



# Mirando hacia la Academia

Con la llegada de estas fechas, en el mundo académico se desata una actividad que le es muy característica y que no es otra distinta de la preparación de congresos, talleres y encuentros de todo tipo. Además de satisfacer la necesaria difusión de resultados y el debate de nuevas ideas, este tipo de actividades es una oportunidad de oro para enterarnos de qué se está haciendo, de qué se supone que debería hacerse y de qué problemas quedan pendientes en cualquier actividad científica o técnica.

En esta ocasión, vamos a intentar dar una visión parcial pero actualizada de lo que se vive en la comunidad informática que habita en las universidades. La idea es ver en qué se está trabajando e intentar estimar cuál es el grado de sincronismo que hay entre el mundo académico, las empresas del sector y las necesidades sociales en general. Quizás con esta mirada hacia la Academia podamos entender qué puede venirnos encima en el área de la seguridad, qué grado de posible colaboración hay entre lo que ocupa al mundo universitario y los problemas que tiene planteado el mundo empresarial, la sociedad española y la europea, en última instancia, como usuarios finales que son.

Como congresos y temáticas hay muchos, cojamos un caso al azar y podremos ver cuáles son los contenidos de un congreso académico típico. Tomemos como ejemplo el **Trust and Privacy in Digital Business** (TrustBus04) que se celebrará en Zaragoza en los primeros días del mes de septiembre de este año.

Lo que más llama la atención de la respuesta a esta llamada es que muchas de las contribuciones se refieren a sistemas distribuidos, a sistemas multi-agente, a sistemas *peer-to-peer* (P2P), y a la gestión de la confianza y seguridad que se puede tener en ellos. En estos escenarios se da bastante importancia a los modelos de reputación y al establecimiento de ésta. También podemos encontrar sistemas de firma digital más avanzados que los habituales en las PKIs que conocemos (*undeniable signatures, conditionally anonymous digital signatures, anonymous public-key certificates*). Aquí

**El sector productivo de la sociedad tiene muchos problemas planteados en la sociedad de la información y, de forma paralela e independiente, el mundo académico sigue adelante con sus menesteres en I+D. ¿Existe interrelación? ¿Es novedosa? De vez en cuando conviene enterarse de lo que están haciendo los demás y, entre ellos, no podemos olvidarnos del mundo universitario. Veamos aquí algunos de los temas que ocupan el día a día de la investigación académica en los asuntos de seguridad.**

se plantea de nuevo el tema de los núcleos encargados de aportar seguridad a los sistemas (*Security Kernels*) y muy especialmente en el caso de sistemas con escasas capacidades computacionales (PDAs, GSMs, etc.) y enlaces inalámbricos (*mobile handsets y wireless terminals*)

Entre los temas más tratados, encontramos el de la distribución de materiales digitales sobre Internet (*e-goods delivery*). Los escenarios tratados son los de distribución multicast de contenidos multimedia y centrándose además en sistemas de pago por visión que sean realmente escalables a un gran número de clientes. En cuanto a las aportaciones sobre comercio electrónico clásico, éstas se centran en el comportamiento del consumidor (*subjetividad*), a su protección (*profiling* y uso indebido de datos personales) y a nuevos sistemas de reputación basados en la opinión de los consumidores (*rater's commenting quality*).

Dentro del tema de la distribución a través de Internet, la protección de los derechos de autor ocupa un papel muy significativo. Aunque no haya grandes novedades en cuanto a los sistemas que utilizar (*esteganografía, fingerprinting, watermarking, algoritmos de trazado, detección e identificador de traidores*). Como ejemplo de distribución no deseada, también el *spam* y las medidas para mitigarlo son motivo de aportaciones por parte de los investigadores; aunque las soluciones aportadas siguen basándose en los puzzles de tiempo como pieza clave del sistema.

También hay una significativa presencia de propuestas relacionadas con los sistemas detectores de intrusos en los que se incluyen nuevos sistemas de análisis de los datos para la detección de comportamientos "anómalos" (*tecnologías de trazado, sistemas multi-agente, clustering, sistemas predictor-corrector, etc.*).

Un tema clásico que todavía tiene presencia en los foros académicos es el de la identidad en el mundo empresarial y los sistemas de gestión de privilegios. Las aportaciones que se hacen van desde el simple *single sing-on*, a sistemas basados en roles mucho más potentes y sofisticados (*threshold attribute certificates*), como son los sistemas en los que las potestades de los usuarios cambian dinámicamente según la confianza que el sistema pueda depositar en ellos. Otro tema muy relacionado con la seguridad en entornos empresariales y de la administración, y que supone una cierta novedad en estos mundillos es el problema de la seguridad de los documentos electrónicos en lo que se refiere a quién los puede leer y dónde los puede leer (*secure reading environments, secure workflow*).

Como tema novedoso podemos encontrar el comercio electrónico sobre redes inalámbricas P2P que se conoce como *m-business* sobre redes *ad-hoc*; en particular, en lo que a los sistemas de pago electrónico se refiere. En este entorno, el esfuerzo se centra ahora en los modelos de confianza y cómo deben gestionarse estos a través de mecanismos automáticos de reputación.

Como servicios renovados, se pueden encontrar propuestas sobre correo-e certificado y matasellado (*certified & time stamped email*), los protocolos de firma de contratos, la firma digital pero con sello de tiempo asociada (*time stamped forward signature*), sobre nuevas formas de realizar subastas con más seguridad y funcionalidades que el bien conocido caso de eBay (*receipt-free e-auctions*) y sobre cómo compartir entre varios la capacidad de generar una firma RSA sin que ninguno conozca cuál es la clave privada, usando técnicas de compartición de secretos (*threshold RSA function sharing*).

Un tema que también ha recibido bastante respuesta es el de

las votaciones electrónicas (*e-voting*), tanto desde el punto de vista tecnológico (*MixNets* y *servicios de aleatorización*), como desde el sociológico para aumentar la aceptabilidad de dichos sistemas (*trust-building arguments*).

Un asunto nuevo que ha saltado a la palestra es el de los riesgos que suponen las etiquetas de identificación por radio (RFIDs) que se piensan poner en todos los productos para facilitar su comercialización. La existencia de estas etiquetas y su no posible desactivación por parte del consumidor podrían llegar a nuevos escenarios de "profiling" más graves que los que hoy ya se dan en el mundo web.

En cuanto a la identificación biométrica, podemos encontrar algunas aportaciones de reconocimiento de caras para escenarios de banca por Internet (*remote facial authentication systems*).

A la vista de estas aportaciones podemos constatar que la oferta de la Academia sigue estando muy por delante de lo que parece preocupar hoy al mundo empresarial y comercial. Los problemas identificados, sin duda, terminarán siendo problemas de toda la sociedad, por lo que la Academia, en cuanto a su búsqueda de problemas y soluciones, sigue cumpliendo su cometido. Lo que todavía está pendiente es la fluida y eficiente relación entre empresas y universidades, pero está claro que su ausencia no se puede achacar a que el mundo académico no tenga cosas muy interesantes que aportar. La relación anterior de temas no ha sido sesgada por ningún criterio de calidad o de oportunidad, pero sí podemos estar de acuerdo en que resulta suficientemente amplia para satisfacer las necesidades y deseos del mundo empresarial y comercial. Así pues, la culpa de que las cosas no funcionen entre la Academia y el sector productivo hay que buscarlas en otra parte. ■

**JORGE DÁVILA MUÑO**

Director  
Laboratorio de Criptografía  
LSSI - Facultad  
de Informática - UPM  
jdavila@fi.upm.es