Dr. Moisés Salinas-Rosales

Profesor Investigador

Seguridad de la Información

Domicilio laboral:
Centro de Investigación en Computación - Instituto Politécnico Nacional
Av. Juan de Dios Bátiz, Esq. Miguel Othón de Mendizabal
Nueva Industrial Vallejo
México City, D. F. 07738
Phone +52 55 57296000 ext. 56595
Email: msalinasr@ipn.mx

1. Formación Académica

• Instituto Politécnico Nacional	Doctorado en Comunicaciones y Electrónica	2009
• The University of Electro-communications	Course on Japanese University Studies in Science and Techology	2003
• Instituto Politécnico Nacional	Maestría en Ciencias de Ingeniería en Microelectrónica	2002
• Instituto Politécnico Nacional	Ingeniería en Computación	1999

2. Empleos

2.1 Centro de Investigación en Computación - IPN

• Profesor Titular "C" Tiempo Completo	Departamento de Investigación en Ingeniería de Cómputo Laboratorio de Ciberseguridad	01/2015 –
• Profesor Titular "B" Tiempo Completo	Departamento de Investigación en Ingeniería de Cómputo Laboratorio de Comunicaciones y redes de Computadoras	01/2013-12/2014
• Jefe de Departamento	Departamento de Desarrollo de Aplicaciones	02/2012-08/2014

2.2 Escuela Superior de Ingeniería Mecánica y Eléctrica, Unidad Culhuacan - IPN

• Profesor Titular "A" Medio Tiempo	Departamento de Ingeniería en Computación	2010-2012
• Profesor Asociado "C" Medio Tiempo	Departamento de Ingeniería en Computación	2006-2010
• Profesor de Asignatura	Sección de Estudios de Posgrado e Investigación	2006-2012
• Profesor de Asignatura	Departamento de Ingeniería en Computación	2000-2006

3. Intereses de Investigación

- Protocolos Criptográficos
- Implementaciones Criptográficas de bajo consumo de energía
- Desarrollo de software seguro
- Detección y Prevención de Ransomware

4. Distinciones

• Sistema Nacional de Investigadores CONACYT	Candidato a Investigador Nacional	2015-2017
• The University of Electro-communications	Best Exchange Student Award	2003

5. Actividades Profesionales

5.1 Organización de Conferencias

• Chair of Technical Program	Congreso Estudiantil de Proyectos y Prototipos de Ingeniería en Computación	2010
• Member of Diffusion Committee	Latincrypt Conference 2012	2012

5.2 Comités de Programa Científico

• Member of Program Committee	Congreso Estudiantil de Proyectos y Prototipos de Ingeniería en Computación	2011, 2012, 2013
• Member of Program Committee	CORE Conference at CIC-IPN	2015, 2016

5.3 Actividades profesionales fuera de la academia

• IT Infrastructure Manager	Colegio Hebreo Maguen David, A.C.	2003-2007
• Consultor de Sistemas Unix	ORT Mexico	1999-2003
• Programador	SAS Microsystems	2000
• Administrador de Sistemas	Instituto Federal Electoral (IFE)	1999
• Linux Systems Administrator	Dept. of Ingeniería en Computación en ESIME Culhuacan-IPN	1998-2000

6. Actividades Académicas

6.1 Cursos impartidos en el IPN:

- Sel. Topics on Computing: Cryptography
- Sel. Topics on Computing: Information Security
- Sel. Topics on Computing: Introduction to Cryptography
- Sel. Topics on Computing: Cryptpgraphic Protocols and Applications
- Informatics Auditing
- Security on Operating Systems
- Introduction to Crypography
- Cryptographic Hardware
- Discrete Mathematics
- Object Oriented Programming
- Operating Systems
- Distribuited Systems
- Foundations on Programming
- Analysis of Algorithms

6.2 Comisiones Académicas desarrolladas en el IPN

• Miembro de la Comisión para los nuevos planes de estudio para los programas de Maestría en Ciencias en Ingeniería de Cómputo y Maestría en Ciencias de la Computación en el CIC-IPN.	2015
• Coordinador Académico del Programa de Especialid.ad en Seguridad Informática y Tecnologías de la Información en ESIME Culhuacan-IPN	2010-2012
• Miembro de la Comisión para la creación del plan de estudio para el programa profesionalizante de Maestría en Ingeniería en Seguridad y Tecnologías de la Información en ESIME Culhuacan –IPN.	2008-2009
• Presidente de la Academia de Computación del Departamento de Ingeniería en Computación en ESIME Culhuacan-IPN.	2006-2008
• Miembro de la Comisión para la creación del plan de estudio para el programa de Especialidad en Seguridad Informática y Tecnologías de la Información en ESIME Culhuacan-IPN	2005-2006

6.3 Dirección de Tesis

• *Universal Steganographic Detector Based on Artificial Immune System for JPEG Images*, José de Jesus Serrano-Perez, CIC-IPN.	M. Sc.	2016
• *Diseño de un protocolo para distribuir llaves criptográficas en una comunicación multipartita*, Oscar Ruiz Palma, CIC-IPN.	M. Sc.	2015
• *Confidencialidad en VoIP para el sistema operativo Android*, Joel Martínez Ortuño, CIC-IPN.	M. Sc.	2014
• *Esquema de cifrado para la transmisión de video en sistema operativo LINUX*, Mónica García Cortés, , CIC-IPN.	M. Sc.	2014
• *Diseño de técnica de endurecimiento en binarios ejecutables para desbordamiento de memoria*, Alfreo Orrala Contreras, SEPI ESIMECU-IPN	M. Eng.	2014
• *Diseño de una implementación en FPGA del cifrador Camelia*, Victor Sampedro Rodríguez, SEPI ESIMECU-IPN	M. Eng.	2013
• *Estructura de controles técnicos open-source que permitan implementar los dominios del ISO 27001 a las PyMES*, Sergio Vargas Salinas, SEPI ESIMECU-IPN	M. Eng.	2013
• *Análisis y diseño de una aplicación segura de facturación electrónica para dispositivos móviles*, Rodrigo Jurado Barrera, Sec. Computación, CINVESTAV	M. Sc.	2012

- *Diseño de estructuras en hardware reconfigurable para aritmética de campos finitos binarios*, Jose Antonio Flores Escobar, SEPI ESIMECU-IPN — M. Eng. — 2012
- *Propuesta de un marco nomativo para el uso de controles criptográficos en APF*, Francisco Asiaín Alvarez, SEPI ESIMECU-IPN — Speciality — 2010
- *Algorítmos de Firma Digital del Estándar DSS y su uso en una Organización Pública*, Simón Pedro Torres, SEPI ESIMECU-IPN — Speciality — 2010
- *Propuesta de un procedimiento de endurecimiento para servidores según las mejores prácticas*, Omar Cyprian Sánchez, SEPI ESIMECU-IPN — Speciality — 2010
- *Comparativa de seguridad de algorítmos para resumenes criptográficos*, Alejandro Chacón Zárate, SEPI ESIMECU-IPN — Speciality — 2010
- *Comparativa de seguridad de algorítmos de cifrado asimétrico*, Roberto Villegas Gómez, SEPI ESIMECU-IPN — Speciality — 2010
- *Revisión de normas ye stándares de sistemas de gestión de seguridad de la información*, Fernando Alcántar Hernández, SEPI ESIMECU-IPN — Speciality — 2010
- *Estrategías de difusión y concientización en sistemas de gestión de seguridad de la información*, Javier Alfredo Reyes Domínguez, SEPI ESIMECU-IPN — Speciality — 2010
- *Aplicación del Estándar de Confiablidad CIP-002 en sistemas EMS/S]CADA del Sistema Eléctrico de Potencia*, Carlos Antonio Moreno Rivera, SEPI ESIMECU-IPN — Speciality — 2009
- *Buenas prácticas de ISD para la seguridad informática en TI*, Jorge Alberto Sosa Ortiz, SEPI ESIMECU-IPN, SEPI ESIMECU-IPN — Speciality — 2009
- *Diseño de una implementación del cifrador RSA en Matlab*, Inti Pavel Hernández Orozco, Aldo Pedro Macías Ruíz, ESIMECU-IPN — B. Eng. — 2010
- *Biblioteca de Artimética de Campo Finito en C*, Analí Elidia Luz Camacho, ESIMECU-IPN — B. Eng. — 2010
- *Componente en HMAC*, Ediel González Huitrón, ESIMECU-IPN — B. Eng. — 2010

7. Publicaciones

7.1 Llibros y capítulos de libros

- "Seguridad en Sistemas de Información" appeared on Plataforma méxico: La expresión tecnológica del Nuevo Modelo de Policía, Ed. Centro de Investigación y Estudios en Seguridad, MEXICO. — ISBN 978-607-95867-4-4 — 2012

7.2 Artículos en revistas

- Aguirre-Anaya Eleazar, Acosta-Bermejo Raúl, Salinas-Rosales Moisés, Sánchez Fraga Rolando, *Towards a Faceted Taxonomy of Denial-of-Service Vulnerabilities in the Linux Kernel*, pub on Research in computing Science, Vol. 81, pp 123-133, ISSN: 1870-4069 — ISSN 1870-4069 — 2014
- Gina Gallegos-Garcia, Aurora Molina, Gabriel Gallegos-Garcia, Moisés Salinas R. Gualberto Aguilar-Torres, *Modelado de un sistema de voto electrónico*, pub on Rev. Digital Universitaria, Vol. 15, No. 4 , ISSN: 1607 - 6079 — ISSN 1607-6079 — 2014
- Moisés Salinas Rosales, Gonzalo Duchén Sánchez, *Protocolo de autenticación basado en identidad redes inalámbricas sensores*, pub on Rev. Facultad de Ingeniería Universidad de Antioquia, No. 52 , ISSN: 0120-6230 — ISSN 0120-6230 — 2010
- Moisés Salinas Rosales, Gina Gallegos-García and Gonzalo Duchén-Sánchez *Efficient Message Authentication Protocol for WSN*, pub on WSEAS Transaction on Computers. Issue 6, Vol 9, ISSN: 1109-2750. — ISSN 1109-2750 — 2009

7.3 Artículos en Conferencias Internacionales

- Serrano-Pérez, Salinas-Rosales**,** Cruz-Cortés**,** *Universal Steganography Detector Based on an Artificial Inmune Systems for JPEG Images,* pub on Proc. The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE. — 2016
- Serrano Pérez José de Jesús, Salinas Rosales Moisés**,** Cruz Cortés Nareli**,** *Sistema inmune artificial para estegoanalisis de imágenes JPEG,* pub on Proc. Congreso Mexicano de Inteligencia Artificial, COMIA 2016. — 2016
- Rodríguez Mota Abraham, Escamilla Ambrosio Ponciano Jorge, Morales Ortega Salvador, Salinas Rosales Moisés, Aguirre Anaya Eleazar, *Image compressive sensing cryptographic analysis*, pub on Proc**.** 26th IEEE International Conference on Electronics, Communications and Computers — 2016

(CONIELECOMP), pp 54-61, ISBN: 978-1-5090-0079-1.

- Escamilla Ambrosio Ponciano Jorge, Salinas Rosales Moisés, Aguirre Anaya Eleazar, Acosta Bermejo Raúl, *Towards a 2-hybrid Android malware detection test framework*, pub on Proc**.** 26th IEEE International Conference on Electronics, Communications and Computers (CONIELECOMP), pp 81-86, ISBN: 978-1-5090-0079-1. 2016
- Escamilla Ambrosio Ponciano Jorge, Salinas Rosales Moisés, Acosta Bermejo Raúl, Rodríguez Mota Abraham, *Internet de las Cosas: 50 Mil Millones de Puntos Inseguros*, pub on Proc**.** SOMI XXX Congreso de Instrumentación, ISBN: 2395-8499. 2015
- Garcia Flores Raúl Santiago, Salinas Rosales Moisés, Aguirre Anaya Eleazar, *Confidentiality for Hadoop Distributed File System (HDFS*, pub on Proc**.** Encuentro Nacional de Ciencias de la Computación SMCC ENC 2015. 2015
- Escamilla Ambrosio Ponciano Jorge, Salinas Rosales Moisés, Acosta Bermejo Raúl, Rodríguez Mota Abraham, *Internet de las cosas: estado actual, retos y perspectivas*, pub on Proc**.** SOMI XXVIII Congreso de Instrumentación. 2013
- Jose A. Flores E., Moises Salinas R., Jose Velázquez L , *Finite Field Polynomial 16-bit Multiplier for Power Constrained Devices***,** pub on Proc. IEEE International Conference on electrical Communications and Computers 2012, ISBN: 978-1-61284-1324-8 2012

  Moises Salinas R., Gina Gallegos G., Gonzalo Duchén S., *Message Authentication for Wireless Sensor Neworks*, pub on Proc. WSEAS ICCIS 2009**,** ISBN: 978-960-474-071-0. 2009
- Gina Gallegos G., Roberto Gómez C., Moises Salinas R., Gonzalo Duchén S , *A New and Secure Electronic Voting Protocol based on Bilinear Pairings*, pub on Proc. IEEE International Conference on electrical Communications and Computers 2009, ISBN 978-0-7695-3587-6. 2009
- Moises Salinas R., Gina Gallegos G., Gonzalo Duchén S., *An authentication Protocol for Sensor Networks using Pairings*, pub on Proc. IEEE International Conference on electrical Communications and Computers 2009, ISBN 978-0-7695-3587-6. 2009
- Gualberto Aguilar, Gabriel Sánchez, Karina Toscano, Moisés Salinas, Mariko Nakano, Hector Perez, *Fingerprint Recognition*, pub on Proc Second International Conference on. Internet Monitoring and Protection, 2007. ICIMP 2007, ISBN: 0-7695-2911-9. 2007
- M. Monzoy-Villuendas, M. Salinas-Rosales, M. Nakano-Miyatake, H. M. Perez-Meana, *Fragile watermarking for color image authentication*, pub on Proc. International Conference on Electrical and Electronics Engineering 2007, ISBN: 978-1-4244-1166-5. 2007
- Masahiro Mambo, Moises Rosales Salinas, Kazuo Ohta, Noboru Kunihiro*, Problems on the MR Micropayment Schemes*, pub on Proc. ACM Symposium on Information, Computer and Communications Security 2006, ISBN:1-59593-272-0 . 2006
- Gina Gallegos, Rubén Vázquez, Moisés Salinas*, Alternativa de solución al esquema de micropago MR3*, pub o Actas del Tercer Congreso Iberoamericano de Seguridad Informática CIBSI 2005, ISBN: 956-7051-10-0. 2005

7.4 Artículos en Conferencias Nacionales

- Edelia Beltrán Arreola, Gina Gallegos García, Moisés Salinas Rosales, Gonzalo Duchén Sánchez, *Diferencias de la primitiva criptográfica de cifrado usando criptografía de clave pública y clave pública basada en la identidad,* pub on: Memorias de la Reunión de Otoño de Potencia, Electrónica y Computación 2010. ISBN: 978-607-95476-1-5. 2010

7.5 Citas a publicaciones

- Favor de referirse a: http://scholar.google.com.mx/citations?user=8-3c8w4AAAAJ&hl=en

8. Actividades de Investigación

8.1 Dirección de Proyectos con Financiamiento

- Modelos de detección de canales encubiertos en redes IP. SIP 20150411 IPN grant for 30,500 MXP 2015
- Diseño de una biblioteca aritmética para criptografía en sistemas de cómputo con recursos limitados SIP 20100088 SIP 20110141 IPN grant for 50,000 MXP 2010-2011

8.2 Colaboración en Proyectos con Financiamiento

• Monitoreo de acceso remoto no autorizado a información privada	CONACYT PN13 216747 SIP-2014-RE/098	2016-2013
• Efficient monitoring for malicious software detection on android smartphones.	SIP 20150617	2015
• Mecanismo de Autenticación para Sistemas de Información Criptográfico-biométricos	SIP 20141357	2014
• Análisis de malware en dispositivo móviles	SIP 20144161	2014
• Controles de seguridad para ambientes móviles	SIP 20131363	2013

9. Propiedad Intelectual

9.1 Autoría de Software

• Visor del Acervo Digital del STC	INDAUTOR 03-2014-111810114800-01	2015
• Sistema de Administración del Acervo Digital para el STC	INDAUTOR 03-2014-111810022700-01	2015
• OSF++V0.9	INDAUTOR 03-2014-030610480500-01	2014
• Database Fingerprint AOP 1,0	INDAUTOR 03-2014-022811065500-01	2014
• Sistema de Enrolamiento Desktop	INDAUTOR 03-2013-041910315100-01	2013
• Sistema de Administración de Publicaciones Electrónicas CIC	INDAUTOR 03-2013-082112415500-01	2013
• Sistema de Administración de una Base de Datos Escolar (SABER)	INDAUTOR 03-2013-101010505600-01	2013
• Lector de Revistas CIC para Ipad	INDAUTOR 03-2013-082112402300-01	2013
• Generación de Petición para Firma de Certificado Digital	INDAUTOR 03-2013-111511135200-01	2013
• Componente de Autenticación	INDAUTOR 03-2013-041910181400-01	2013
• Aplicación “Toma Fotos”	INDAUTOR 03-2013-041910201300-01	2013
• Sistema de Votación Electrónica IEDF	INDAUTOR 03-2012-082111373800-01	2012
• Software de Análisis de tráficode red para un Sistema Difuso	INDAUTOR 03-2012-092411070500-01	2012
• Sistema Integral de Registro Biométrico	INDAUTOR 03-2012-121912312200-01	2012
• Software para la estimacion de tiempo en nanosegundos de llamadas al sistema en GNU/LINUX	INDAUTOR 03-2011-103110442900-01	2011
• Componente de HMAC para TinyOS	INDAUTOR 03-2011-092211234900-01	2011
• Componente de Aritmética de campo finito GF(2M) en NesC	INDAUTOR 03-2011-092211175000-01	2011
• Cifrador CCMX128	INDAUTOR 03-2011-092211001700-01	2011
• Criptografía Visual basada en el esquema del umbral	INDAUTOR 03-2011-060310132700-01	2011