Taxonomía de ataques a entornos de creación de firmas electrónicas

Jorge López Hernández-Ardieta Ana Isabel González-Tablas Ferreres Benjamín Ramos Álvarez
Grupo SeTI
Departamento de Informática
Universidad Carlos III de Madrid
Email: jlhernan,aigonzal,benja1@inf.uc3m.es

***Resumen*—La firma electrónica se ha convertido en un elemento fundamental en la sociedad de la información, disfrutando del reconocimiento como medio de prueba en procedimientos legales. Así mismo, la firma electrónica es considerada una evidencia de no repudio respecto a los compromisos adquiridos por los participantes en una transacción electrónica. Sin embargo, la realidad nos muestra que la tecnología no está libre de vulnerabilidades, existiendo múltiples amenazas que pueden comprometer la seguridad de los sistemas. Es por tanto imprescindible disponer de las herramientas adecuadas que asistan al desarrollo de sistemas seguros, de forma que pueda aplicarse la legislación con plenas garantías para las partes implicadas. En particular, el proceso de generación de la firma es una de las etapas más sensibles, y a la cual se debe prestar especial atención. En este artículo se presenta la primera taxonomía completa de ataques a entornos de creación de firma, y que permitirá el análisis riguroso y sistemático de las causas que pueden socavar la fiabilidad de la misma, y así poder actuar en consecuencia.**

I. Introducción

Una taxonomía es un sistema o esquema para la clasificación sistemática del conocimiento. Mediante un análisis riguroso y sistemático, dicho conocimiento es clasificado en un conjunto limitado de categorías bien definidas. De esta forma, una taxonomía permite descomponer conceptos o fenómenos complejos en unidades de información más abordables, no sólo permitiendo su estudio sino también proporcionando una base de partida común sobre la cual analizar y clasificar hechos desconocidos hasta el momento.

Para que una taxonomía sea útil, debe estar muy especializada en un área de conocimiento o fenómeno concreto. Hasta la fecha se ha propuesto un gran número de taxonomías centradas en los sistemas de la información, así como taxonomías focalizadas en el área de la seguridad. Existen taxonomías para la clasificación de sistemas de detección de intrusiones [11], errores y vulnerabilidades en los sistemas [12], [13], [14], ataques software [16], incidentes de seguridad en redes de comunicaciones [15], [17] o ataques a dispositivos seguros [21]. Estas taxonomías han permitido profundizar en el estudio de múltiples problemáticas de seguridad mediante la categorización de ataques y vulnerabilidades.

En cuanto a taxonomías relacionadas con firma electrónica, Kain propuso en 2003 una taxonomía no formal de ataques a firmas electrónicas mediante la manipulación del documento a firmar [19]. Sin embargo, la taxonomía no es completa, y se centra exclusivamente en ataques que modifican la semántica del documento, obviando otros muchos tipos de ataque posibles. Otros investigadores han estudiado vulnerabilidades y ataques a tarjetas inteligentes [20], cuyo compromiso claramente afecta a la fiabilidad de la firma electrónica, aunque sólo unos pocos han proporcionado una clasificación rigurosa de ataques a dichos dispositivos [21]. Por otra parte, numerosos trabajos se han centrado en los ataques de canal indirecto, los cuales tienen un gran impacto en la seguridad de los dispositivos criptográficos [22].

Sin embargo, a día de hoy no se ha propuesto ninguna taxonomía que abarque de forma integral y rigurosa los problemas de seguridad que afectan a la firma electrónica. El presente artículo pretende dar respuesta a esta necesidad, ya que las firmas electrónicas se han convertido en un elemento clave en múltiples escenarios, pero todavía no se ha estudiado de forma sistemática las amenazas que pueden influir en la fiabilidad de las mismas. Deseamos que la taxonomía aquí propuesta sirva de guía para diseñar soluciones de firma más seguras y robustas, una vez conocidos los riesgos existentes.

El artículo recoge en primer lugar la motivación en la Sección II. Posteriormente, la Sección III acota el modelo de sistema que tomaremos como objeto de estudio para definir la taxonomía. La Sección IV propone la primera taxonomía completa de ataques a entornos de creación de firma. La evaluación de la taxonomía frente a los requisitos fundamentales para taxonomías se incluye en la Sección V. Por último, se concluye el artículo en la Sección VI.

II. Motivación

La firma electrónica se ha convertido en un elemento fundamental en la sociedad de la información. Numerosas legislaciones de todo el mundo han otorgado a la firma electrónica una equivalencia funcional respecto a la firma manuscrita, así como un reconocimiento como mecanismo de seguridad primordial en transacciones electrónicas, especialmente dentro del ámbito del comercio electrónico [2], [3], [4], [5], [6].

En el caso particular de las legislaciones Europea y Española, la firma electrónica disfruta de plena eficacia jurídica, pudiendo ser empleada como medio de prueba en procedimientos legales [7]. Dependiendo de los requisitos cumplidos por la firma en cuestión, ésta contará con un juicio favorable de validez a priori (*ex ante*) o necesitará de un juicio a posteriori (*ex post*) del Tribunal. En el primer caso, si el supuesto

firmante repudiara el compromiso adquirido en un documento firmado, debería aportar evidencias en sentido contrario y que generaran una duda razonable respecto a la seguridad de la firma. Así pues, la carga de prueba en este escenario recae sobre el supuesto firmante que niega la validez de la firma [1]. En el segundo caso, el supuesto firmante podría también repudiar la autoría de dicha firma pero sería la otra parte afectada quien debiera aportar garantías sobre la seguridad de la misma.

En esta línea, existe también un reconocimiento en los estándares internacionales de proporcionar a las firmas electrónicas (criptográficas) la cualidad de evidencia de no repudio [8]. Una evidencia de no repudio es información que, bien por sí misma o usada en conjunción con otros datos, se emplea para probar la ocurrencia de un evento o acción. Aunque la evidencia no prueba necesariamente por sí misma la veracidad del hecho, sí es usada para tal fin. Por tanto, una evidencia de no repudio que se verifica correctamente de acuerdo a la política de no repudio que aplica es suficiente para resolver una posible disputa, impidiendo al firmante repudiar el compromiso adquirido en la transacción.

Así pues, consideramos imprescindible disponer de las herramientas adecuadas para el estudio riguroso del problema de seguridad de las firmas electrónicas, con el fin de poder asistir al desarrollo de sistemas más seguros que permitan aplicar la legislación con plenas garantías para las partes afectadas. En este sentido, una taxonomía de ataques permitirá conocer dicha problemática, y actuar en consecuencia. Dicha taxonomía no se ha propuesto hasta la fecha.

La taxonomía aquí presentada considera firmas electrónicas generadas mediante criptografía asimétrica (firmas digitales), al ser no sólo una de las posibles tecnologías concretas de implementación sino también la única tecnología que, a día de hoy, es capaz de alcanzar determinados requisitos establecidos en la legislación. En particular, la taxonomía se centra en una de las etapas más sensibles del ciclo de vida de una firma, esto es, la fase de generación.

III. Modelo de Sistema

La Figura 1 muestra el modelo de sistema que tomamos como punto de partida para el estudio de los ataques al entorno de creación de firmas. Dicho modelo se sustenta en el propuesto en el estándar CEN CWA 14170 [9].

La aplicación de creación de firma (SCA) es la aplicación dentro del sistema (SCS) que incorpora la funcionalidad de generación de firmas electrónicas, apoyándose en el dispositivo (seguro) de creación de firmas (S)SCDev. El entorno de creación de firmas (SCE) incluye los entornos físico y lógico del SCS, así como el firmante y las políticas existentes. El SCDev es el dispositivo software o hardware que incorpora los datos de creación de firma (SCD), es decir, la clave privada de firma usada por el firmante para generar las firmas electrónicas. El SSCDev es un SCDev que cumple con los requisitos estipulados en el Anexo III de la Directiva Europea de firma [2]. El acceso al SCD se protege mediante los datos

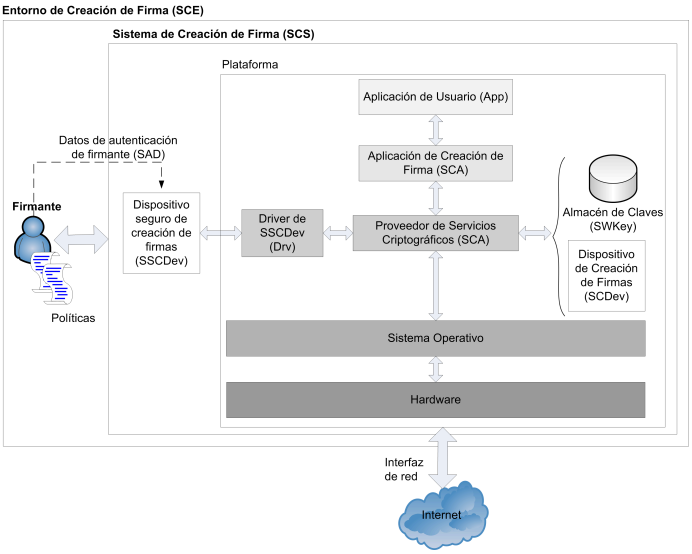

Figura 1. Modelo de Sistema

de autenticación del firmante (SAD), consistentes en un PIN o contraseña.

En este artículo nos referimos al término DTBS cuando los datos a firmar incorporan tanto el documento en sí como una serie de atributos de firma que enriquecen la semántica de dicho documento o particularizan el compromiso adquirido en el acto de firma. Por otra parte, DTBSR se referirá a la representación del DTBS que se envía al SCDev/SSCDev para el cómputo de la firma - generalmente se corresponderá con el resumen criptográfico del DTBS.

IV. Taxonomía de Ataques a Entornos de Creación de Firma

La taxonomía aquí propuesta toma como modelo de sistema el descrito en la Sección III. Así pues, la taxonomía categoriza ataques orientados a comprometer la seguridad del proceso de generación de firmas electrónicas llevado a cabo en un sistema que cumple el modelo indicado.

En particular, la taxonomía está formada por cuatro dimensiones, que se detallan en las siguientes subsecciones. El concepto de dimensión fue introducido por Landwehr et al. [12], y es una propiedad que permite la clasificación de un ataque o vulnerabilidad desde un punto de vista integral. Cada ataque se descompone en varias propiedades, y cada propiedad se emplea para clasificar el ataque desde una perspectiva diferente, todas complementarias entre sí.

Las categorías tienen un identificador asociado consistente en el número de dimensión en el que están englobadas (D) y el número de categoría o subcategoría según el orden jerárquico establecido (CAT).

IV-A. Dimensión Objetivo del Atacante

Esta dimensión cubre el objetivo final del atacante. Identificamos tres categorías dentro de esta dimensión:

D1-CAT1: Firma no consciente de datos

El atacante no hace uso directo de los datos de creación de firma pero desea engañar al firmante para que, de forma no consciente, firme ciertos datos.

D1-CAT2: Uso no autorizado de los datos de creación de firma (SCD)

El atacante desea emplear los datos de creación de firma sin el conocimiento ni consentimiento del firmante. Para ello, el atacante necesitará bien comprometer directamente los datos de creación de firma bien tener acceso a la operación de firma.

D1-CAT3: Sustitución/Modificación de datos firmados

El atacante desea sustituir o modificar parte o la totalidad de los datos firmados, pero una vez que la firma se ha realizado.

IV-B. Dimensión Método de Ataque

Esta dimensión incluye las categorías de método de ataque empleado por el atacante para conseguir uno de los objetivos anteriormente identificados. En concreto, se han diseñado cinco categorías de primer nivel, que se refinan a su vez en subcategorías, y así hasta un cuarto nivel de profundidad en algunos casos:

D2-CAT1: Manipulación del entorno

Esta categoría abarca los métodos que pretenden manipular el entorno (principalmente la Plataforma del SCS) con el fin de influenciar en los datos firmados, bien sea durante la generación de la firma o con posterioridad.

D2-CAT2: Modificación previa a la generación de la firma

Esta categoría contiene los métodos de ataque que intervienen antes de la generación de la firma, y cuyo objetivo es la modificación de los datos a firmar, bien sea de forma directa (modificación del propio contenido a firmar) o indirecta (los datos fraudulentos se incorporan por referencia desde los datos a firmar).

D2-CAT2.1: Modificación de documento. Esta subcategoría de métodos se refiere a las modificaciones realizadas en el documento a firmar.

D2-CAT2.1.1: Adición de contenido dinámico. Esta subcategoría de métodos implica la inclusión de contenido dinámico en el documento a firmar. De esta forma, la sintaxis del documento se mantiene intacta, y por tanto la integridad de la firma, mientras que la semántica variará de acuerdo al comportamiento del código dinámico.

D2-CAT2.1.1.1: Código oculto. El atacante inserta etiquetas especiales o campos ocultos en el documento a firmar. Este código oculto será traducido por determinados valores dependiendo de condiciones específicas que pueden ser controladas por el atacante.

D2-CAT2.1.1.2: Código activo. El atacante inserta código especial, como scripts o macros, en el documento a firmar. Este código se ejecutará durante la apertura o visualización del documento, pudiendo realizar ciertas operaciones como la modificación del contenido mostrado.

D2-CAT2.1.1.3: Vínculos. El atacante inserta vínculos en el documento a firmar que apuntan a contenido externo no controlado por el firmante. Una vez realizada la firma, el atacante puede manipular dicho contenido externo a su antojo.

D2-CAT2.1.2: Modificación de contenido. El atacante modifica el contenido del documento a firmar, pero sin incluir ningún tipo de contenido dinámico (p. e. modificación del propio texto del documento).

D2-CAT2.2: Modificación de atributo. Esta subcategoría de métodos se refiere a las modificaciones realizadas en los atributos a firmar.

D2-CAT2.2.1: Adición de contenido dinámico. Esta subcategoría de métodos implica la inclusión de contenido dinámico en los atributos a firmar. El comportamiento es igual que en el caso anterior para el documento, pero enfocado en los atributos.

D2-CAT2.2.1.1: Código oculto. El atacante inserta etiquetas especiales o campos ocultos en los atributos a firmar. Este código oculto será traducido por determinados valores dependiendo de condiciones específicas que pueden ser controladas por el atacante.

D2-CAT2.2.1.2: Código activo. El atacante inserta código especial, como scripts o macros, en los atributos a firmar. Este código se ejecutará durante la visualización o aplicación de los atributos, pudiendo realizar ciertas operaciones como la modificación del contenido mostrado.

D2-CAT2.2.1.3: Vínculos. El atacante inserta vínculos en los atributos a firmar que apuntan a contenido externo no controlado por el firmante. Una vez realizada la firma, el atacante puede manipular dicho contenido externo a su antojo.

D2-CAT2.2.2: Modificación de contenido. El atacante modifica el contenido de los atributos a firmar, pero sin incluir ningún tipo de contenido dinámico (p. e. modificación del valor de cierto atributos).

D2-CAT2.3: Modificación de DTBS. El atacante modifica la información contenida en la estructura que representa los datos a firmar (DTBS).

D2-CAT2.4: Modificación de DTBSR. El atacante modifica el resumen de los datos a firmar (DTBSR). Este ataque se produciría en la última etapa antes de la computación de firma.

D2-CAT3: Modificación posterior a la generación de la firma

Esta categoría contiene métodos de ataque ejecutados una vez que la firma ha sido realizada, y cuyo objetivo es la modificación de los datos ya firmados, bien sea de forma directa (modificación del propio contenido firmado) o indirecta (modificación de datos referenciados desde los datos firmados).

D2-CAT3.1: Contenido externo. El atacante modifica datos externos referenciados desde los datos firmados (p. e. XSD, DTD). La diferencia entre este método y *D2-CAT2.1.1.3: Vínculos* o *D2-CAT2.2.1.3: Vínculos* radica en que, en este método, el vínculo a los datos externos no se incluye por el atacante, mientras que en estos otros dos casos, es el atacante

quien, de forma explícita, inserta dicho vínculo al contenido externo.

D2-CAT3.2: Criptoanálisis. El atacante aplica métodos de criptoanálisis para obtener un documento o atributos diferentes a los firmados de forma que no se invalide la firma.

D2-CAT3.2.1: Función resumen. El atacante aplica métodos específicamente diseñados para romper la seguridad de la función resumen empleada en el cálculo de la firma.

D2-CAT3.2.1.1: Ataque de colisión. El atacante es capaz de encontrar un par de mensajes $M \neq M'$ donde $hash(M) = hash(M')$ con una complejidad menor a $O(2^{n/2})$ (p. e. ataque del cumpleaños).

D2-CAT3.2.1.2: Ataque de preimagen. El atacante, dado un valor resumen H, es capaz de encontrar un mensaje M' donde $hash(M') = H$ con una complejidad menor que $O(2^n)$.

D2-CAT3.2.1.3: Ataque de segunda preimagen. El atacante, dado un mensaje M, es capaz de encontrar un segundo mensaje M', $M' \neq M$, que satisfaga $hash(M) = hash(M')$ con una complejidad menor que $O(2^n)$.

D2-CAT4: Invocación no autorizada de la operación de firma

Esta categoría recoge los métodos de ataque que no posibilitan al atacante conocer el SCD pero sí hacer uso de él sin el conocimiento ni consentimiento del usuario.

D2-CAT4.1: Compromiso de datos de autenticación de firmante (SAD). Esta subcategoría cubre los métodos que permiten al atacante recuperar el SAD.

D2-CAT4.1.1: Ingeniería social. El atacante manipula o engaña al firmante para que éste revele el SAD.

D2-CAT4.1.2: Intercepción del SAD. El atacante intercepta el SAD durante la operación del SCS.

D2-CAT4.1.2.1: Observación. El atacante observa al firmante introducir el SAD en la Plataforma.

D2-CAT4.1.2.2: Intercepción de comunicación entre procesos/entidades. El atacante intercepta el SAD durante su transmisión entre dos procesos o entidades físicos o lógicos que pertenecen al SCS.

D2-CAT4.1.2.3: Compromiso de extremo. Mediante el compromiso de la seguridad de un extremo (proceso o entidad que interviene en la comunicación del SAD dentro del SCS), el atacante es capaz de interceptar el SAD.

D2-CAT4.1.3: Obtención por prueba y error. El atacante emplea métodos probabilísticos (p. e. ataque de diccionario), técnicas de análisis de emanaciones acústicas del teclado o simplemente un ataque por fuerza bruta para adivinar el SAD.

D2-CAT4.2: Evitación de Autenticación. El atacante evita la autenticación para acceder a la operación de firma.

D2-CAT5: Compromiso de datos de creación de firma (SCD)

Esta categoría incluye métodos que permiten al atacante obtener el SCD. Esta es la categoría que aglutina los métodos de ataque más peligrosos, dado que el atacante podría, una vez conocido el SCD, realizar tantas firmas en nombre del usuario legítimo como deseara, incluso desde un entorno diferente al SCE.

D2-CAT5.1: Intercepción del SCD. El atacante intercepta el SCD durante el proceso de creación o distribución.

D2-CAT5.1.1: Intercepción de comunicación entre procesos/entidades. El atacante intercepta el SCD durante su transmisión entre dos procesos o entidades físicos o lógicos que pertenecen al SCS.

D2-CAT5.1.2: Compromiso de extremo. Mediante el compromiso de la seguridad de un extremo (proceso o entidad que interviene en la comunicación del SCD dentro del SCS), el atacante es capaz de interceptar el SCD.

D2-CAT5.2: Eavesdropping (ataque de canal indirecto). Los ataques de canal indirecto explotan el filtrado de información en base a las características del dispositivo hardware usado durante la ejecución de los algoritmos criptográficos. De esta manera, la clave privada puede llegar a conocerse. La importancia de este tipo de ataques radica en que la complejidad o robustez del algoritmo criptográfico no afecta al éxito del ataque, dado que el fundamento de los ataques de canal indirecto reside en la dependencia entre la información procesada (p. e. la clave privada de firma) y/o las operaciones realizadas por el dispositivo (p. e. tarjeta inteligente) con el comportamiento del hardware subyacente.

D2-CAT5.2.1: Tiempo. Un ataque de análisis de tiempo explota los tiempos de ejecución medidos para un cierto número de operaciones.

D2-CAT5.2.2: EMA. Un ataque de análisis electromagnético (EMA) explota la correlación entre los datos secretos y las variaciones en las radiaciones emitidas por los dispositivos.

D2-CAT5.2.3: Potencia. Un ataque de análisis de potencia analiza la relación entre el consumo de potencia de un dispositivo criptográfico y los datos manejados durante las operaciones criptográficas.

D2-CAT5.2.4: Microarquitectural. Un ataque de análisis microarquitectural estudia los efectos que los componentes pertenecientes a los procesadores comunes y su funcionalidad tienen sobre la seguridad de los criptosistemas software.

D2-CAT5.2.5: Observación óptica. Las emanaciones ópticas también pueden filtrar información al atacante. En caso que los datos procesados por un dispositivo que emanara este tipo de señales se correspondieran con el SCD, el atacante podría comprometerlo.

D2-CAT5.3: Acceso no autorizado al SCDev. El atacante compromete el SCD accediendo al SCDev donde se almacena.

D2-CAT5.3.1: Compromiso de datos de autenticación de firmante (SAD). El atacante es capaz de extraer el SCD una vez conocido el SAD. Este método de ataque requiere que el SCD sea exportable. Esta subcategoría se ramifica a su vez en las mismas subcategorías que *D2-CAT4.1 Compromiso de datos de autenticación de firmante (SAD)*.

D2-CAT5.3.2: Evitación de Autenticación. El atacante es capaz de acceder al SCD (y leerlo) incluso sin necesidad de conocer el SAD. Este método de ataque requiere que el SCD pueda ser leído.

D2-CAT5.4: Criptoanálisis. El atacante aplica métodos de criptoanálisis para conocer el SCD.

D2-CAT5.4.1: Algoritmo asimétrico. Esta subcategoría recopila cualquier ataque centrado en comprometer la clave privada usada en el algoritmo asimétrico concreto. Existen múltiples algoritmos asimétricos que pueden emplearse para realizar una firma electrónica basada en criptografía (p. e. RSA, DSA, curva elíptica, etc.). Dependiendo del algoritmo, el conjunto de posibles métodos de ataque variará.

No todos los métodos de ataque pueden permitir al atacante alcanzar los tres objetivos establecidos en la primera dimensión. El Cuadro I relaciona las categorías de la primera dimensión con las categorías de primer nivel de la segunda dimensión.

IV-C. Dimensión Patrón de Ataque

Un patrón de ataque describe cómo un tipo de ataque observado se lleva a cabo. Es la descripción del mecanismo empleado para explotar un sistema pero desde el punto de vista del atacante. CAPEC (Common Attack Pattern Enumeration and Classification) [10] es una extensa colección de patrones de ataque que se considera un referente a nivel mundial. Es una base de datos pública y cuyos patrones de ataque se generan tras un análisis exhaustivo de ataques reales. Para cada patrón de ataque se proporcionan datos relevantes como el flujo de ejecución del ataque o los requisitos que deben cumplirse para que el ataque pueda ser llevado a cabo.

En esta dimensión se incluye una selección de patrones de ataque de entre los 287 existentes actualmente en CAPEC. El criterio de selección no ha sido otro que el análisis de aplicabilidad de cada patrón de ataque en base al modelo de sistema planteado, y cuya instanciación pudiera comprometer la seguridad de un proceso de generación de firma. Se han identificado 192 patrones de ataque válidos que, por cuestiones de espacio, no se incluyen en el artículo.

IV-D. Dimensión Objeto del Ataque

Esta dimensión categoriza los posibles elementos que pueden ser objeto del ataque. Un ataque puede afectar a uno o varios elementos, por lo que la clasificación de un ataque podría necesitar la selección de varias categorías de esta dimensión (véase Sección IV-E).

Por cuestiones de espacio y relevancia en relación con otras dimensiones, no se proporciona un listado de las categorías existentes ni una descripción de las mismas. Simplemente se indican a continuación las categorías de primer nivel: D4-CAT1: Criptografía, D4-CAT2: Software, D4-CAT3: Hardware, D4-CAT4: Usuario.

IV-E. Método de Clasificación

El método de clasificación de una taxonomía debe guiar a un usuario de forma clara y unívoca en la clasificación de un nuevo elemento. Para clasificar un ataque en base a la taxonomía aquí presentada, deben seguirse los siguientes pasos:

1. Debe identificarse el objetivo del ataque, y clasificarse de acuerdo a la dimensión *Objetivo del Atacante*.
2. Una vez conocido el objetivo, debe clasificarse el método empleado por el atacante para alcanzar dicho objetivo, de acuerdo a la dimensión *Método de Ataque*, y la Tabla I. El método debe clasificarse en la subcategoría de mayor profundidad posible.
3. El patrón de ataque concreto empleado debe seleccionarse de acuerdo a la dimensión *Patrón de Ataque* y la información existente en la base de datos de CAPEC. Al igual que en el caso del método, debe seleccionarse el patrón de ataque más concreto posible.
4. Deben identificarse los elementos del SCE que se ven afectados de forma directa o indirecta por el ataque, y clasificarse en base a la dimensión *Objeto del Ataque*. En caso que el ataque afecte a más de un elemento, deberán seleccionarse varias instancias (categorías) de esta dimensión.
5. En cada paso, si se detecta la necesidad de añadir una nueva categoría o subcategoría, ésta debe incorporarse a la taxonomía, y clasificar el ataque como corresponda.

Así pues, un ataque se clasificará con una categoría de la dimensión *Objetivo del Atacante*, una (sub)categoría de la dimensión *Método de Ataque*, una (sub)categoría de la dimensión *Patrón de Ataque*, y una o varias (sub)categorías de la dimensión *Objeto del Ataque*.

V. Evaluación de la Taxonomía

Una taxonomía debe satisfacer una serie de requisitos generales [18]. Una taxonomía debería ser *ampliamente aceptada* en el campo de aplicación. La taxonomía propuesta se fundamenta en trabajos previos que han tenido un fuerte impacto en la comunidad científica. Así mismo, la taxonomía aplica el diseño basado en dimensiones, que ha demostrado ofrecer una perspectiva integral del campo de estudio abordado. Por ello, y por la falta actual de una taxonomía centrada en ataques a firma electrónica, creemos que la taxonomía aquí propuesta será un primer paso en el estudio de esta problemática.

La taxonomía debería ser *exhaustiva* en el sentido de que pudiera cubrir la clasificación de cualquier elemento dentro del campo de estudio. Este requisito es difícil de cumplir dado que no es posible conocer todos los ataques existentes a firmas electrónicas, especialmente en un campo tan dinámico como el de la seguridad. Sin embargo, la evaluación de la taxonomía frente ataques reales es fundamental para verificar su completitud. En este sentido, se ha llevado a cabo de forma satisfactoria una clasificación de 70 ataques encontrados en la literatura, pero que, por motivos de espacio, no se incluyen en el artículo.

Las categorías de la taxonomía deberían ser *excluyentes entre sí*, de forma que cada ataque fuera clasificado exclusivamente en una categoría de cada dimensión. El diseño de la taxonomía y el método de clasificación aseguran este principio. La posibilidad de seleccionar varias categorías en la dimensión *Objeto del Ataque* no implica que se viole este requisito, sino

Objetivo	Método
D1-CAT1: Firma no consciente de datos	D2-CAT1: Manipulación del entorno D2-CAT2: Modificación previa a la generación de la firma
D1-CAT2: Uso no autorizado de los datos de creación de firma (SCD)	D2-CAT4: Invocación no autorizada de la operación de firma D2-CAT5: Compromiso de datos de creación de firma (SCD)
D1-CAT3: Sustitución/Modificación de datos firmados	D2-CAT3: Modificación posterior a la generación de la firma

Cuadro I
RELACIÓN ENTRE DIMENSIÓN OBJETIVO Y DIMENSIÓN MÉTODO

que la taxonomía permite la clasificación de varios elementos afectados por el ataque si fuera necesario.

El método de clasificación debería ser *determinista* y *repetible* en base al diseño de la taxonomía. El método aquí proporcionado es claro, sencillo e inequívoco teniendo en cuenta las dimensiones diseñadas.

La taxonomía debería emplear *terminología ampliamente aceptada* y ser *apropiada*, basándose en un modelo claro de referencia. La terminología y modelo de sistema empleados en la presente taxonomía se derivan de los estándares actuales. Así mismo, el modelo acota exactamente los elementos de alto nivel que intervienen y las relaciones entre ellos.

Para ser útil, una taxonomía debería estar *especializada* en un área de conocimiento concreta. En nuestro caso, la taxonomía se centra en ataques a entornos de creación de firmas electrónicas basadas en criptografía de clave pública.

Por último, la taxonomía debería ser *útil*. En este sentido, la taxonomía propuesta permite la clasificación sistemática de ataques a entornos de creación de firmas, lo cual sin duda redundará en un mayor conocimiento a la hora de diseñar soluciones más eficaces no sólo contra ataques conocidos sino contra ataques potenciales todavía por aparecer.

VI. CONCLUSIONES

La importancia de la firma electrónica, con su amplio reconocimiento por las legislaciones y estándares internacionales vigentes, así como las consecuencias que de ella se derivan, nos llevan a la necesidad de diseñar sistemas y soluciones robustos ante las amenazas existentes y futuras, por otra parte numerosas. Una taxonomía de ataques permitiría categorizar los ataques posibles de forma genérica y abstracta, beneficiando el estudio de contramedidas globales aplicables a cualquier entorno de firma.

Aunque se han propuesto numerosas taxonomías en el ámbito de la seguridad, ninguna ha abordado de manera integral el problema de seguridad de las firmas electrónicas. En este artículo se ha presentado la primera taxonomía de ataques a entornos de creación de firma electrónica. La taxonomía se ha dividido en cuatro dimensiones, lo cual permite el análisis y clasificación de ataques desde un punto de vista holístico. La taxonomía se ha validado satisfactoriamente frente a los requisitos y principios fundamentales para taxonomías, incluyendo el requisito de completitud mediante la clasificación de setenta ataques publicados en la literatura (no incluidos en el presente artículo).

Como trabajo futuro se ampliará la taxonomía incorporando categorías de ataque orientados a la fase de verificación (p. e. aprovechar la latencia en la actualización de CRL para firmar con un certificado revocado). Como resultado, se dispondrá de una taxonomía completa de ataques a la firma electrónica, posibilitando la clasificación y estudio de cualquier ataque que afecte a su fiabilidad como evidencia de no repudio.

REFERENCIAS

[1] A. McCullagh and W. Caelli. Non-repudiation in the digital Environment. First Monday, vol. 5, no. 8, 2000.

[2] 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.

[3] Ley 59/2003, de 19 de Diciembre, de Firma Electrónica, 2003.

[4] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, United Nations, 2001.

[5] Electronic Signatures in Global and National Commerce Act (e-sign). Federal Trade Commission, Department of Commerce. United States of America. 30 Junio, 2000.

[6] Personal Information Protection and Electronic Documents Act. Department of Justice. Government of Canada. 30 Mayo, 2008.

[7] D. Cruz Rivero. Eficacia formal y probatoria de la firma electrónica. Marcial Pons (Ed.). ISBN: 84–9768–353–6, 2006.

[8] ISO/IEC 13888-3 Information technology – Security techniques – Non repudiation – Part 3: Mechanisms Using Asymmetric Techniques. 2009.

[9] CEN CWA 14170 – Security Requirements for signature creation applications. The European Committee for Standardization (CEN), 2004.

[10] Common Attack Pattern Enumeration and Classification (CAPEC) - A Community Knowledge Resource for Building Secure Software. MITRE.

[11] A. Axelsson. Intrusion Detection Systems: a Survey and Taxonomy. Technical Report No 99-15, Department of Computer Engineering, Chalmers University, Gothenburg, 2000.

[12] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi. A taxonomy of computer program security flaws. ACM Computing Surveys, vol. 26, no. 3, pp. 211–254, 1994.

[13] M. Bishop. A taxonomy of (Unix) system and network vulnerabilities. Technical Report CSE–9510. Department of Computer Science, University of California, 1995.

[14] F. Piessens. A taxonomy of causes of software vulnerabilities in Internet software. 13th International Symposium on Software Reliability Engineering, pp. 47–52, 2002.

[15] U. Lindqvist and E. Johsson. How to Systematically Classify Computer Security Intrusions. IEEE Security and Privacy, pp. 154–163. 1997.

[16] H. Langweg and E. Snekkenes. A Classification of Malicious Software Attacks. Proceedings of 23rd IEEE International Performance, Computing, and Communications Conference, 2004.

[17] S. Hansman. A Taxonomy of Network and Computer Attack Methodologies, technical report, Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, 2003.

[18] D. L. Lough. A taxonomy of computer attacks with applications to wireless networks. Tesis Doctoral, 2001.

[19] K. Kain. Electronic Documents and Digital Signatures. Doctoral Thesis, 2003.

[20] P. Girard, J-L. Giraud. Software attacks on smart cards. Information Security Technical Report, vol. 8, no. 1, pp. 55–66. 2003.

[21] A. J. Rae, L. P. Wildman. A Taxonomy of attacks on secure devices. Proceedings of the Fourth Australian Information Warfare and IT Security Conference, pp. 251–264. 2003.

[22] The side-channel cryptanalysis lounge. European Network of Excellence in Cryptology.