# Entrevista a Román Medina-Heigl Hernández (RoMaNSoFt)

Vie, 09/16/2011 - 12:55

Twitter:@roman_soft
Web:Aquí

Compartir

No he tenido posibilidad de conocer a Román personalmente todavía. Según sus amigos Román es una persona con una mente brillante, algo tímido y sobre todo muy perfeccionista.

En el mundo de la seguridad informática ha destacado desde hace más de una década. Además, Román es "profeta en su tierra" ya que es conciudadano nuestro de Úbeda ;).

Dentro de su formación académica cabe destacar que es Ingeniero de Telecomunicación, con acreditaciones en materia de seguridad y gestión como CISSP e ITIL v3.

Gracias Román por dedicarnos tu tiempo ;).

No he querido repetir cuestiones ya formuladas a Román en el pasado. Os recomiendo leer también las que tiene publicadas en su web http://www.rs-labs.com

Comentario de Román: Querrás decir según Chema :) Es cierto que soy bastante perfeccionista y que no me gusta ser el centro de atención de nada ni nadie (a pesar de que a veces pueda parecer lo contrario :P). Ah, que esto no son todavía las preguntas :))

**1._ Este año se está convirtiendo en un punto de inflexión en materia de (in)seguridad. ¿Qué opinión te mereció lo acontecido con Stuxnet hace ya unos meses?**

¿Inflexión por qué? Siempre ha habido malware, ataques más o menos sofisticados, etc. La diferencia es que cada vez estamos más concienciados y preparados técnicamente: somos capaces de descubrir y detectar muchos ataques que antes pasaban desapercibidos. Por fin nos hemos dado cuenta de que por muy parcheados que estén nuestros sistemas siempre existirán 0-days que permitirán vulnerarlos y por tanto, debemos centrar nuestros esfuerzos en:

1/ Situar varias barreras de seguridad que dificulten el progreso de un hipotético atacante (el conocido concepto de "defensa en profundidad"), y 2/ Ser capaces de detectar la intrusión lo antes posible (idealmente antes de que todas nuestras barreras resulten vulneradas).

Stuxnet ha servido para recalcar la importancia de la seguridad de los sistemas SCADA y recordarnos que los ataques dirigidos siempre han existido y seguirán existiendo. Además, me llamó mucho la atención el despliegue de medios del atacante (supuestamente Israel y EEUU), o en otras palabras, el grado de sofisticación del ataque, encadenando varios 0-days y con diferentes vectores de ataque, para maximizar su efectividad.

**2._ Recientemente ha sido comprometida la seguridad de Comodo y Diginotar, ambas autoridades de certificación. ¿Es realmente posible imaginar un Internet seguro? ¿Existirían otros modelos alternativos?**

Siempre es más fácil destruir que construir, atacar que defender. En este sentido, el atacante siempre tiene las de ganar e irá un paso por delante puesto que le basta con encontrar una sola puerta abierta para vulnerar un sistema. Y cuando ésta se cierre buscará (y seguro que encontrará) otra. En Internet hay muchos sistemas, y cada uno con muchas puertas abiertas o entre-abiertas esperando a ser atacadas :)

El caso del SSL es una puerta que se ha quedado entre-abierta y que es imposible de cerrar. Hay un factor que se llama "confianza" que la obstaculiza. Como todos saben, la seguridad de una transacción SSL común se reduce (asumiendo que la fortaleza de las claves y algoritmos criptográficos empleados es "razonable") a

poder verificar que el certificado digital empleado por el servidor es correcto, esto es, no está siendo suplantado, y para ello nos tenemos que fiar de una (o varias) CA's que lo acrediten, tenemos que "confiar" en ellas. Entre CA's raiz e intermedias creo recordar que Moxie Marlinspike hablaba de que podía haber unas 600, es decir, podríamos decir que hay 600 puertas que protegen una misma cosa; y con que encontremos solo una de ellas lo suficientemente débil habremos traspasado la barrera y por tanto comprometido la seguridad de la transacción SSL. Por supuesto, todo esto sin contar con que habrá puertas cerradas pero donde se han emitido "casualmente" copias de la llave que las abren a Gobiernos, etc. En este último caso, ni siquiera necesitas encontrar una brecha, coges tu copia de la llave y entras...

Precisamente el citado Moxie proponía recientemente una alternativa al sistema clásico de CA's que es bastante curiosa: a la par que te descargas el certificado SSL de un sitio, pides a otros (los "notarios") que se lo descarguen también, te lo envíen y finalmente compruebas que todos ellos coinciden. La solución la bautizaron como "Convergence" (http://convergence.io/details.html) y la idea es que si a tí te están haciendo un ataque MitM y por tanto ves un certificado falso, tus "notarios" (que se supone deben estar distribuidos) no se verán afectados (o al menos no todos) y por tanto, será posible detectar el certificado falso. Se podría decir que los notarios son a este modelo lo que las CA's al modelo clásico: un elemento en el que hay que confiar. La gran diferencia es que tú puedes elegir y crear tus propios notarios (mientras que las CA's tú no las eliges, "están ahí"), por un lado, y por otro que para vulnerar el modelo habría que comprometer a todos los notarios en los que yo estoy confiando (en el modelo clásico basta con una CA comprometida para poderte engañar).

Personalmente pienso que la ventaja del modelo que propone Moxie (básicamente el ser un sistema "distribuido") es a la vez su desventaja porque no lo veo fácil de desplegar a nivel general. No veo yo a un usuario de a pie realizando la configuración de esta herramienta y seleccionando "notarios". Por otro lado, si esta selección/configuración inicial fuera automática, ¿se seleccionarían al azar de un gran listín de notarios disponible de forma centralizada? ¿Y si alguien compromete este listín? ¿Quién crea los "notarios" y los pone a disposición del público? ¿Y algo estilo eMule donde todos seamos clientes y a la vez notarios de otros? Creo que hay muchos flecos que pulir, a día de hoy no me parece operativo para el público en general. Desde mi punto de vista, "Convergence" podría ser a la web, lo que PGP al correo: una solución útil en ciertos (y limitados) entornos. Pero no creo que sea la solución.

Yo me inclino más por aprovechar DNSSEC aunque tampoco es una solución perfecta y sobre todo, falta que se extienda. En definitiva, creo que seguiremos usando las CA's de toda la vida todavía por mucho tiempo...

Perdón, me he enrollado :) Pero es que este tema da mucho para hablar...

**3._ ¿Podrías relatarnos tu participación en el Swiss Cyber Storm de este año junto a grandes como Kachakil, Whatsbcn, Uri, Dreyer, y demás int3pids?**

¿No has tenido suficiente con la parrafada anterior? Mejor resumiré: cinco aventureros (los que has nombrado más un servidor) nos plantamos en Suiza, resolvimos todos los retos que pudimos en el concurso, y se ve que no lo hicimos mal porque ganamos un coche de premio :) Esto es lo que se puede contar.

El resumen que no se puede contar (o no debería pero voy a hacerlo) es: llegamos un viernes tarde y nos vamos de cervezas hasta las tantas (de la mano de un conocido "Googler" afincado en Zürich... ¡saludos Ero!). Stop.

Nos levantamos pronto el sábado (yo no pegué ojo), nos pegamos un viaje de 45 mins (nos quedamos a dormir en Zürich y el evento era en un pueblo perdido... Rapperswil) y nos ponemos a resolver pruebas como locos. Stop. Sobre las 17 o 18h nos llevan a un garito donde se celebraría la Fiesta: más cervezas y de nuevo hasta las tantas. Stop. Otro madrugón el domingo y para el lugar del evento. Más pruebas y finalmente... ganamos :) Yo apenas me pude quedar a la ceremonia de premios porque si no, perdía el avión (los demás o tenían el avión más tarde o se quedaban más días haciendo turismo por Suiza). Como ves, fue un fin de semana muy duro :)

Ahora en serio... El concurso estuvo muy bien organizado y las pruebas entretenidas. Se notaba que estaba todo bastante bien calculado y cuidado. Por ejemplo, el concurso estaba pensado para que no te pudieras llevar trabajo a casa al terminar la jornada del sábado (eran pruebas individuales que "caducaban") y así todo el mundo acudiera a la fiesta y socializara.

Eso se agradece. Además, había otra razón para ir a la fiesta (aparte de las cervezas, claro): una prueba extra, que consistió en que te iban dando unos papelillos con unos símbolos raros y un trozo de texto ASCII, y que al final resultó que había que recolectar, ordenar según los símbolos, y finalmente decodificar el base64 de la cadena ASCII obtenida. Dicho así parece simple pero tenía su gracia, porque los papeles te los iban dando con cada consumición y hasta que no tenías unos cuantos no podías empezar a ver la relación :) Como anécdota, nuestro Albert ("whats") se dedicó a hacerle ingeniería social a la camarera para que nos diera papelillos extra (solo por los papelillos, no penséis mal :)). Y hubo algún equipo que se dedicó con una cámara a fotografiar los papelillos de los demás, por la espalda, cuando estábamos distraídos (¡en plan paparazzi!).

Siguiendo con el concurso, cada prueba se cerraba una vez trascurrida una hora de que alguien la hubiera resuelto; durante esa hora, los equipos que faltaran por resolverla se dejaban la piel para intentar sacar la prueba, y el equipo que la había resuelto debía preparar una mini-presentación explicando su resolución. A la hora, ya nadie podía puntuar nunca más en esa prueba, y alguien del equipo (en nuestro caso Dreyer, nuestro orador favorito xDD) subía al estrado y la exponía en perfecto inglés. Luego, el público "votaba" y puntuaba la exposición pudiendo así ganar puntos extra. La votación era electrónica y se hacía in situ utilizando el propio "badge" del evento vía RF. Una de las pruebas del concurso consistió en hackear dicho sistema de votación para poder falsear los votos (gracias a Dios esta prueba la pusieron hacia el final del concurso porque hubo quien consiguió romper el sistema).

También había pruebas cuya solución no estaba prevista, esto es, su solución era crear un 0-day en toda regla en un software dado (por ejemplo, en un conocido software comercial de sandboxing, o una solución de intercambio de correo seguro -también comercial-). Supongo que ésta era una de las razones por las que te hacían firmar un NDA como requisito indispensable para poder participar en el concurso.

Otra anécdota graciosa: para una de las pruebas pusieron una lámpara giratoria (como la de las ambulancias) que se activaba automáticamente cuando alguien la resolvía y enviaba la password correcta. Imaginad: todo el mundo concentrado (lo que se podía porque había música cañera y más o menos alta) y de repente se ilumina y comienza a girar la bombilla... ¡éramos los int3pids!

**4._ He visto en tu CV que has obtenido la certificación ITIL v3, ¿Podrías darnos más información sobre su alcance y aceptación en el sector?**

ITIL no deja de ser un conjunto de buenas prácticas para la Gestión de TI, que está ampliamente difundido y aceptado en las empresas de cierta envergadura (para empresas pequeñas no tiene mucho sentido añadir toda la sobrecarga que estas prácticas conllevarían -aunque esto es solo mi opinión-).

Viene bien tener la certificación si te mueves en el sector TI, y no solo para puestos de gestión, puesto que ayuda a entender (y hasta justificar) muchos de los procedimientos y "burocracias" que actualmente existen en las grandes empresas.

De todas formas, no es una certificación que tenga que ver con seguridad. Para esto último, mi recomendación sería CISSP (ISC2).

**5._ Actualmente te encuentras trabajando en Repsol. ¿Trabajas con sistemas SCADA? ¿Podrías contarnos algo de tus ocupaciones?**

Trabajo en el área de Seguridad de la Información, y más concretamente, en Ingeniería de Seguridad, donde básicamente nos dedicamos a proponer e implantar proyectos y/o servicios que supongan una mejora de la seguridad de la Compañía (a nivel internacional, no solo de España) y también llevamos tareas específicas como tareas de revisión de seguridad de plataformas/sistemas/redes, la gestión de incidentes de seguridad o el análisis forense, por nombrar algunas.

Mi principal labor es gestionar recursos en los diferentes proyectos y servicios en los que estamos involucrados. Esto no quiere decir que sea solo un mero gestor puesto que me gusta aprovechar mi vertiente más técnica para encaminar y atajar problemas "difíciles" y siempre que puedo procuro involucrarme en algunas tareas técnicas, me ofrezco de conejillo de indias para probar nuevos productos, configuraciones, cacharros, etc :-)

Los sistemas SCADA han cobrado especial relevancia desde la aparición de Stuxnet (no es que antes no fueran importantes, lo que pasa es que solo nos acordamos de Santa Bárbara cuando truena). De todas formas, en España todavía estamos muy en pañales. De hecho, ha sido en este año (en base al Real Decreto 704/2011, 20 de mayo de 2011) cuando se aprobó el Reglamento de Protección de infraestructuras críticas (como parte del desarrollo de la Ley 8/2011, de 28 de abril del presente). Ahora hace falta desarrollarlo y para ello hará falta colaboración de todos los actores involucrados, siendo algunos de ellos las grandes empresas presentes en el panorama nacional y relacionadas con sectores estratégicos (en el caso de Repsol, la industria química y la energía). Ya veremos cómo acaba todo esto y si personalmente me acaba salpicando :) Pero a día de hoy, no, nunca he trabajado con SCADA.

**6._ Conozco tu pasión por UNIX y algunos lenguajes de programación. Pero ¿Y de Java cual es tu opinión?**

Java es un mal con el que nos ha tocado convivir :) Se supone que es prácticamente universal pero la realidad es que siempre hay problemas de compatibilidad, versiones, etc (siempre tiemblo cuando me entregan un producto y su administración está basada en Java). A mí nunca me ha convencido y por eso nunca lo he adoptado como lenguaje de programación.

Sí me ha tocado enfrentarme a crackmes y retos en Java, para lo cual realmente no hay que ser ningún experto en Java (si el código es normalito se entiende bastante bien con un poco de sentido común) y además es más entretenido saber destripar un .class (jad, jd-gui, etc) e incluso hacer alguna pequeña modificación sin tener el código fuente (con herramientas como cck que trabajan directamente con instrucciones de JVM).

**7._ Me gustaría saber tus predicciones sobre tecnologías nuevas y no tan nuevas como NFC o VOIP, ¿se implantarán definitivamente en nuestra vida?**

No me considero muy puntero en lo que a tecnologías se refiere, me siguen atrayendo más los ordenadores que los gadgets, smartphones y cacharritos en general. En este sentido, soy un usuario más (puede que avanzado en algunos casos, pero en otros primerizo :)) que se deja llevar así que no se si atreverme a lanzar predicciones...

En general, para que una idea progrese hacen falta al menos dos cosas: usabilidad/comodidad para el usuario, por un lado, y por otro lado, alguna empresa fuerte que promueva y empuje la idea. En el caso del NFC desde el punto de vista del usuario creo que es algo cómodo y que puede aportar, y por la parte empresa, hay algunas como Google que parecen estar detrás de un sistema de pagos móviles vía NFC así que se dan

los dos factores.

Todavía se tendrían que ver muchos más móviles con chip NFC para que la idea sea efectiva así que a corto plazo no lo veo pero a medio/largo plazo sí que lo puedo llegar a ver. Desde luego, si se llegara a implantar como algo común le tendrían que dar una vuelta al tema de la seguridad (porque en RFID, p.ej, la mayoría de tarjetas que se usan para el acceso a edificios etc se pueden clonar con cierta facilidad -sin necesidad de contacto físico con la víctima, basta con estar cerca de ella-).

Respecto al VoIP, todos hemos usado programas como Skype o Viber ya sea en el desktop o en el móvil. Como tecnología es bastante madura y puede llegar a ser segura (si se protege adecuadamente con una capa SSL). En este caso, el que prolifere o no de cara al usuario/abonado está en manos de las operadoras quienes por un lado deberían mejorar las infraestructuras de red, y por otro contemplar la comunicación VoIP seriamente dentro de su modelo de negocio. Por ahora, les sigue interesando más tarificarte por conceptos "clásicos" como el establecimiento de llamada o la duración de la misma en lugar de únicamente por paquetes de datos / tráfico; perderían pasta con la VoIP, a priori, así que hasta que llegue alguien "regalando" el ancho de banda y no tengan más remedio que adecuarse al mercado esto no va a cambiar.

Anivel corporativo, sí que hay muchas empresas que internamente utilizan VoIP y ésta será la tendencia (sobre todo cuando se trata de empresas con varias sedes donde el ahorro en teléfono tradicional puede llegar a ser considerable).

**8._ Sobre las empresas españolas de Telecomunicaciones ¿Crees que están al mismo nivel que el resto de Europa?**

Si te refieres al servicio que recibimos los españoles, no es ningún secreto que aquí en España tenemos en general las tarifas de internet y de telefonía móvil más caras de Europa. Respecto a tecnologías, se sigue exprimiendo el par de cobre (con el ADSL) y la cobertura de fibra es muy limitada aún por lo que la calidad de nuestra conexión a internet es pobre.

**9._ ¿Continúas con tu labor docente en la UOC? ¿Y Chema Alonso te ha vuelto a liar para algún proyecto nuevo?**

jajaja. ¡Chema siempre te intenta liar! (todavía le tengo guardado lo de aquel AseguraIT :)). El caso es que cada vez dispongo de menos tiempo (o esa es la sensación que me da a mí: siempre ando liado, nunca me aburro) y prefiero dedicarlo a las cosas que realmente me gustan (por ejemplo, participando en retos y CTFs con mis "int3pidos" compis :)).

Este ha sido mi segundo año como profesor consultor en el master de seguridad informática de la UOC. Es gratificante ver como los alumnos se lo curran para aprender y progresar, y es lo que yo trato de fomentar e inculcar durante el curso, más allá del propio contenido de la asignatura que imparto.

**10._ ¿Sigues pensando que “HD Moore” es el referente mundial en seguridad en este momento?**

Al menos es uno de mis referentes, en lo que al mundo técnico se refiere (espero que no le pase como a Dave Aitel, que ha acabado ejerciendo de puro hombre marketing). Quizás personas como Bruce Schneier son aún más mediáticas y más influyentes en el mundo de la seguridad en general. Pero sin desmerecer a este último, a mí me siguen gustando más perfiles puramente técnicos (Dino Dai Zovi es otro ejemplo).

Y nunca me dejarán de impresionar todas las personas y teams contra los que competimos habitualmente en los CTFs. La calidad técnica de todos ellos suele ser abrumadora, unos auténticos tiger-teams.

**11._ ¿Nos podrías recomendar algún libro que te haya gustado especialmente?**

Un clásico de las novelas relacionadas con seguridad: "El huevo del cuco" de Clifford Stoll.

**12._ Un amigo tuyo quiere preguntarte de donde viene tu "adicción" a los gofres. ¿Adivinas quién?**

Por pocas me confundo y digo "kamborio" (¿alguien se acuerda del hack a la web de La Moncloa allá por 2001?) pero éste sería si me hubieras preguntado por las crêpes :) El de los gofres debe ser "pepelux" (empresario alicantino aunque más conocido por su afición a los wargames y CTFs) :)

Tampoco tiene mucho misterio la cosa: en general, soy goloso y me encanta todo lo que no tiene colesterol, como la bollería y los dulces }:-) (vale, tienen "un poquito" pero están tan ricos...).

Para terminar agradecer la oportunidad que me habéis brindado para conversar con vosotros por medio de esta entrevista, mi más sincera enhorabuena por la iniciativa "EnRed 2.0" y también desearos todo lo mejor para las jornadas de seguridad que estáis preparando en Jaén para el próximo año (20, 21 y 22 de Marzo de 2012), cita obligada para todo aquel a quien le pique el gusanillo de la seguridad informática y... quiera saber lo que es una cerveza con una tapa en condiciones ;-)

C/ Guadalquivir nº 62 - Bajo Derecha, 23003 - Jaén enred20@enred20.org


Hosting donado por