

JORGE RODRÍGUEZ CANSECO

Colaborador Computer Security Lab (COSEC)

<https://es.linkedin.com/pub/jorge-rodriguezcanseco/a7/94/337>

Graduado en Ingeniería Informática por la Universidad Carlos III de Madrid. Es actual colaborador con el COmputer SEcurity Lab (COSEC) de dicha universidad, y lo fue previamente del grupo de arquitecturas y sistemas.

Ha trabajado en temas relacionados con la Informática Forense y el análisis de memoria volátil, llegando a presentar MONOCLE, su propio framework automatizado para análisis forense por medio de scripts.

En la actualidad se encuentra cursando el máster universitario en Ciberseguridad, impartido por la Universidad Carlos III de Madrid. Sus intereses incluyen la criptografía, el análisis formal de protocolos y el análisis de malware.

¿Por qué participar en el CIBSI / TIBETS?

CIBSI/TIBETS es un gran esfuerzo conjunto que reúne a un gran número de especialistas y expertos que tratan de hacer de nuestro cada vez más digitalizado mundo, un lugar más seguro.

La amplia variedad en los temas que se tratan en el lo hacen interesante para conocer de primera mano los avances que se están realizando en la actualidad, siendo de interés para un numeroso público.

En su opinión, ¿cuál es la relevancia de su investigación en este Congreso?

En CIBSI 2015, presento MONOCLE, un framework para el análisis forense automatizado. Debido al gran número de tecnologías presentes hoy en día, es difícil que un analista forense sea capaz de estar familiarizado con todas y cada una de ellas.

Adicionalmente, el proceso de análisis de un equipo incluye normalmente muchas etapas que son siempre realizadas del mismo modo.

Con MONOCLE pretendemos ofrecer una nueva manera de abordar dichos análisis, ofreciendo un framework que sea capaz de realizar estas tareas de forma automática por medio de scripts.

Si bien se encuentra en sus primeras etapas de desarrollo, este ya ha demostrado su efectividad y potencial en los test realizados.

¿Cuál piensa que será el devenir de la Seguridad de la Información?

La progresiva instauración de una sociedad en donde la mayoría de la información (tanto pública como privada) es cada vez mas accesible desde la red, propone nuevos retos que debemos afrontar.

Cada nuevo dispositivo presenta una nueva amenaza a la seguridad que, en caso de no controlarse, puede poner en peligro a los usuarios.

Esto unido a la mejora en las capacidades de dichos dispositivos provoca que la sociedad sea cada vez mas susceptible a sufrir ataques por medio de la Red.

El trabajo constante para proteger la seguridad de la información es un tema que, por suerte, está cada vez más interiorizado en la sociedad y por parte de las empresas.

El esfuerzo conjunto y la concienciación ciudadana son los pilares en los que debemos apoyarnos a fin de tratar de ir un paso por delante

en materia de seguridad informática.

¿Cuál es el mayor riesgo que tiene una sociedad como la Iberoamericana en materia de ciberseguridad?

El mayor riesgo que presenta una sociedad es la falta de concienciación. El hecho de que Latinoamérica no sea de las sociedades mas azotadas por el cibercrimen, no implica que nunca vaya a serlo. Es por esto que es necesario invertir en mecanismos y métodos que permitan estar preparados para dichos eventos en caso de que se produzcan.

Si se hace patente para la sociedad el hecho de que este peligro es actual y muy real, será posible incluir más medidas al respecto desde la base a medida que las empresas y las infraestructuras crecen.

¿Cómo ve a Latinoamérica en materia de seguridad de la información frente al resto del mundo?

Latinoamérica es una región que está comenzando a interiorizar el hecho de que los ataques a la seguridad de la información son un riesgo muy importante a tener en cuenta.

Iniciativas como este mismo congreso son prueba fehaciente de ello. El trabajo duro y la perseverancia son las mejores armas para defenderse de los peligros que entraña el mundo virtual.

ARTÍCULOS PRESENTADOS EN CIBSI-TIBETS 2015

MONOCLE – Extensible open-source forensic tool applied to cloud storage cases. *Full Paper*

Martes, 10 Noviembre
Bloque Seguridad en Cloud y Patrones