

Un requisito esencial para el adecuado crecimiento del comercio electrónico y de la administración electrónica es que los protocolos subyacentes a las aplicaciones de estas dos áreas proporcionen las adecuadas propiedades de seguridad. Sin embargo, no existe aún una metodología clara para la fase de diseño de los protocolos de seguridad en tales ámbitos, y tampoco una metodología adecuada para el análisis de los mismos una vez que han sido diseñados. Es precisamente en este área en la que el proyecto europeo CASENET se sitúa, de tal forma que su objetivo general es el desarrollo de metodologías y herramientas para construir protocolos seguros y fiables que puedan ser utilizados en aquellas aplicaciones que involucren transacciones electrónicas. Sin duda, el comercio-e y el gobierno-e son dos claros ejemplos.

Proyecto CASENET: integración del diseño y análisis de protocolos seguros para el comercio-e

INTRODUCCIÓN

Recientemente, la Comisión Europea aprobó el proyecto **CASENET** (*Computer-Aided solutions to Secure ElectroNic commerce Transactions*) dentro del V Programa Marco de Desarrollo e Investigación Tecnológica, y más concretamente, como proyecto del **Programa IST** (*Information Society Technologies Programme*) cuyo presupuesto para el periodo 1998-2002 asciende a más de 3.500 MEuros.

CASENET, que oficialmente dio comienzo el pasado 1 de diciembre, tendrá una duración de 2 años y un presupuesto de casi de 3,7 MEuros, del que parte será subvencionado por la Comisión Europea dentro de las líneas de acción II.4.1. -*Trust in Information Infrastructures*- y II.4.2. -*Enhancing Security in Electronic Transactions*- del citado Programa IST.

El uso de Internet, en general, y de la WWW y de su equivalente inalámbrica en particular, ha abierto desde no hace mucho un escenario completamente nuevo tanto para el comercio-e como para el gobierno-e, y son precisamente estas áreas dos de las más potenciadas por el IST. Tanto los nuevos servicios, como los ya existentes, trasladados a Internet y con una calidad mejorada, están generando grandes beneficios y pueden generar beneficios mucho mayores. Sin embargo, el potencial crecimiento de los negocios en el mundo digital puede ser bruscamente frenado por los problemas relacionados con la seguridad de las aplicaciones que se ejecutan en los sistemas conectados a la Red.

Es notoria y bien conocida la falta de seguridad en Internet. Las aplicaciones *on-line* no sólo son susceptibles de fallos, sino que, además, están expuestas a ataques activos si no se diseñan y se verifican apropiadamente. Estos fallos y los ataques potenciales pueden causar (y de hecho han causado) un grave daño a los agentes participantes en las transacciones comerciales (empresas de la industria, instituciones financieras, proveedores de servicio y, por supuesto, consumidores). Además de una pérdida financiera directa, la pérdida de datos críticos o de información confidencial puede causar un daño incalculable a todo tipo de participantes.

Una solución común para dotar de seguridad a las aplicaciones finales de comercio-e y gobierno-e es la utilización de protocolos criptográficos en el nivel de aplicación de la pila de protocolos OSI. Cada protocolo criptográfico puede proporcionar esos servicios de seguridad que cada aplicación final necesita. Con una demanda cada vez mayor para proporcionar seguridad a numerosos tipos de aplicaciones de los ámbitos referidos, estamos asistiendo

también a una incipiente demanda de procedimientos de diseño e implementación de protocolos criptográficos fiables. Sin embargo, y de forma simultánea, se afronta el problema de que el número de expertos e investigadores de calidad en el área de la seguridad es proporcionalmente pequeño. Como resultado, muchos protocolos criptográficos están siendo diseñados, y continuarán siéndolo, por ingenieros de software cuya vocación es resolver problemas generales en las aplicaciones, y sin una experiencia adecuada en criptografía y seguridad de la información.

La complejidad natural de los sistemas informáticos en red ha sido la principal causa de fallos de diseño e implementación en los sistemas hardware y software. Los sistemas que usan protocolos criptográficos están abiertos a todavía mayores causas de fallos porque las primitivas criptográficas han de ser diseñadas para interactuar con entornos absolutamente hostiles. Debido a esto, ocurre que, a menudo, los protocolos criptográficos son vulnerables a fallos, aún siendo diseñados por expertos en el área de seguridad. Por ejemplo, los diversos fallos ocultos en los protocolos de Needham-Schroeder [NeSc78] sirven de lección sobre la falta de fiabilidad en los protocolos diseñados incluso por expertos en seguridad.

El objetivo de los métodos formales para la especificación, diseño, modelado y análisis de sistemas es ayudar a construir sistemas más fiables. En el caso de los protocolos criptográficos, la fiabilidad implica alcanzar propiedades de seguridad tales como confidencialidad, autenticidad, disponibilidad, determinación de responsabilidades, y un largo etcétera.

Precisamente, el proyecto CASENET va a tomar como base el estado de la tecnología para la especificación, diseño, modelado y análisis formal de protocolos criptográficos para diseñar y desarrollar herramientas específicas que permitan a los usuarios, expertos o no, alcanzar los objetivos de seguridad que las aplicaciones a desarrollar han de contener.

DESCRIPCIÓN Y ORGANIZACIÓN DEL CONSORCIO

El consorcio de CASENET incluye nueve socios, que se pueden subdividir en tres grupos, a saber: **i**) socios que están involucrados en las labores básicas de investigación y desarrollo, **ii**) socios que aportarán aplicaciones reales donde probar e integrar los resultados proporcionados por los del primer grupo, y **iii**) socios que incorporarán los resultados finales en herramientas propias o por desarrollar, para una posterior comercialización en el sector.

Respecto al primer grupo de socios, los de investigación, componen el **consorcio Hewlett Packard Laboratories** de Bristol (Reino Unido), el **Institute for Secure Telecooperation (SIT)** del **Fraunhofer Gesellschaft** (anteriormente GMD, principal instituto de investigación en Alemania), el **Departamento de Lenguajes y Ciencias de la Computación de la Universidad de Málaga** (España) y el **Norwegian Computing Center -NR-** (Noruega). Estos cuatro socios investigadores proporcionan la experiencia necesaria para el desarrollo de las metodologías. Así, la labor principal de NR se centra en el área de los métodos y lenguajes de especificación, contribuyendo a la selección y desarrollo de herramientas y métodos para la especificación y el diseño. Por otro lado, la labor de la Universidad de Málaga se centra en el desarrollo de metodologías y herramientas de diseño de protocolos de seguridad, así como y en todas las cuestiones relacionadas con la seguridad en el comercio electrónico. SIT posee una considerable experiencia en el análisis de protocolos de seguridad por lo que es esa su área de atención dentro del proyecto. Finalmente, HP Labs. proporciona una dilatada experiencia en la investigación de primitivas criptográficas, base de todos los protocolos de seguridad.

En el segundo grupo, hay dos socios del ámbito empresarial y uno del ámbito gubernamental. Más concretamente, **NetUnion** (Suiza) y **Sadiel S.A.** (España) son los socios dentro del ámbito empresarial que dotan al consorcio de escenarios de prueba específicos consistentes en aplicaciones y protocolos de comercio-e y gobierno-e a desarrollar o mejorar. La ciudad de Colonia (Alemania) proporcionará el escenario de prueba del ámbito de la Administración Pública. Todos estos socios proporcionan enlaces a comunidades de usuarios candidatas para las pruebas. Además, durante la ejecución del Proyecto, y en estrecha colaboración con los socios de investigación, identificarán y especificarán las transacciones relevantes y los requisitos de seguridad de sus aplicaciones, validando y evaluando las metodologías y herramientas resultantes de CASENET dentro de sus aplicaciones respectivas. La realimentación a los socios investigadores permitirá un mayor refinamiento de las metodologías y herramientas.

Finalmente, el tercer grupo, el del sector de socios industriales que se centrará en la comercialización de las metodologías y herramientas finales del proyecto está formado por las empresas **Solinet** (Alemania) y **Teletel** (Grecia). Está previsto que ambas, como compañías de desarrollo de sistemas de telecomunicación, utilicen los resultados de CASENET para extender su sistema *Safire*, un entorno propio de desarrollo y ejecución de protocolos. La extensión de *Safire* es contemplada como un avance tecnológico decisivo en la industria, proporcionando un marco de trabajo cómodo para la especificación de transacciones comerciales electrónicas, y la producción de protocolos con propiedades de seguridad probadas.

Debido a que la gestión de un proyecto de esta envergadura es muy elevada, se han separado los asuntos administrativos de los técnicos para una mejor eficiencia, creando dos comités diferentes. El primero de ellos, el *Comité de Administración* del Proyecto tiene como objetivo establecer, ejecutar y asegurar la producción de resultados del proyecto de acuerdo al calendario establecido. Además, este Comité también aprobará, autorizará, corregirá y revisará asuntos concernientes a la organización del proyecto, incluyendo la relación con la Comisión Europea y la colaboración con otros consorcios europeos, los asuntos de propiedad intelectual, el control financiero y la asignación de presupuestos. El Comité estará dirigido por la **Dra. Sigrid Gürgens** del SIT.

El segundo, el *Comité Técnico* del Proyecto, estará encargado de discutir y planificar las cuestiones técnicas. Será también responsable de la revisión de los documentos técnicos producidos

por el consorcio, de poner en marcha los mecanismos adecuados para asegurar la viabilidad técnica de la serie de entregables del consorcio a la Comisión Europea, así como de las tareas técnicas a realizar por cada uno de los socios individualmente. Por último, también tendrá como misión identificar la necesidad de organizar reuniones técnicas con personal investigador de otros consorcios. Este comité estará dirigido por el **Dr. Javier López**, de la Universidad de Málaga.

CÓMO SE ENMARCA CASENET EN EL MARCO GENERAL DEL COMERCIO-E

Tradicionalmente, las tecnologías utilizadas para permitir el comercio-e han existido mayoritariamente en entornos cerrados. El potencial del comercio-e sólo se ha podido llevar a cabo parcialmente por todos los agentes económicos involucrados en las Tecnologías de la Sociedad de la Información. Ejemplo de ello son los millones de pymes europeas que son la fuente de la actividad económica, de empleos y de innovación de servicios en Europa. De forma similar, las Administraciones Públicas y los ciudadanos prácticamente no se han beneficiado aún de esta nueva tecnología emergente.

La Comisión Europea, tanto en el IV como el V Programa Marco, ha estimulado los proyectos de comercio-e y negocio-e. El objetivo principal ha sido animar el desarrollo y el despegue del comercio electrónico en las pymes, en los sectores públicos regionales y locales y en los ciudadanos de los estados miembros de la Unión Europea, pretendiendo asegurar la competitividad de los negocios europeos en el mercado global.

Sin embargo, y como promulga la Comisión Europea, el comercio-e, como dominio de investigación y desarrollo tecnológico, necesita estrategias investigadoras que se puedan estructurar en un conjunto de proyectos complementarios. Esta idea es la que intenta reflejar la **figura 2**, divulgada en algunos documentos de la propia Comisión. Se puede observar que los diferentes dominios de investigación se han clasificado en diferentes niveles, de tal forma que cada uno depende de los situados por debajo de él.

Como ya se ha comentado, el objetivo de CASENET es desarrollar e implementar un marco de trabajo de herramientas para producir protocolos cuyas propiedades de seguridad hayan sido probadas. Esto indica claramente que el área de investigación relevante del proyecto es la localizada en el recuadro de tecnología subyacente de la figura, es decir, en el nivel sobre el que se sustentan todos los demás niveles.

Dentro del IV y V Programa Marco se ha dedicado un gran esfuerzo de investigación a proyectos interesantes que se han concentrado en temas relacionados con los niveles superiores de la figura anterior. Sin embargo, la tecnología de seguridad subyacente utilizada en ellos ha sido, fundamentalmente, la desarrollada tiempo atrás para las aplicaciones de red tradicionales, cuyos requisitos rara vez han superado el de la simple distribución de claves o de autenticación de usuarios. Estos requisitos sólo cubren parcialmente el conjunto global de necesidades de las redes abiertas y distribuidas, no habiendo existido hasta el momento ningún proyecto dedicado a proporcionar la mencionada tecnología subyacente de seguridad. CASENET se posiciona aquí.

Debido a que los requisitos de aplicaciones de comercio-e y gobierno-e son, en esencia, diferentes de las de las aplicaciones tradicionales, muchos protocolos que han funcionado correctamente durante años pueden contener agujeros de seguridad que no se pueden detectar con facilidad al trasladarlos a los nuevos entornos. Peor aún, los protocolos que están siendo desarrollados en la actualidad para ser utilizados en las transacciones comerciales

Nombre de Entidad	Dirección Web
Ciudad de Colonia	http://www.stadt-koeln.de
Fraunhofer Gesellschaft (Institute for Secure Telecooperation)	http://sit.gmd.de
Hewlett-Packard Labs. - Bristol	http://www.hpl.hp.com
NetUnion	http://www.netunion.com
Norwegian Computing Center	http://www.nr.no
Sadiel S.A.	http://www.sadiel.es
Solinet	http://www.solinet.com
Teletel	http://www.teletel.gr
Universidad de Málaga (Dpto. Lenguajes y Ciencias de la Computación)	http://www.lcc.uma.es

Figura 1. Entidades componentes del consorcio CASENET

no tienen garantizado el estar libre de errores, ya que las herramientas y los métodos para analizarlos no están diseñados para capturar los especiales requisitos de las aplicaciones de comercio-e.

CASENET proporcionará a los suministradores de tecnología los mecanismos, herramientas y software que han de formar la base sólida sobre la que construir los diferentes niveles de la figura 2. Por lo tanto, los resultados innovadores del proyecto serán de beneficio no sólo para los niveles que componen el comercio-e, sino también para otras categorías de administración de procesos de negocio como sistemas de negocio electrónico, plataformas de colaboración, herramientas de soporte a empresas virtuales, así como para las capas más altas, que incluyen proyectos que unirán redes de negocio de sectores industriales.

ESTADO DE LA TÉCNICA E INNOVACIÓN TECNOLÓGICA

Dentro del área del diseño de protocolos criptográficos existen algunos buenos documentos que sirven de guías de referencias, como por ejemplo, el informe técnico de la DEC «*Prudent Engineering Practice for Cryptographic Protocols*» de Abadi y Needham [AbNe94], o el artículo «*Robustness Principles for Public Key Protocols*» de Anderson y Needham [AnNe95]. Sin embargo, estas guías de referencia no forman una teoría computacional y, por lo tanto, no conducen a ningún método de análisis automático (ni siquiera asistido por ordenador) para razonar sobre la seguridad de un protocolo.

Por otro lado, el análisis formal ha mostrado ser eficiente para identificar fallos de seguridad en muchos protocolos de distribución de claves y de autenticación. El primer intento serio de formalizar el concepto de «protocolo correcto» fue la Lógica de Autenticación de Burrows, Abadi y Needham [BAN89]. Uno de los defectos de esta Lógica fue la falta de un modelo formal con el que definir las semánticas de la misma.

Kailar, en [Kai196], argumentaba de forma convincente que lo realmente importante en las aplicaciones de comercio electrónico no es lo que uno cree (en alusión a la BAN), sino probar la responsabilidad. Así, proporciona una sintaxis que permite expresar tales propiedades y un conjunto de reglas para verificarlas. De forma similar a la Lógica BAN, la propuesta de Kailar carece de un modelo semántico formal.

Heintze y Tygar [HeTy96] estudiaron los protocolos como conjuntos de agentes modelados con máquinas de estado finito no deterministas, a la vez que no restringían las acciones de los adversarios sobre el protocolo. Este modelo captaba bien el problema de seguridad, pero el problema asociado de indecidibilidad limitaba el valor práctico del modelo.

Meadows [Mead95] desarrolló un testeador de modelos en Prolog, denominado analizador de protocolos NRL. En su funcionamiento, el usuario suministraba una descripción de un estado inseguro y la búsqueda en Prolog intenta encontrar un estado inicial. Un problema serio es que no se garantizaba que el algoritmo de *backtracing* del Prolog terminara.

Woo y Lam [WoLa93] propusieron un modelo intuitivo para la autenticación de protocolos. Su modelo se asemeja a la programación secuencial, donde cada entidad es modelada independientemente. Ese modelo no proporciona una herramienta automática y aunque la descripción de mismo es bastante intuitiva, no es formal.

Lowe [Lowe96] usó el testeador de modelos FDR para CSP, y encontró un error desconocido anteriormente en el protocolo de

autenticación de clave pública de Needham-Schoeder. Sin embargo, el modelo CSP está lejos de seguir adelante. Además, está restringido a una única ejecución del protocolo como resultado de estar parametrizado por los valores utilizados por los participantes.

Más recientemente, Schneider [Schn98] utilizó CSP para modelar protocolos en un entorno hostil y para expresar propiedades de seguridad. La verificación se llevaba a cabo descubriendo una función de clasificación. Sin embargo, en la práctica, la construcción de una función de este tipo con todas las propiedades requeridas es difícil.

También recientemente, Gürgens, López y Peralta [GLP99] usaron el probador de teoremas Otter para analizar un protocolo dentro de una aplicación de firma digital en tarjetas inteligentes, encontrando un fallo de seguridad desconocido previamente. Sin embargo, no ha quedado completamente claro cuál es la capacidad de automatización de la estrategia de búsqueda de Otter.

A partir del trabajo anterior de Meadows, Syverson y Meadows [SyMe98] especificaron algunos requisitos para las transacciones de pago en el protocolo SET, usando una variación del NRL. Posteriormente se comenzó un trabajo en el que usaba NRL para analizar sus especificaciones.

Actualmente no está claro cuál de las soluciones existentes (o de sus combinaciones) para análisis de protocolos de seguridad será de utilidad práctica en el ámbito de los protocolos de comercio-e y gobierno-e. Tampoco está claro si el actual estado de la técnica, en los que el análisis y el diseño de protocolos se tratan

de forma separada, dará lugar a algún método de análisis que sea viable.

Hasta la fecha, no existe ningún método integrado de análisis y diseño para el desarrollo de protocolos criptográficos seguros en las áreas de aplicación ya mencionadas. CASENET pretende hacerlo. Más aún, una de sus metas es que las metodologías y herramientas resultantes del proyecto proporcionen un procedimiento asistido por ordenador para desarrollar sistemáticamente protocolos de comercio electrónico, comenzando, obviamente, por una definición clara de los servicios de seguridad a satisfacer, y finalizando con una especificación del protocolo acompañada con el resultado de un razonamiento formal

de las propiedades de seguridad. No cabe duda de que la integración del diseño y el análisis representarán una contribución técnica innovadora.

Ahondando en la innovación proporcionada por el proyecto CASENET, es necesario decir que éste dotará de la posibilidad de garantizar el cumplimiento de los requisitos de los usuarios, así como de la legislación en las transacciones que requieran privacidad y seguridad. Más concretamente, los requisitos de las directivas comunitarias y las legislaciones nacionales en áreas tales como la privacidad de datos y la firma digital son complejas, y además, las necesidades de los usuarios en estas áreas aparecen, con bastante frecuencia, distorsionadas. No cabe duda de que la capacidad de definir estos requisitos de una manera formal, y que todos y cada uno de ellos sean observados por los protocolos que lo implementan, es una de las mayores contribuciones para cumplir la legislación, la auditoría de transacciones y la resolución de disputas.

El proyecto alcanzará esta innovación mediante: **a)** desarrollo de métodos formales, técnicas y herramientas para la formalización de transacciones y requisitos de seguridad necesarios; **b)** desarrollo de metodologías y herramientas para la generación de protocolos que contengan propiedades de seguridad que puedan ser fuertemente validadas frente a esos requisitos, y **c)** propor-

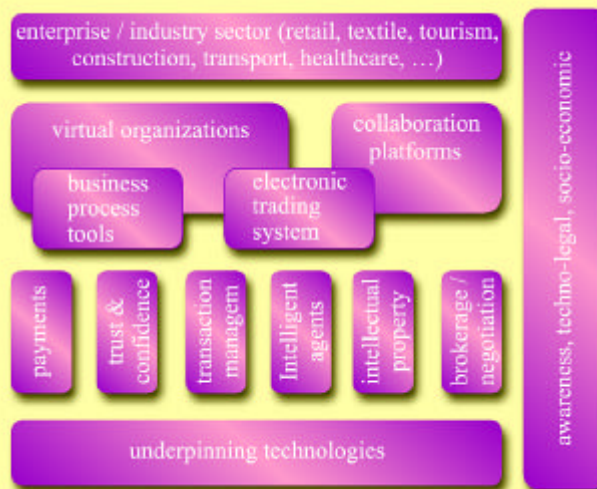


Figura 2. Niveles de dominios de investigación

cionar un conjunto de métodos y herramientas integrado para los puntos a y b.

CASENET también pretende promover la innovación en la parcela de los negocios porque proporcionará una metodología eficiente y robusta para el prototipado de aplicaciones seguras de comercio electrónico, así como de modelos de negocios. Estos resultados mejorarán el crecimiento de nuevos servicios y permitirán una evaluación más rápida de un número mayor de potenciales escenarios de implantación.

Además, el hecho de que los resultados de CASENET se examinen en los tres escenarios de prueba ya mencionados en secciones anteriores, asegurará una participación importante de usuarios finales en el proceso de I+D, y proporcionará una plataforma válida para la aplicación de los resultados del proyecto.

OBJETIVOS ESPECÍFICOS Y TAREAS DEL PROYECTO

El objetivo global del proyecto CASENET es desarrollar e implementar un marco de trabajo de herramientas software para, de una manera formal y sistemática, especificar, modelar, analizar e implementar protocolos criptográficos que proporcionen seguridad al comercio electrónico y las transacciones comerciales. Esto plantea objetivos específicos que se han contemplado como tareas concretas en el proyecto:

- *Desarrollar metodologías que permitan la especificación formal y el modelado de protocolos criptográficos.* Una herramienta bajo esa metodología puede ayudar al diseñador de un protocolo de seguridad a especificar los requisitos de seguridad de una transacción, así como a modelar el comportamiento de un protocolo que es diseñado para conseguir transacciones seguras. El formalismo de las metodologías permite que éstas se puedan realizar de forma rutinaria y, por lo tanto, puede facilitar la especificación e incrementar la precisión del modelo.

El proyecto producirá un documento que especifica la metodología necesitada por un usuario para definir un protocolo con un propósito especial. Además, también producirá una herramienta software que, tomando como entrada un lenguaje de especificación formal, produzca una salida en un lenguaje de especificación de bajo nivel. A partir de este punto, la metodología también ayudará a transformar esta última especificación en código de programa.

- *Desarrollar metodologías de análisis que permitan el análisis formal de los protocolos criptográficos.* Con la semántica formal definida bajo estas metodologías, una herramienta puede entender la especificación de los requisitos de seguridad, el comportamiento del protocolo modelado y los escenarios específicos de ataque, así como realizar comparaciones cuantitativas y cualitativas entre ellos. En el caso de presencia de fallos de seguridad (por ejemplo, el comportamiento no cumple con los requisitos), se podrá modificar el diseño del protocolo, remodelando el comportamiento, y, de esta forma, volver a repetir el análisis hasta que el análisis

no encuentre ningún fallo. En esta tarea se producirá una especificación formal de la metodología de análisis y la herramienta que toma esa especificación como entrada y produce los resultados del análisis.

- *Desarrollar un conjunto de herramientas software que implemente las metodologías mencionadas.* Las herramientas incluirán paquetes para la especificación, el modelado y el análisis. También incluirán un paquete para el diseño del protocolo, y un paquete para chequear un protocolo que haya pasado a través del proceso de análisis formal.

La figura 3 resume bien los distintos componentes que la solución proporcionada por CASENET pretende aportar, así como la interrelación entre todos ellos.

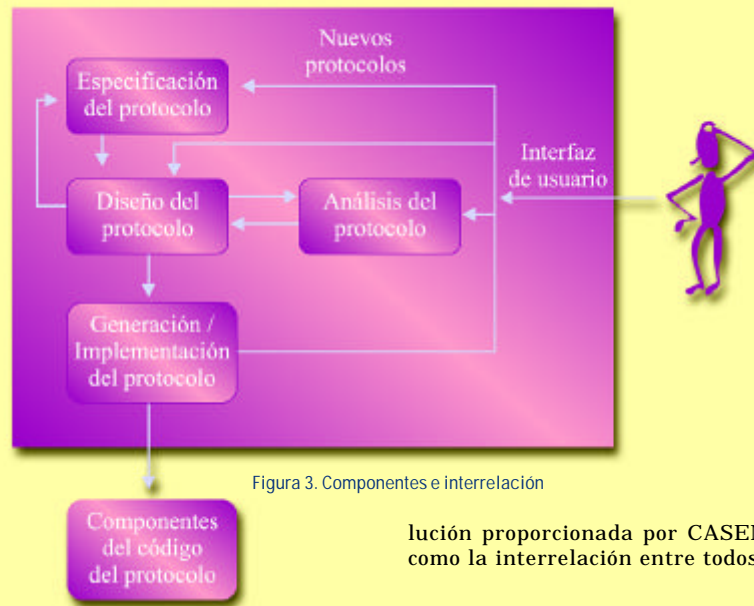


Figura 3. Componentes e interrelación

lución proporcionada por CASENET pretende aportar, así como la interrelación entre todos ellos.

2 **Javier López Muñoz**
Coordinador del Grupo de Seguridad
Departamento de Lenguajes y
Ciencias de la Computación
UNIVERSIDAD DE MÁLAGA
 jlm@lcc.uma.es

REFERENCIAS

- [1] [AbNe94] Abadi, M. and Needham, R. Prudent engineering practice for cryptographic protocols, DEC SRC Research Report 125, June, 1994.
- [2] [AnNe95] Anderson, R. and Needham, R. Robustness principles for public key protocols, Proceedings of Advances in Cryptology - CRYPTO'95, pp 236-247, LNCS 963, Springer, 1995.
- [3] [BAN89] Burrows, M., Abadi, M., and Needham, R. 1989. A logic of authentication, Research Report 39, Digital Equipment Corp. Systems Research Center.
- [4] [GLP99] Gürgens, S., Lopez, J, and Peralta, R. Efficient Detection of Failure Modes in Electronic Commerce Protocols, IEEE International Workshop on Electronic Commerce and Security, pp. 850-857, 1999
- [5] [Kail96] Kailar, R. Accountability in electronic commerce protocols, IEEE Transactions on Software Engineering, 22(5):313-328, May 1996.
- [6] [HeTy96] Heintze, N. And Tygar, J.D. A model for secure protocols and their compositions, IEEE Transactions on Software Engineering, Vol 22, No 1, pp 16-30, January 1996.
- [7] [Mead95] Meadows, C. The NRL protocol analyzer: an overview, Proceedings of the Second International Conference on the Practical Applications of Prolog, 1995.
- [8] [Lowe96] Lowe, G. Breaking and fixing the Needham-Schroeder public-key protocol using FDR, In Tools and Algorithms for the Construction and Analysis of Systems, vol 1055 of Lecture Notes in Computer Science, pp 147-166, Springer-Verlag, 1996.
- [9] [NeSc78] Needham, R. and Schroeder, M. "Using encryption for authentication in large networks of computers", Communications of the ACM, 21(12):993-999, 1978.
- [10] [Schn98] Schneider, S. Verifying authentication protocols in CSP, IEEE TSE, 24(9), September 1998.
- [11] [SyMe98] Meadows, C. and Syverson, P. A formal specification of requirements for payment transactions in the SET protocol, DRAFT for Preproceedings for Financial Cryptography 98, pp23-26, 1998.
- [12] [WoLa93] Woo, T. and Lam, S. A semantic model for authentication protocols. Proceedings the IEEE Symposium on Security and Privacy, IEEE Computer, Society Press, May 1993.