Entrevista de Mercé Molist a Jorge Ramió

Madrid, 27 de diciembre de 2015

Publicada de forma resumida en página web del Centro de Investigación para la Gestión Tecnológica del Riesgo CIGTR

http://es.cigtr.info/2015/12/jorge-ramio-una-gran-amenaza-se-cierne.html#.VoAZqVLwzaw

DATOS PREVIOS

- Jorge Ramió, a punto de cumplir los 64 años, inició sus estudios de ingeniería en Chile. Siendo profesor en universidades chilenas, en 1977 gana la beca Reina Sofía para estudiar en España e inicia un primer doctorado que culmina leyendo la tesis en 1982. Desde 1987 es profesor en la Universidad Politécnica de Madrid, donde además de enseñar seguridad informática y criptografía entre otras asignaturas, logra el título de Máster por la UPM en 2011 y posteriormente el título de Doctor por la Universidad de León en 2013. Está casado con chilena nacionalizada española desde el año 1977 y tiene un hijo también ingeniero, MBA y deejay.
- Criptored nace el 1 de diciembre de 1999, teniendo como objetivo principal convertirse en una red social de profesionales de la seguridad informática y sitio en la red donde compartir información, no sólo en España sino en toda Iberoamérica. Por este motivo el proyecto nace con el nombre de Red Temática Iberoamericana de Criptografía y Seguridad de la Información Criptored, que con el paso de los años y cumpliendo ya sus objetivos, se ha quedado en la marca Criptored. Uno de esos objetivos era superar los mil miembros, lo que se consigue en febrero de 2015 con 23 países representados, y por ello en septiembre de este año desaparece el concepto de ficha de miembro de la red temática y se crea, en su lugar, un grupo profesional en LinkedIn que en tres meses alcanza los 1.887 miembros.
- Durante su 16 años de vida, Criptored ha sido protagonista de diversos proyectos asociados a la difusión masiva de la seguridad: 8 congresos CIBSI celebrados en diferentes países de Latinoamérica, la enciclopedia visual de la seguridad de la información intypedia, el primer MOOC en español Crypt4you, el Mapa de Enseñanza de la Seguridad de la Información MESI, las píldoras formativas Thoth, formación online con destacados expertos como profesores invitados y haber servido gratuitamente más de 5 millones de documentos en Internet.

ENTREVISTA COMPLETA

PREGUNTA: ¿Cómo se te ocurrió dedicarte a la informática? Cuando eras joven no debía ser tan omnipresente como ahora…

RESPUESTA: Bueno, en realidad mis primeros estudios universitarios fueron de electrónica, de ahí derivé tras mi primer doctorado hacia las telecomunicaciones y en los últimos 29 años, ya en la UPM, me he dedicado preferentemente a la seguridad y a la criptografía. Al comienzo de los años 70 cuando estudiaba electrónica en Chile, la informática era muy incipiente y, como es lógico, ni de lejos tenía el alcance que observamos hoy en día. Las Facultades de Informática,

tanto en Chile como en España, se estaban comenzando a crear a partir de la segunda mitad de esa década, y lo que nos interesaba estudiar en aquellos años era más bien electrónica donde sí había un gran desarrollo y un potencial mercado de trabajo. Es decir, puedo considerarme como equipo visita en el campo de fútbol de la informática, algo que además es común en profesores que llevan 3 o 4 décadas en las universidades españolas. Obviamente esta situación se ha ido normalizando con el tiempo con la entrada de profesores que ya habían estudiado informática en la universidad.

PREGUNTA: Veo en tu LinkedIn que en los años 70-80 estuviste haciendo de profesor en Chile, lo que me provoca gran curiosidad: ¿eres chileno?

RESPUESTA: No, nací en Barcelona y por tanto soy español, pero me he criado en Chile, donde viví desde 1958 hasta 1986, aunque entre medias he estado en Madrid más de 3 años estudiando con una beca. En el fondo, podría decir que he vivido la mitad de mi vida allí y la otra mitad aquí. Haces bien en tener curiosidad; Chile es un país hermoso y su gente adorable. Guardo excelentes recuerdos de mi vida allí, como no puede ser de otra manera, vuelvo bastante a menudo por aquellas tierras donde tengo familia, para impartir conferencias y clases y, además, estoy felizmente casado con una chilena.

PREGUNTA: Tu proyecto más conocido es Criptored. ¿Por qué razón lo pusiste en marcha y qué te ayuda a seguir tirando de este carro?

RESPUESTA: Es algo anecdótico. Las razones que me impulsaron a crear Criptored, nacen de una discusión a través de una lista de correo que tuvimos varios profesores de seguridad informática a mediados de 1998, meses antes de la quinta edición del congreso RECSI que se celebraría en Torremolinos, en cuanto a qué área de conocimiento era la más apropiada para las enseñanzas de seguridad y criptografía, que eran las temáticas que se llevaban por aquellos años. Observé que éramos un buen número de profesores entusiasmados en aquellos debates e interesados en intercambiar nuestra documentación, algo por lo demás común en el entorno de la seguridad, y me pregunté por qué no centralizar todo ese esfuerzo en una página web, dado que en aquel entonces no existían aún las redes sociales tan comunes hoy en día. Más aún, veía que con ello podría ayudar a muchos colegas y amigos de otras universidades de Latinoamérica que, al igual que sucede hoy en día, en temas de enseñanza de seguridad de la información estaban unos cuantos años por detrás de España y tenían un desarrollo aún muy incipiente. Sobre qué me ayuda a seguir en la brecha, simplemente el interés en hacer algo que beneficie a los demás, dejar tu aporte o grano de arena a la sociedad, por pequeño que éste sea. En los últimos años colabora conmigo en Criptored el Doctor Alfonso Muñoz, con quien he creado proyectos de gran calado y difusión como intypedia, Crypt4you, la sección formación y Thoth. Además, desde sus inicios tengo la suerte de que colabore en el proyecto otro colega de la universidad, D. Daniel Calzada, quien mantiene la seguridad del sitio web. Los tres trabajamos ad-honorem.

PREGUNTA: Es quizás de tus proyectos el menos dirigido a la enseñanza y más a la información de eventos y otros para la comunidad de seguridad. ¿Cuál crees que es el secreto de su éxito?

RESPUESTA: Es verdad, porque en temas más académicos me he dedicado a publicar libros electrónicos y software de prácticas para laboratorio de criptografía, todo gratuito y en la red. Yo creo que el éxito está basado en el cariño que ponemos los tres en que las cosas salgan bien y, luego, algo que aquí en España se valora muy poco, la innovación. Y para pruebas te muestro estos tres ejemplos. El proyecto intypedia que nace en 2010 fue el primero en enseñar seguridad mediante vídeos con avatares y vamos camino de las 600 mil visitas en

YouTube. No pudimos seguir por falta de patrocinador porque hacer ese tipo de vídeos costaba dinero y había que contratar a profesionales. El MOOC Crypt4you de 2012 fue el primero en español y casi simultáneo con el arranque de los MOOCs en los Estados Unidos, mucho antes de que la fiebre de los MOOC invadiera las universidades españolas; proyecto activo y en el que por cierto también rondamos las 600 mil visitas. Por último, el proyecto de píldoras formativas Thoth en el que contamos con el apoyo económico de Talentum Startups para pagar a los becarios y que nace en 2014, fue de los primeros en su género y no existe otro ejemplo similar en lengua hispana. Lo más parecido y guardando las debidas proporciones claro sería Khan Academy, pero la diferencia de presupuesto es astronómica. Con más de 30 píldoras publicadas y 55 mil visitas en YouTube, el objetivo es poder seguir publicando una píldora al mes. Esos alcances mediáticos en otros países podrían ser considerados como dignos de un apoyo institucional; aquí en España no. Es más, en el ámbito del reconocimiento académico esta labor no sirve de nada.

PREGUNTA: Eres Doctor en Sistemas Inteligentes en la Ingeniería. ¿Qué significa eso?

RESPUESTA: Buena pregunta, que también me la hago porque suena muy rimbombante. Simplemente se trata de un Doctorado que hay en la Universidad de León en el que me apunté sólo para leer mi segunda tesis doctoral en diciembre de 2013 y que se trataba, básicamente, de una especie de libro blanco sobre la enseñanza de la seguridad informática en España. Un repaso de las últimas cuatro décadas, cuya investigación ha dado lugar a diversas publicaciones y donde nace MESI, otro proyecto que puede encontrarse en Criptored.

PREGUNTA: Eres profesor de seguridad informática... ¿qué te atrajo a ese mundo?

RESPUESTA: Cuando llegué a España procedente de Chile en 1986 a la que se llamaba Escuela Universitaria de Informática en el campus sur la UPM, no existía ninguna asignatura de seguridad en sus planes de estudio, por lo que impartía asignaturas de sistemas operativos, bases de datos e introducción a la informática. En 1992 hay un cambio en el plan de estudios y se buscan asignaturas optativas. Recuerdo que estaba dudando entre proponer como nueva asignatura optativa algo relacionado con la ofimática o bien con la seguridad. Después de buscar en Internet (no había la información que hoy tenemos, ni mucho menos) me decido -no sé muy bien por qué- por la seguridad. Así, una de las primeras personas a la que acudo para que me oriente, entregue información, temarios, etc., es el Dr. Arturo Ribagorda, profesor de la Universidad Carlos III de Madrid, que ya llevaba varios años en este tema y toda una autoridad. La recepción fue excelente, me encontré de un día para otro con una gran cantidad de información y ello fue un aliciente para comenzar a crear nueva documentación de libre distribución, software para prácticas, etc. Comienzo así a impartir temas de seguridad y criptografía en 1994 y 21 años después continuamos en ello.

PREGUNTA: Cuando hablo con jóvenes profesionales de la seguridad que han estudiado en la universidad (en cualquiera, no sólo la tuya) siempre me dicen que en la universidad se aprende algo, pero que sin la práctica no se aprende nada. ¿Significa eso que en la universidad se está enseñando mal o no suficiente?

RESPUESTA: Complicada pregunta, que sin embargo no tengo inconveniente alguno en contestar. Aunque siempre existirá el debate de si es mejor una universidad generalista que una no generalista y por tanto con mayor dedicación a la práctica, lo cierto es que en seguridad es muy difícil abarcar tantos aspectos en dos o tres asignaturas, y en el mejor de los casos en que la carrera en cuestión tenga esas tres asignaturas. Lo que se agrava si hablamos además de prácticas. Como no hay un recorrido más largo o especialización en seguridad, al

final hay que optar por impartir los conocimientos básicos de seguridad, de criptografía, de normativas, de gestión de la seguridad, de seguridad en redes... y no da para más, se quedan fuera muchos otros temas que son de interés para el desempeño de un profesional de la seguridad y, cómo no, gran parte de esas prácticas que echan de menos quienes luego trabajan en seguridad. Opino que desde hace ya unos cuantos años debería existir un grado universitario en seguridad, como lo proponía yo mismo en un trabajo presentado a las jornadas JENUI en 2001 en Palma de Mallorca, pero ninguna universidad se atreve a dar el paso, aunque eso sí, todas están locas por impartir másteres en seguridad, que en España tenemos ya 26 y algún otro por venir. No tiene mucho sentido, pero es lo que hay. Temas para hacer un excelente grado de ingeniería en seguridad tenemos por decenas, contando además en ese hipotético plan de estudios con otras enseñanzas básicas de la ingeniería, de la informática y de las telecomunicaciones, pero lo difícil es contar con una docena de profesores expertos en estas temáticas nuevas, más aún en la situación actual de las universidades españolas donde no existe renovación generacional. Seguimos al pie del cañón los viejos rockeros de siempre hasta que nos jubilemos y no entra savia nueva, entre otras cosas porque esa gente joven y experta en seguridad puede llegar ganar en otros sectores que no sea el de la educación entre tres y cuatro veces más que en la universidad porque el mercado así lo demanda. Creo que sobran los comentarios.

PREGUNTA:¿Tus proyectos Thoth, Intypedia o MOOC Crypt4you, que usan audiovisuales o enseñanza a distancia, son una muestra de cómo tú enseñarías seguridad en las universidades?

RESPUESTA: Sí, de hecho el objetivo del proyecto de píldoras formativas Thoth es generar un gran libro multimedia que permita abarcar muchas temáticas de la seguridad y que, por sí solo, configure una herramienta de enseñanza completa. Uso habitualmente ese material en mis clases y está clarísimo que se trata de un valor añadido. De hecho, sé que hay profesores en España y en Latinoamérica que usan las píldoras Thoth y las lecciones de intypedia por ejemplo para comenzar un tema y llamar así la atención a sus alumnos. En el caso de las píldoras formativas Thoth, no debemos perder de vista que su objetivo es la formación personal, al ser un material audiovisual de consulta rápida sobre un tema muy específico. En este proyecto, el apartado dedicado a la criptografía llegará hasta la píldora 50 aproximadamente y después podrán venir temas de SGSI, malware, seguridad en redes, informática forense, etc. Si tuviésemos un mínimo presupuesto para afrontar este tema de una manera más ambiciosa, se podría llegar a la utopía de publicar una píldora por semana, esto es más de 50 píldoras al año y formar en poco tiempo un verdadero libro multimedia, pero todo esto tiene un coste y no contamos con mecenas -al menos de momento- como el Sr. Salman Khan.

PREGUNTA: Eres también autor del Mapa de Enseñanza de la Seguridad de la Información MESI. ¿Está la enseñanza de la seguridad bien cubierta en España o faltarían más centros y asignaturas?

RESPUESTA: Exacto. Como te decía anteriormente, formaba parte de mi tesis doctoral. Como se desprende del documento público de esa tesis y de la propia página web del proyecto MESI, en España hemos hecho un inmenso avance en los últimos 5 años sobre la formación universitaria en seguridad, alcanzando las 229 asignaturas dedicadas en exclusiva a la seguridad y de ellas 89 son obligatorias, lo que ya es un gran triunfo, otras 122 asignaturas dedicadas parcialmente a estos temas y nada menos que 26 másteres. Siempre quedan asignaturas pendientes que aborden temáticas más actuales, que bien no se imparten o bien su impartición es casi anecdótica, como sería el caso de análisis de malware, ingeniería inversa,

auditoría de máquina, seguridad industrial, informática forense, pentesting, seguridad en infraestructuras críticas, APTs, etc. Lo que sí hace falta como decía antes, es que alguna universidad se atreviese a ofrecer un grado universitario en seguridad, que tendría además dos aspectos muy interesantes a tener en cuenta: la gran demanda de expertos en ciberseguridad que se espera para el horizonte 2020 y el interés de los jóvenes por todo lo relacionado con la seguridad informática. No se puede pedir más, interés y mercado de oportunidades juntos.

PREGUNTA: Cada día nos despertamos con 3 o 4 noticias graves sobre la seguridad de las redes y sus dispositivos, y/o el avance de la delincuencia informática. La impresión es que está fuera de control. ¿Qué se está haciendo mal?

RESPUESTA: En seguridad hay una máxima y es que ésta nunca es posible al 100% por su propia naturaleza. Hablamos de la seguridad como un proceso dinámico que se va adaptando mediante una mejora continua, por lo cual nada será nunca completamente seguro. Y por otra parte, otra frase muy escuchada y que cae perfecta en este mundo de la seguridad es que resulta mucho más fácil destruir que construir. Quien está dispuesto a realizar un ataque, se centra únicamente en el frente donde desea explotar una vulnerabilidad, en cambio quien protege las infraestructuras, debe estar pendiente de todo, y ello sin caer en la paranoia de forma que la institución tenga continuidad de negocio y la seguridad no se convierta en un impedimento. Es una guerra desigual que sólo se puede intentar equipara si en el lado de los buenos se cuenta con muchísimo dinero y los mejores profesionales, pero debemos tener en cuenta que cada vez los malos cuentan también con más dinero pues los ataques son más sofisticados. El concepto de buenos y malos no debe asociarse a responsables de seguridad y hackers respectivamente, como resulta común verlo reflejado en cierta prensa. Los papeles pueden perfectamente intercambiarse, basta con recurrir a las hemerotecas digitales y ver lo que ha pasado en los últimos años en materia de seguridad, espionaje, etc. El problema que se nos avecina es el entorno de la llamada ciberseguridad, mal llamada ciberseguridad por algunos que la confunden con seguridad en redes y en tecnologías de la información. La ciberseguridad une el mundo IT (del inglés Information Technology) por todos conocido, con el mundo OT (del inglés Operation Technology) de las máquinas y sistemas industriales, ya no tan conocido. El aspecto principal es el control (de ahí proviene la palabra cibernética y por tanto el término ciber) de equipos y sistemas del mundo OT mediante dispositivos y sistemas del mundo IT. Esa es la gran amenaza que se cierne sobre las infraestructuras críticas, porque ya no estamos hablando de mi PC infectado por un virus (años 80), ni de la red corporativa arrasada por un gusano (años 90), ni solamente de los fallos en redes globales y delitos informáticos (años 00), sino de las infraestructuras críticas de un país, cuyos daños pueden afectar a una amplia población e incluso costar vidas humanas (años 10). No creo que se esté haciendo nada mal. Se avanza, hay colaboración entre instituciones y países, cada vez hay mayores y mejores medidas de seguridad, hay más sensibilidad de la sociedad ante este tema. Somos más conscientes de los riesgos que corremos como sociedad ante estas nuevas amenazas y por otra parte cuesta mucho mantener en secreto un incidente, normalmente éste obtiene una mayor publicidad de manera casi inmediata.

PREGUNTA: Una pregunta un poco loca, esperando tu ingenio en la respuesta: ¿Es posible enseñar a alguien a ser hacker?

RESPUESTA: Me encantaría poder responder a esta pregunta de una forma sensata; voy a intentarlo porque ya me gustaría a mí tener conocimientos de hacking, pero he llegado algo tarde a este tren. Yo creo que sí. De hecho, en esa hipotética carrera universitaria de ingeniero en seguridad, dos o más asignaturas deberían tener este perfil de desafíos, juegos de rol en

que algunas veces seamos los malos y otras veces los buenos, retos, captura de la bandera, etc. La mejor manera de saber cómo afrontar estos retos de hacking es haber vivido o experimentado en carne propia estas experiencias, saber qué puede estar pensando quien está al otro lado. Es tan simple como observar que muchos directores de seguridad de grandes empresas vienen de este mundo o bien han vivido experiencias similares; por algo será. Y no me negarás que a la gente joven este tipo de asignaturas prácticas les encantaría y, además, sería el momento oportuno para darles nociones de deontología y ética profesional, algo fundamental en este mundo de la seguridad y más aún en este entorno hacking.

PREGUNTA: Y una pregunta más personal: ¿cómo se hace para tener siempre esta sonrisa en los labios que da tanta buena energía a quienes te rodeamos?

RESPUESTA: Creo que es el hecho de estar contento con lo que se hace. Saber que estás aportando algo a la cultura universal, por poco que sea, que eso queda ahí y que a alguien le va a servir hoy, mañana y quizás también dentro de varios años, tener siempre un nuevo proyecto en el que pensar y renovarse. Y obviamente contar con una familia que te apoya y saben que todas estas horas que dedico a compartir información de forma gratuita hace que me sienta feliz, útil a la sociedad y finalmente realizado profesionalmente y como ser humano.

Más información:

- Criptored: http://www.criptored.upm.es/
- Jorge Ramió: http://www.lpsi.eui.upm.es/~jramio/
- Mercè Molist: https://twitter.com/mercemolist