AC:
  $v^{pub}_{K_A} s_A = m, v^{pub}_{K_A}(s^{TS_A}_A) = TS_A$
  $v^{pub}_{K_B} s_B = m, v^{pub}_{K_B}(s^{TS_B}_B) = TS_B$
  $v^{pub}_{K_C} s_C = m, v^{pub}_{K_C}(s^{TS_C}_C) = TS_C$

IV-D. Cuarto Evento

Para este evento de estudio vamos a implementar una Autenticación Mutua y Verificación de Integridad bajo las consideraciones que se mostraron en el caso de estudio IV-C, inmediato anterior. También para este estudio se emplearán tanto técnicas de criptografía simétrica como pública, en particular los algoritmos son el AES de 256-bits y RSA de 2048 respectivamente. Para empezar nuestro protocolo del evento citado veamos como empleamos los algoritmos de cifrado:

- 1. A: genera K_s
- 2. A: $E^{AES}_{K_s}(m) = C_1$
- 3. A: $E_{RSA^{pub}_{K_B}}(E_{RSA^{priv}_{K_s A}}(K_s)) = C_2$
  donde $E_{RSA^{priv}_{K_A}}(K_s)$ es la firma
- 4. A envía B: C1, C2
- 5. B: $E_{K^{priv}_B}(C_2)) = Firma$
- 6. B: $D_{K^{pub}_A}(E^{priv}_{K_A}(K_s)) = K_s$
- 7. $D^{AES}_{K_s}(C_2) = m$

Ahora vamos a implementar la Confidencialidad y Autenticación mutua:

- 1. A: $E_{K_{ab}}(m) = C_1$
- 2. A envía B: C_1
- 3. B: $D_{K_{ab}}(C_1) = m$
- 4. B: $E_{K_{ab}}(m') = C_2$
- 5. B envía A: C_2
- 6. A: $D_{K_{ab}}(C_2) = m'$
- 7. A: m'=m, compara

Si le sumamos Integridad al protocolo anterior se obtiene:

- 1. A: $E_{K_{ab}}(m) = C_1$
- 2. A: $E_{K^{CBC}_{ab}}(m) = C^A_{MAC-256}$
- 3. A envía B:($C_1, C^A_{MAC-256}$)
- 4. B: $D_{K_{ab}}(C_1) = m'$
- 5. B: $E_{K^{CBC}_{ab}}(m) = C^B_{MAC-256}(')$
- 6. B: $C^B_{MAC-256}(') = C^B_{MAC-256}$ compara
- 7. B envía A: $(C^B_{MAC-256}('), m')$
- 8. A: $E_{K^{CBC}_{ab}}(m') = C^A_{MAC-256}$
- 9. A: $C^A_{MAC-256} = C^A_{MAC-256}(')$ compara

V. Conclusiones

Se presentaron varios desarrollos de seguridad en protocolos de comunicación implementando servicios y mecanismos de seguridad que nos ayudan a salvar vulnerabilidades y riesgos ante atacantes. Se han presentado cuatro eventos como casos de estudio para la implementación de protocolos seguros, que si bien sus estructuras son conocidas a veces no se sabe cuando, como y donde implementarlas. La confidencialidad, integridad, autenticidad dentro de protocolos se pueden garantizar de manera confiable mediante técnicas de Criptografía. La relevancia es la factibilidad técnica y eficiencia de los protocolos, al implementarlos ya sea en *software* o *hardware* dentro los protocolos que usamos para sistemas de comunicación y que pueden ser usados en otras aplicaciones.

Referencias

[1] Schneier B., "Applied Cryptography", John Wiley and Sons, Inc., EUA. (1996).

[2] Daltabuit E., Hernández L., Mallén G., Vázquez J., "La seguridad de la Información," Ed. Limusa, 2007.

[3] Menezes A., Oorschot P. V and Vanstone S. "Handbook of Applied Cryptography", CRC Press, (1997).

[4] INTERNATIONAL STANDARD, ISO 7498-2, "Information processing - Open Systems Interconnection - Basic Reference Model. Security Architecture," First edition 1989-02-15.

[5] Golomb S. W. Shift Register Sequences, Prentice Hall Inc. EUA. , (1967).

[6] NIST, "Federal Information Processing Standards Publication 197", ADVANCED ENCRYPTION STANDARD (AES), November 26. (2001).

[7] NIST Special Publication 800-38ª, "Recommendation for block cipher modes of operation", (2001).

[8] Rivest R., Shamir A., Adleman L., (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM, Vol. 21 (2), pp.120–126. Previously released as an MIT "Technical Memoïn April 1977. Initial publication of the RSA scheme.

[9] Barak Boaz, "Computer Science 433 Cryptography", Princeton University Computer Science Department. (2006).

[10] Diffie W., Hellman M. E. "New Directions in Cryptography", IEEE Information Theory Workshop, Lenox, MA, EUA. (1975).