Aumento de la Fiabilidad de la Evidencia en un Protocolo de Intercambio Justo mediante la División del Entorno de Firma

Jorge L. Hernández-Ardieta, Ana I. González-Tablas, Benjamín Ramos Álvarez, y Arturo Ribagorda Garnacho

Departamento de Informática, Grupo SeTI, Universidad Carlos III de Madrid
Avda. de la Universidad 30, 28911 – Leganes, España.
jlopez.ha@gmail.com, aigonzal@inf.uc3m.es, benja1@inf.uc3m.es, arturo@inf.uc3m.es

Resumen El respaldo legal de la firma electrónica unido a su reconocimiento como evidencia de no repudio por parte de los estándares internacionales hace que la seguridad del proceso de creación de firmas sea una cuestión de suma importancia. Sin embargo, numerosos estudios demuestran que existe una gran variedad de ataques a entornos de creación de firmas, lo cual socava la fiabilidad de la firma electrónica como evidencia de no repudio y evidencia en procedimientos legales. En este artículo se presenta un protocolo en el cual se aumenta considerablemente la fiabilidad de la evidencia generada aun cuando el firmante emplea un entorno de creación de firmas inseguro. El protocolo se ha diseñado tomando como base un protocolo de intercambio justo presentado con anterioridad, en el cual se asegura que ningún participante obtiene una ventaja respecto al otro durante la transacción.

Palabras clave: Firma electrónica, evidencia, no repudio, protocolo de intercambio justo, ataques.

1. Introducción

Se han hecho muchos esfuerzos por promocionar el comercio electrónico, especialmente en relación a la mejora de su seguridad. Quizá el más relevante ha sido el apoyo que los Gobiernos y la Industria han dado a la firma electrónica. Una firma electrónica se considera como datos en formato electrónico que se adjuntan o asocian a otros datos electrónicos y que actúan como método de autenticación [16]. Sin embargo, múltiples legislaciones consideran la firma electrónica legalmente equivalente a la firma manuscrita, asignándola la propiedad de evidencia en procedimientos legales [16,21,13,45]. Por otra parte, los estándares internacionales también consideran a la firma electrónica como evidencia de no repudio en transacciones electrónicas [29,30], tanto cuando se aplica en transacciones de comercio electrónico como de otra índole. Es obvio que la firma electrónica se considera un elemento clave, y por tanto su seguridad es una cuestión crítica que debe analizarse con rigurosidad.

Aunque las legislaciones actuales son neutras desde un punto de vista tecnológico, el hecho es que los requisitos establecidos sólo se cumplen actualmente por las firmas digitales basadas en criptografía asimétrica [38,14] y soportadas por una Infraestructura de Clave Pública (PKI) [11] la cual permita establecer confianza en las identidades digitales empleadas. Como resultado, cuando una firma digital se verifica correctamente, el firmante, cuya identidad está vinculada a la clave pública correspondiente, no podría rechazar haber creado dicha firma, y, por ende, no podría negar su participación ni compromiso adquirido en la transacción dada.

Sin embargo, los entornos donde se producen estas firmas, especialmente aquellos empleados por los usuarios finales, no son todo los seguros que debieran ser, dada la cantidad de amenazas que se ciernen sobre ellos [25]. Ciertos ataques se centran en comprometer la clave privada de firma con el fin de poder posteriormente generar firmas electrónicas sin el consentimiento ni conocimiento del firmante [12,22,43,34]. Otros ataques tienen por objetivo engañar al firmante de forma que éste firme unos datos diferentes a los deseados sin detectarlo [41,42]. Numerosos resultados muestran que es difícil asegurar la fiabilidad de una firma electrónica si se emplean documentos o datos con formatos complejos, como por ejemplo aquellos que permiten la inclusión de macros o gráficos [3,31,32]. Este tipo de ataques, que nosotros denominamos ataques semánticos, anulan los mecanismos WYSIWYS [40] (*What You See Is What You Sign*), mediante los cuales se intenta ofrecer al firmante un último paso de verificación de los datos inmediatamente anterior a la generación firma.

Si no se puede proveer al firmante de medios seguros para la creación de firmas, éste no debería ser responsable del compromiso adquirido en documentos firmados en su nombre (ej. orden de compra, contrato, correo electrónico, etc.). El firmante podría fácilmente probar que la clave privada pudo haber sido comprometida o que el documento que intentaba firmar pudo haber sido modificado justo antes de realizar la firma. El firmante podría probar ante el juez que existe una duda razonable respecto a la seguridad del entorno de firma, y por tanto la validez de la firma se vería puesta en cuestión. Ya existe jurisprudencia al respecto. Recientemente se ha producido un fallo en favor del demandado al ser incapaz la entidad demandante de demostrar un cierto grado de seguridad en el proceso de creación de la firma repudiada [2]. No obstante, la actual legislación en materia de firma electrónica traslada al firmante la carga de prueba [35], siendo éste quien debe probar la falsedad de la firma. Este contexto sin duda le sitúa en un escenario de incertidumbre, provocando una falta de confianza en la tecnología y sus procesos.

El protocolo que se presenta en este artículo tiene por objetivo incrementar la fiabilidad de las firmas electrónicas, reforzando su propiedad de evidencia de no repudio así como su capacidad de evidencia en procedimientos legales. El efecto buscado es aumentar la confianza de los usuarios en esta tecnología, lo cual fomentará el uso del comercio electrónico, entre otros modelos de negocio. Este protocolo toma como punto de partida el protocolo de intercambio justo

OFEPSP [24], el cual asegura la equidad en la transacción en la que tanto origen como receptor participan.

La seguridad del protocolo aquí propuesto se ha verificado formalmente [27] tomando como referencia el modelo de intruso Dolev-Yao [15], en el cual el atacante tiene absoluto control sobre la red pero no puede realizar criptoanálisis. En este sentido el atacante puede intercambiar, reenviar, reutilizar o eliminar cualquier mensaje intercambiado entre los participantes. Las propiedades de seguridad verificadas incluyen la correcta autenticación de los participantes así como el aseguramiento de la integridad de los mensajes intercambiados.

El artículo se ha estructurado como sigue. La siguiente sección 2 proporciona una breve descripción de OFEPSP. Las modificaciones de diseño realizadas se detallan en la sección 3. La sección 4 incluye los resultados del análisis formal de seguridad del protocolo. Finalmente se concluye el artículo en la sección 5.

2. OFEPSP

OFEPSP [24] es un protocolo orientado a transacciones electrónicas donde dos participantes pueden intercambiar información de forma equitativa y segura. El origen de la transacción envía cierto mensaje firmado electrónicamente mientras que el receptor responde con una prueba de recepción de dicho mensaje. Al emplear firmas electrónicas durante el proceso, ambos participantes adquieren determinado compromiso en la transacción: el origen no puede repudiar haber enviado el mensaje y el receptor no puede repudiar su recepción. Como protocolo de intercambio justo, OFEPSP asegura que ningún participante obtiene una ventaja respecto al otro en la transacción. Por lo tanto, o bien ambos participantes obtienen la información esperada de la otra parte o ninguno obtiene información relevante del otro. Al ser un protocolo optimista, existe una Tercera Parte de Confianza (TTP) que interviene en el protocolo con el fin de resolver situaciones de desequilibrio, pero únicamente cuando se produce un error en el protocolo (p. ej. se pierde un mensaje por fallo en la red) o cuando alguna de las partes se comporta de forma maliciosa.

La mayoría de los protocolos de este tipo emplean cifrado simétrico para evitar que un participante desvele información útil al otro sin que éste haya adquirido cierto compromiso en la transacción [33]. Por el contrario, OFEPSP está diseñado en base a políticas de firma [18,39]. Una política de firma es un documento que recoge las reglas y requisitos para la creación y validación de firmas electrónicas, y bajo las cuales una firma electrónica se considera válida en un contexto transaccional concreto. Las políticas de firma se definen tanto en formato entendible por el ser humano como en formato estructurado, como XML y ASN.1, permitiendo una generación y validación automática de firmas. Una referencia a la política de firma empleada por el firmante se incluye como atributo firmado en las firmas generadas, permitiendo al verificador comprobar si dicha firma cumple con los requisitos impuestos por la política de firma referenciada.

OFEPSP emplea una política de firma para establecer los pasos y condiciones a seguir por los participantes de la transacción (origen, receptor, TTP) de forma

que se asegure la justeza de la misma. Gracias a este diseño, OFEPSP permite al origen evaluar las condiciones que dictaminarán la transacción. De esta forma, el origen se convierte en un participante activo que puede decidir si confía o no en la entidad que emite dicha política así como aceptar o no los términos que en ella se establecen. Por el otro lado, el receptor publica las condiciones a cumplir por cualquier origen que quiera realizar una transacción con él. Así pues, OFEPSP tiene una clara orientación a escenarios de comercio electrónico donde estas características aportan un valor añadido.

A día de hoy los organismos de estandarización ETSI e IETF han publicado un conjunto de informes técnicos no estándares y una RFC Experimental, respectivamente, en los cuales se define la estructura de una política de firma en formato ASN.1 [39,20] y XML [17]. Sin embargo, estas propuestas sólo permiten establecer los requisitos para una única firma electrónica. No se contempla la gestión de múltiples firmas electrónicas en cuanto a sus requisitos individuales ni las relaciones entre ellas. Por ello, protocolos en los cuales la evidencia se componga de múltiples firmas electrónicas, como es el caso de los protocolos de intercambio y no repudio justos, no quedan cubiertos. ETSI publicó un informe técnico en el que se recogían los requisitos de alto nivel que debería cumplir una política de firmas para cubrir este objetivo [19].

En [26] proponemos un framework completo para la definición y uso de políticas de firmas extendidas, cubriendo así la necesidad establecida por ETSI. De esta forma, se puede definir cualquier árbol de firmas que sea necesario para otorgar validez a la transacción. El árbol de firmas incluye por tanto las firmas necesarias que deben estar presentes para que los compromisos adquiridos por los participantes de la transacción sean vinculantes, así como los requisitos particulares de cada firma y las relaciones espacio-temporales entre ellas: orden de generación, dependencia respecto a otras firmas, etc. Así mismo, el framework define el algoritmo de generación y validación de firmas de acuerdo a la política de firmas extendida requerida. Gracias a esta nueva propuesta, protocolos como OFEPSP o el que detallamos en la sección 3 pueden ser fácilmente implementados.

OFEPSP se compone de un protocolo principal y un protocolo de recuperación. El protocolo principal permite a origen y receptor interactuar durante una serie de etapas hasta que se genera la evidencia final llamada NRA (*Non-Repudiation evidence of Acknowledgment*). Durante la ejecución del protocolo principal se generan dos evidencias intermedias no vinculantes, pero de las cuales depende el NRA. Así pues, el origen genera la firma no vinculante NRO (*Non-Repudiation evidence of Origin*), mientras que el receptor genera el NRR (*Non-Repudiation evidence of Receipt*). NRO y NRR se generan sobre los datos de la transacción, mientras que el NRA se generan sobre la firma NRR. De esta manera se compone un árbol de firmas con dos firmas en el primer nivel (NRO y NRR) y una tercera firma (NRA) en el segundo nivel, dependiente de NRR. La evidencia vinculante, así definida por la política de firma, consiste en el árbol de firmas completo.

Esta evidencia es la que realmente ata a los participantes respecto a los compromisos adquiridos en la transacción. Por tanto, hasta que el árbol de firmas no se genere correctamente, los participantes no adquieren ningún compromiso vinculante. Una vez generado, el origen no puede repudiar el envío del mensaje y el receptor no puede rechazar su recepción. Estos compromisos pueden extenderse a otros más particulares dependiendo del tipo de compromiso necesitado en el contexto de negocio en el cual tiene lugar la transacción, y que se configura y personaliza a nivel de política de firma. Por ejemplo, la evidencia puede implicar no sólo el no repudio de origen y no repudio de recepción para origen y receptor, respectivamente, sino también un compromiso de aceptación de contenido por ambas partes.

Por último, el protocolo de recuperación permite al receptor obtener el NRA en caso que se produzca algún error en la comunicación o si el origen se comporta maliciosamente.

3. Protocolo de Intercambio Justo con División del Entorno de Creación de Firma

Esta sección detalla el nuevo diseño que aumenta la fiabilidad de la evidencia vinculante aun cuando se empleen entornos de firma inseguros. El nuevo diseño añade además un nuevo subprotocolo de aborto que permite al origen abortar la transacción en caso que detecte que ésta es una transacción no deseada.

La siguiente sección 3.1 introduce el diseño ideado así como las suposiciones del entorno de partida. La notación empleada en la definición del protocolo se explica en la sección 3.2. Finalmente se describe el protocolo principal y ambos subprotocolos.

3.1. Aproximación al Diseño

La principal novedad del protocolo aquí propuesto radica en el empleo por parte del origen de dos entornos diferentes para la generación de las firmas electrónicas que componen la evidencia del protocolo.

Por un lado, el origen debe firmar la información a enviar al receptor mediante el Entorno de Creación de Firmas (ECF). ECF debe disponer de una aplicación de firma electrónica que permita al origen generar firmas electrónicas basadas en criptografía asimétrica, empleando un dispositivo de creación de firmas hardware (SCDev1) - ej. una tarjeta inteligente. SCDev1 almacenará de forma segura una clave privada de firma (Key1).

Por otro lado, proponemos que el origen confirme la transacción haciendo uso de un segundo entorno, llamado Entorno de Confirmación de Transacción (ECT), y un SCDev diferente (SCDev2), que contenga una clave privada de firma distinta (Key2).

En [28] hemos demostrado formalmente cómo la división del entorno de creación de firmas mejora sustancialmente la fiabilidad de la evidencia resultante. En particular, el uso de dos entornos y dos SCDev-Key diferentes asegura que

un atacante no obtendrá ningún beneficio en caso de comprometer la seguridad del ECF o ECT. Por ello, la seguridad del protocolo es sustancialmente mayor que la de los actuales sistemas de firma electrónica, los cuales se basan en un único entorno.

El mensaje a firmar por el origen debe ser normalizado de acuerdo a una plantilla, la cual restringe el formato del mensaje (ASCII) así como el contenido del mismo. La plantilla debe ser definida por el receptor de acuerdo a las necesidades de la transacción. El mensaje m enviado por el origen será posteriormente procesado por el receptor teniendo en cuenta la plantilla empleada. De esta forma la semántica de la información se mantiene a lo largo de toda la transacción, evitando los ataques semánticos.

Un ejemplo de plantilla para la restricción de la semántica de la información generada en un proceso de negocio es el estándar UBL desarrollado por OASIS [37]. UBL define un conjunto de componentes de negocio reutilizables para la composición de documentos que se generan e intercambian en una transacción dada. Por ejemplo, se definen componentes para facturas, pedidos y recibos. Así mismo, UBL se integra perfectamente en el estándar ebXML de OASIS [36], el cual define el framework y el protocolo para el intercambio de mensajes genéricos de negocio. El protocolo aquí propuesto puede por tanto adaptarse fácilmente para soportar UBL como modelo de información cuando la transacción se englobe en un contexto de comercio electrónico.

El diseño y seguridad del protocolo dependen de las siguientes consideraciones:

1. El origen será normalmente un usuario final. Tanto ECF como ECT se consideran entornos inseguros. Ello es debido a que el usuario empleará plataformas habitualmente poco seguras, es decir, plataformas donde la probabilidad de sufrir un ataque o verse infectadas por malware es alta. Un ejemplo puede ser un ordenador personal/corporativo que actúe como ECF y un dispositivo móvil con capacidades criptográficas que actúe como ECT.
2. La seguridad de tanto ECF como ECT puede verse comprometida. Sin embargo, la probabilidad de un ataque distribuido a ECF y ECT por malware diferente, y que colabore con el fin de generar una evidencia vinculante fraudulenta, se demuestra sustancialmente menor que en caso de emplear un único entorno [28].
3. El entorno empleado por el receptor para generar las firmas electrónicas correspondientes se considera seguro. En este sentido, dicho entorno opera conforme a sus especificaciones, lo cual no implica que estas especificaciones no puedan ser perjudiciales para el origen (p. ej. el receptor intenta estafar al origen en un proceso de compra on-line). Por ello, el receptor no es de confianza aunque se descarta la posibilidad de que su entorno sufra un ataque que comprometa la seguridad del protocolo. Este requisito aplica a escenarios donde el receptor es una corporación u organización más que un usuario final, como en transacciones de comercio electrónico.

4. La información a intercambiar debe estar en formato ASCII sin formato (texto plano). Este requisito es fácilmente alcanzable en contextos como sistemas de correo electrónico o comercio electrónico.

3.2. Notación Básica

A continuación se detalla la notación empleada en la definición del protocolo:

SP Política de Firma empleada en el protocolo
$X \rightarrow Y : m$ Entidad X envía un mensaje m a la Entidad Y
$X \leftarrow Z : SP$ Entidad X solicita SP a la entidad Z
$S_X(m)$ Firma electrónica generada por la entidad X sobre el mensaje m
$S_X(m|SP)$ Firma electrónica generada por la entidad X sobre el mensaje m en base a la política de firma SP

$POO = S_O(m, \ell, tpl\_id|SP)$
Prueba de Origen (*Proof of Origin*) respecto al mensaje m.
$POR = S_R(m, \ell, tpl\_id|SP)$
Prueba de Recepción (*Proof of Receipt*) respecto al mensaje m.
$NRO = S_O(POR|SP)$
Evidencia de no repudio de origen (*Non-Repudiation evidence of Origin*) respecto al mensaje m generada sobre POR.
$NRR = S_R(NRO|SP)$
Evidencia de no repudio de recepción (*Non-Repudiation evidence of Receipt*) respecto al mensaje m generada sobre NRO.
$NRA_O = S_O(NRR|SP)$
Evidencia de no repudio de aprobación (*Non-Repudiation evidence of Acknowledgment*) generada sobre NRR. Esta es la firma que termina de componer la evidencia vinculante del protocolo.
$NRA_{TTP} = S_{TTP}(NRR|SP)$
Evidencia de no repudio de aprobación generada por el Tercero de Confianza (TTP) sobre NRR. Esta firma compone igualmente la evidencia vinculante del protocolo, pero cuando se ejecuta el subprotocolo de recuperación.

Cada ejecución del protocolo se identifica mediante un identificador único ℓ. Las entidades deben emplear la plantilla para fijar la semántica de la información a enviar por el origen. Esta plantilla debe referenciarse en cada mensaje haciendo uso de su identificador *tpl_id*.

Al igual que en OFEPSP, la evidencia vinculante consiste en el árbol de firmas completo, que en este caso se compone de las firmas electrónicas POO y POR en el primer nivel, y las firmas NRO, NRR y NRA en niveles consecutivos y dependientes secuencialmente.

3.3. Protocolo Principal

En el protocolo principal el origen inicia la transacción al enviar el mensaje firmado al receptor empleando ECF. Posteriormente, el origen confirmará dicha transacción empleando ECT. El receptor intercambiará diferentes firmas

electrónicas con tanto ECF como ECT hasta que la firma electrónica (NRA) que completa el árbol es generada. A continuación se detalla el protocolo principal empleando la notación anteriormente descrita:

(1) $O_{ECF} \leftarrow R : tpl\,[tpl\_id]\,, S_R\,(tpl\,[tpl\_id])$

Primero, el origen (O) solicita al receptor (R) la plantilla identificada por *tpl_id* (1) haciendo uso de ECF.

(2) $O_{ECF} \leftarrow$ *TTP-SP*: $SP, S_{TTP-SP}\,(SP)$

En el siguiente paso (2), el origen obtiene la política de firma SP necesaria para interactuar con el receptor. Una vez que el origen dispone de la plantilla y la política de firma, puede generar el mensaje y POO.

(3) $O_{ECF} \rightarrow R : m, \ell, tpl\_id, POO$

Posteriormente (3), el origen inicia el protocolo al enviar el mensaje m, el identificador único de protocolo ℓ, el identificador de la plantilla y POO.

(4) $R \leftarrow$ *TTP-SP*: $SP, S_{TTP-SP}\,(SP)$

(5) $R \rightarrow O_{ECT} : m, \ell, tpl\_id, POO, POR$

El receptor recupera la política de firma (4), si no dispone de ella, y valida el POO recibido. Después genera y envía el POR al origen, pero en este caso al ECT (5). El paso (4) puede evitarse, mejorando la eficiencia del protocolo, si el receptor accede al TTP-SP una única vez y en ejecuciones posteriores del protocolo emplea la copia local.

(6) $O_{ECT} \rightarrow R : NRO$

El origen debe generar el NRO si y sólo si la información recibida en el paso (5) corresponde a una transacción deseada, y POO y POR son correctamente verificados.

(7) $R \rightarrow O_{ECF} : NRR$

Una vez que el origen ha confirmado la transacción mediante ECT, el receptor envía el NRR el entorno ECF del origen (7).

(8) $O_{ECF} \rightarrow R : NRA_O$

En el último paso (8) el origen completa la transacción enviando el NRA al receptor.

Aunque no se ha mostrado, las firmas POO, POR, NRO, NRR y NRA deben contener el correspondiente sello temporal. El sello de tiempo es una prueba proporcionada por una Autoridad de Sellado de Tiempo (TSA) de que ciertos datos existían antes de un momento determinado. El procedimiento de obtención del sello temporal debe hacerse conforme al estándar [1], implicando así la participación de una TSA. La política de firma recogerá las condiciones de dependencia temporal y secuencial entre todas las firmas del protocolo. El verificador

podrá comprobar que dichas condiciones se cumplen tomando como referencia temporal los sellos de tiempo incluidos en las firmas.

3.4. Subprotocolo de Recuperación

Este subprotocolo permite al receptor obtener la evidencia NRA en caso que ocurra un error en la transacción o el origen se comporte de forma maliciosa. Este subprotocolo debe ejecutarse si el receptor no es capaz de obtener el NRA por parte del origen, e implica los siguientes pasos:

(1) $R \rightarrow TTP : H\left(m, \ell, tpl\_id\right), \ell, POO, POR, NRO, NRR$

Si el protocolo ha sido abortado por el origen, entonces

(2a) $TTP \rightarrow R : S_{TTP}\left(S_O\left(abort, \ell | SP\right) | SP\right)$

en caso contrario

(2b) $TTP \leftarrow$ *TTP-SP*: SP

(3b) $TTP \rightarrow R, O_{ECF}, O_{ECT} : NRA_{TTP}$

En (1) el receptor envía al TTP las firmas POO, POR, NRO y NRR. Con el objetivo de proteger la privacidad de los participantes, sólo se envía el resumen (*hash*) de la información firmada en POO y POR, esto es, el mensaje, el identificador único correspondiente a la presente ejecución y la referencia a la plantilla. Aun así, el TTP es capaz de verificar POO y POR empleando directamente dicho resumen, siempre y cuando el esquema de firma digital se base en criptografía de clave pública (p. ej. RSA, DSA, ECDSA). TTP debe descifrar POO y POR - empleando la correspondiente clave pública -, obteniendo el resumen de los datos firmados, y comparar dicho valor con el proporcionado en $H\left(m, \ell, tpl\_id\right)$. ℓ se envía en (1) para permitir al TTP recuperar y actualizar la información correspondiente a dicha transacción.

Si el protocolo había sido abortado previamente, TTP simplemente reenvía la evidencia de aborto al receptor (2a). En caso contrario, TTP genera NRA_{TTP} teniendo en cuenta la política de firma referenciada - (2b) y (3b) -, pero sólo en la primera solicitud. Al mantener una copia local de dicha información, puede reutilizarla en posteriores solicitudes, aumentando el rendimiento.

Es importante resaltar que las firmas electrónicas generadas durante el protocolo (POO, POR, NRO, NRR y NRA) deben ser generadas de acuerdo a estándares internacionales de firma [24]. De esta forma, se incluye una referencia a la política de firma empleada como atributo firmado en la firma electrónica, permitiendo al TTP conocer y obtener dicha política. Así mismo, este mecanismo impide a un atacante sustituir la política de firma referenciada.

3.5. Subprotocolo de Aborto

El subprotocolo de aborto permite al origen abortar el protocolo en caso que detecte que una transacción no deseada se ha iniciado en su nombre, si sospecha del comportamiento del receptor u ocurre algún error durante el protocolo que impida su completitud. Este subprotocolo se compone de los siguientes pasos:

(1) $O_{ECF|ECT} \rightarrow TTP : abort, \ell, S_O\,(abort, \ell|SP)$
Si el protocolo ha sido recuperado por el receptor, entonces
(2a) $TTP \rightarrow O_{ECF|ECT} : NRA_{TTP}$
en caso contrario
(2b) $TTP \leftarrow$ *TTP-SP*: SP
(3b) $TTP \rightarrow O_{ECF|ECT} : S_{TTP}\,(S_O\,(abort, \ell|SP)\,|SP)$

Por cuestiones de eficiencia, $S_{TTP}\,(S_O\,(abort, \ell|SP)\,|SP)$ sólo se genera la primera vez (2b) y (3b), siendo reutilizado en posteriores ocasiones. Por otra parte, si el protocolo ha sido recuperado por el receptor con anterioridad (2a), TTP simplemente reenvía al origen la copia local de NRA_{TTP}.

4. Análisis de Seguridad del Protocolo

La validación formal de protocolos de seguridad es de suma importancia, especialmente antes de que el mercado pueda tomarlos como referencia, e implementaciones de dichos protocolos se implanten en sistemas comerciales. La experiencia ha demostrado que una verificación heurística - por lo general siempre incompleta - y no formal de las propiedades de seguridad que un protocolo dice cumplir suponen una incertidumbre en cuanto a su seguridad real. Numerosos protocolos actuales adolecen de vulnerabilidades descubiertas tras su estandarización. La causa es que una validación no formal siempre obvia vectores de ataque potenciales, permitiendo a un atacante aprovecharse de vulnerabilidades no descubiertas durante el diseño del protocolo.

Los métodos de razonamiento automático pueden aplicarse para analizar y verificar formalmente las propiedades de seguridad establecidas en la especificación de un protocolo. Estos métodos generalmente buscan un contra-ejemplo a lo estipulado en la especificación. En caso de no encontrarse, se puede considerar que la especificación del protocolo implementa las propiedades establecidas.

El protocolo propuesto en la sección 3 se ha validado formalmente empleando las herramientas de validación automática AVISPA (*Automated Validation of Internet Security Protocols and Applications*) y SPAN (*Security Protocol ANimator for AVISPA*).

AVISPA [4,6] proporciona un conjunto de aplicaciones para la construcción y análisis formal de modelos de protocolos de seguridad. AVISPA incorpora cuatro motores de razonamiento automático: OFMC (*On the-Fly Model-Checker*) [8], CL-AtSe (*Constraint-Logic-based model-checker*) [44], SATMC (*SAT-based Model-Checker*) [5], y TA4SP (*Tree Automata based Automatic Approximations*

for the Analysis of Security Protocols) [9]. Por otra parte, SPAN [23] proporciona una interfaz gráfica de usuario que permite al diseñador del protocolo interactuar con las capacidades de AVISPA de forma sencilla.

Estas herramientas necesitan la especificación del protocolo para poder analizarlo. AVISPA permite especificar la dinámica del protocolo así como las propiedades de seguridad que se deseen verificar empleando el lenguaje de especificación de protocolos HLPSL (*High Level Protocol Specification Language*) [7,10].

Así mismo, para poder analizar las propiedades de seguridad es necesario establecer el modelo de atacante que se tomará como referencia. AVISPA utiliza el modelo estándar de intruso de Dolev-Yao (DY) [15], en el cual el atacante tiene absoluto control sobre la red pero no puede realizar criptoanálisis. En este sentido el atacante puede intercambiar, reenviar, reutilizar o eliminar cualquier mensaje intercambiado entre los participantes.

En [27] se detalla el procedimiento seguido para validar el protocolo propuesto en la sección 3 empleando AVISPA y SPAN, así como los resultados obtenidos. No obstante, a continuación se describe brevemente las conclusiones más importantes de dicha validación.

La metodología que se ha seguido se resume en tres etapas:

1. Especificación del protocolo mediante HLPSL.
2. Verificación de la corrección de la especificación.
3. Finalmente, la validación de la seguridad del protocolo.

De la etapa de especificación HLPSL cabe destacar la definición de las propiedades de seguridad a verificar. AVISPA soporta tres tipos de objetivos o propiedades de seguridad: secreto, autenticación fuerte y autenticación débil. Ambos objetivos de autenticación aseguran la integridad del mensaje autenticado. La diferencia entre los dos tipos de autenticación es que una autenticación débil no protege frente a ataques por replicación. La propiedad estipulada para el protocolo es la autenticación débil de los participantes respecto a todas las firmas electrónicas generadas (POO, POR, NRO, NRR, NRA). Es importante mencionar que AVISPA no soporta de forma explícita la propiedad de justeza o equidad, por lo que, en esta primera aproximación, no ha podido verificarse dicha propiedad del protocolo.

Antes de verificar la seguridad del protocolo en base a su especificación, es importante comprobar que ésta efectivamente implementa el comportamiento esperado, especialmente si se ha empleado un lenguaje de bajo nivel como HLPSL. Para ello se han ejecutado diversas utilidades ofrecidas por AVISPA y SPAN, garantizando la corrección sintáctica y cumplimiento funcional de la especificación.

Por último, en la etapa de validación se han definido múltiples escenarios de análisis que han sido utilizados por los motores OFMC y CL-AtSe para verificar las propiedades de seguridad indicadas. El resultado obtenido ha sido satisfactorio en todos los casos, lo cual ofrece las garantías buscadas en cuanto a la seguridad del protocolo. Los motores SATMC y TA4SP no pudieron emplearse debido a ciertas limitaciones actuales de la herramienta, y que les impedían analizar un protocolo de las características del propuesto.

5. Conclusiones y Trabajo Futuro

En este artículo se ha presentado un protocolo novedoso que permite mejorar de forma considerable la fiabilidad de la evidencia generada durante una transacción gobernada por un protocolo de intercambio justo. Esta evidencia se compone de múltiples firmas electrónicas, las cuales deben cumplir los requisitos impuestos por una política de firma determinada. El diseño del protocolo obliga al origen de la transacción a emplear dos entornos de creación de firmas diferentes, con diferentes claves privadas de firma en cada uno de ellos. Así mismo, la información intercambiada en la transacción debe ceñirse a una plantilla definida por el receptor, restringiendo la semántica de los datos.

De esta forma, la mayoría de los ataque conocidos no pueden violar la seguridad del protocolo, al necesitar comprometer no sólo ambos entornos sino también ejecutar un ataque colaborativo que permita generar evidencias de forma fraudulenta. La probabilidad de este tipo de ataques es sustancialmente menor que la probabilidad que tienen los actuales sistemas de firma implantados en el mercado de sufrir cualquiera de los ataques existentes.

Por otra parte, se ha presentado los principales resultados de un trabajo previo en el cual se verificó formalmente el protocolo propuesto. La verificación se llevó a cabo mediante herramientas de razonamiento automático. Teniendo en cuenta los resultados del análisis, podemos garantizar que las propiedades de seguridad estipuladas en el diseño del protocolo efectivamente se cumplen.

El objetivo inmediato es completar la verificación formal incluyendo la propiedad de equidad. Para ello se deberá especificar dicha propiedad mediante fórmulas objetivo y predicados especiales. Por otra parte, se va a proponer al grupo de trabajo de PKIX de IETF la redacción de una RFC Experimental que recoja el framework completo de políticas de firma extendidas mencionado en el artículo.

Agradecimientos. Este trabajo ha sido parcialmente realizado en el marco del proyecto SEGUR@, subvencionado por CDTI, Ministerio de Industria, Turismo y Comercio de España, dentro del programa CENIT, con referencia CENIT-2007 2004. (https://www.cenitsegura.es)

Referencias

1. Adams, C., Cain, P., Pinkas, D., Zuccherato, R.: RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). Internet Engineering Task Force (2001)
2. Adjunct Law Prof Blog - A Member of the Law Professor Blogs Network: Employer did not show electronic signature on arbitration pact was valid. Blog, 3rd March 2009, http://lawprofessors.typepad.com/adjunctprofs/2009/03/employer-did-no.html
3. Alsaid, A., Mitchel, J. C.: Dynamic content attacks on digital signatures. Information Management & Computer Security 13 (4), 328 - 336 (2005)

4. Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., Hankes Drielsma P., Heám, P.-C., Kouchnarenko, O., Mantovani, J., Mödersheim, S., von Oheimb, D., Rusinowitch, M., Santos Santiago, J., Turuani, M., Viganò, L., and Vigneron, L.: The AVISPA Tool for the automated validation of internet security protocols and applications. In K. Etessami and S. Rajamani, editors, 17th International Conference on Computer Aided Verification, CAV'2005, volume 3576 of Lecture Notes in Computer Science, pages 281–285, Edinburgh, Scotland. Springer (2005)
5. Armando, A., and Compagna. L.: SATMC: a SAT-based model checker for security protocols. In Proc. of the 9th European Conference on Logics in Artificial Intelligence (JELIA'04), LNAI, 3229, 730–733, Lisbon, Portugal. Springer-Verlag (2004)
6. AVISPA: Automated validation of internet security protocols and applications (2003) FET Open Project IST-2001-39252. http://www.avispa-project.org/
7. AVISPA. Deliverable 2.1: The High-Level Protocol Specification Language. Available at http://www.avispa-project.org/publications.html (2003)
8. Basin, D. A., Sebastian, M., and Viganò, L.: Ofmc: A symbolic model checker for security protocols. Int. J. Inf. Sec., 4(3):181–208 (2005)
9. Boichut, Y., Heam, P.-C., Kouchnarenko, O., and Oehl, F.: Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In Proc. of Automated Verification of Infinite States Systems (AVIS'04), 1 - 11. ENTCS (2004)
10. Chevalier, Y., Compagna, L., Cuellar, J., Hankes Drielsma, P., Mantovani, J., S. Mödersheim, and Vigneron, L.: A High Level Protocol Specification Language for Industrial Security-Sensitive Protocols. In Proc. SAPS'04. Austrian Computer Society, 2004.
11. Cooper, D., Santesson, S., Farrel, S., Boeyen, S., Housley, R., Polk, W.: RFC 5280 - Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile. Internet Engineering Task Force (2008)
12. Dasgupta, P., Chatha, K., Gupta, S. K. S.: Vulnerabilities of PKI based Smartcards. Proceedings of the IEEE Military Communications Conference 2007 (MILCOM 2007), 1-5. ISBN:978-1-4244-1513-7 (2007)
13. Department of Justice. Government of Canada. Personal Information Protection and Electronic Documents Act. April 13th (2000)
14. Diffie, W., Hellman, M.: New Directions in Cryptography. IEEE Transactions of Information Theory, 22 (6), 644-654. ISSN: 0018-9448 (1976)
15. Dolev, D., and Yao, A.: On the Security of Public-Key Protocols. IEEE Transactions on Information Theory, 2(29) (1983)
16. European Directive 1999/93/CE of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (1999)
17. European Telecommunications Standards Institute: ETSI TR 102 038 v1.1.1 - TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies (2002)
18. European Telecommunications Standards Institute: ETSI TR 102 041 v1.1.1 - Signatures policies report (2002)
19. European Telecommunications Standards Institute: ETSI TR 102 045 v1.1.1 - Electronic signatures and infrastructures (ESI); Signature policy for extended business model (2003)
20. European Telecommunications Standards Institute: ETSI TR 102 272 v1.1.1 - Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies (2003)

21. Federal Trade Commission, Department of Commerce. United States of America: Electronic Signatures in Global and National Commerce Act. Available at www.senate.gov/search/index.html under S.761 in the 106th Congress (2000)
22. Girard, P., Giraud, J-L.: Software attacks on smart cards. Information Security Technical Report, 8 (1), 55 - 66 (2003)
23. Glouche, Y., Genet, T., Heen, O., and Courtay, O.: A Security Protocol Animator Tool for AVISPA. In ARTIST2 Workshop on Security Specification and Verification of Embedded Systems, Pisa (2006)
24. Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., Alvarez, B. R.: An Optimistic Fair Exchange Protocol based on Signature Policies. Computers & Security, 27 (7-8), 309 - 322. ISSN 0167-4048. Ed. Elsevier (2008)
25. Hernández-Ardieta, J. L., González-Tablas, A. I., Ramos, B.: Repudio de firmas electrónicas en Infraestructuras de Clave Pública. Actas de la X Reunión sobre Criptología y Seguridad Informática (X RECSI 2008). Salamanca (2008)
26. Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., Ramos, B., Ribagorda, A.: Extended Electronic Signature Policies. 2nd ACM International Conference on Security of Information and Networks (SIN 2009). ACM Press. North Cyprus (2009)
27. Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., Ramos, B.: Formal Validation of OFEPSP+ with AVISPA. Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security. Lecture Notes in Computer Science, Springer-Verlag. York (2009)
28. Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., Ramos, B., Ribagorda, A.: On the Need to Divide the Signature Creation Environment. International Conference on Security and Cryptography (SECRYPT 2009). Milan (2009)
29. ISO/IEC DIS 13888-1. Information technology - Security techniques - Non repudiation - Part 1: General model. ISO/IEC JTC1/SC27 N1503 (1996)
30. ISO/IEC 13888-3 Information technology - Security techniques - Non repudiation - Part 3: Mechanisms Using Asymmetric Techniques. ISO/IEC (1997)
31. Jsang, A., Povey, D., Ho, A.: What You See is Not Always What You Sign. In the proceedings of the Australian UNIX User Group. Melbourne (2002)
32. Kain, K.: Electronic Documents and Digital Signatures. Master Thesis (2003)
33. Kremer, S., Markowitch, O., Zhou, J.: An intensive survey of fair non-repudiation protocols. Computer Communications 25, 1601 - 1621 (2002)
34. Marchesini, J., Smith, S.W., Zhao, M.: Keyjacking: the surprising insecurity of client-side SSL. Computers & Security, 24 (2), 109-123 (2005)
35. McCullagh, A., Caelli, W.: Non-repudiation in the digital Environment. First Monday, 5 (8). Available at http://firstmonday.org/issues/issue5_8/mccullagh/index.html (2000)
36. Organization for the Advancement of Structured Information Standards: ebXML Business Process Specification Schema Technical Specification v2.0.4 (2006)
37. Organization for the Advancement of Structured Information Standards: Universal Business Language (UBL) v2.0 (2008)
38. Rivest, R. L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21 (2), 120-126. ISSN:0001-0782 (1978)
39. Ross, J., Pinkas, D., Pope, N.: RFC 3125 - Electronic Signature Policies. International Engineering Task Force (2001)
40. Scheibelhofer, K.: What You See Is What You Sign - Trustworthy Display of XML Documents for Signing and Verification. Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security Issues of the New Century, 192, ISBN:0-7923-7365-0 (2001)

41. Spalka, A., Cremers, A. B., Langweg, H.: Protecting the Creation of Digital Signatures with Trusted Computing Platform Technology Against Attacks by Trojan Horse Programs. Proceedings of IFIP TC11 16th International Conference on Information Security. Kluwer, Boston (2001)
42. Spalka, A., Cremers, A. B., Langweg, H.: Trojan Horse Attacks on Software for Electronic Signatures. Informatica 26 (2), 191 - 203 (2002)
43. Tiri, K.: Side-channel Attack Pitfalls. Proceedings of the 44th Annual ACM IEEE Design Automation Conference, 15-20. ISBN:0738-100X (2007)
44. Turuani, M.: The CL-Atse Protocol Analyser. In F. Pfenning, editor, Proc. of 17th International Conference on Rewriting Techniques and Applications, RTA, Lecture Notes in Computer Science, Seattle (WA), Aug. Springer (2006)
45. United Nations. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001)