Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización

Javier Díaz, Lía Molinari, Paula Venosa, Nicolás Macia, Einar Lanfranco, Alejandro Sabolansky

Laboratorio de Investigación de Nuevas Tecnologías Informáticas (LINTI). Facultad de Informática. Universidad Nacional de La Plata. 50 y 120. La Plata

{javierd,lmolinari,pvenosa,nmacia,einar,asabolansky}@info.unlp.edu.ar

Resumen

Desde los inicios de la década del 2000, el LINTI desarrolla una línea de investigación en seguridad, inicialmente, y ciberseguridad en la actualidad, que no ha tenido interrupciones. Importantes experiencias como CERTUNLP, PKIGRID UNLP, entre otras, fueron la implementación que ejercitan las actividades de investigación que se realizan. La evolución de las TICs conlleva situaciones de riesgo que se van revelando día a día. Tecnologías emergentes habilitan el tratamiento de gran cantidad de datos, pero también habilitan su exposición. La investigación sobre tendencias y comportamientos es una tarea de investigación que muchas veces trasciende lo informático. En este artículo se afianza la línea de investigación existente con la inclusión de nuevos desafíos como IoT, forensia, desarrollo seguro de aplicaciones, normativa, estándares y buenas prácticas, y el habitual compromiso de trasladar los resultados de la investigación a la docencia y a la extensión, enfocados a formar profesionales con habilidades, capacidades y conocimientos para entender y administrar adecuadamente los sistemas de gestión de la ciberseguridad.

Palabras clave: seguridad de la información, CSIRTs, Internet de las cosas, forensia, PKI

Contexto

La línea de investigación “Ciberseguridad” presentada en este trabajo, se inserta en el proyecto de investigación "Internet del Futuro: Ciudades Digitales Inclusivas, Innovadoras y Sustentables, IoT, Ciberseguridad, Espacios de Aprendizaje del Futuro" del Programa Nacional de Incentivos a docentes-investigadores, que se desarrolla en el LINTI de la Facultad de Informática de la Universidad Nacional de La Plata (UNLP). Este proyecto está acreditado por la UNLP y financiado por partidas del presupuesto nacional.

Introducción

Las Tecnologías de la Información y las Comunicaciones (TIC) están incorporadas en todos los aspectos de la vida cotidiana. Entre otras situaciones, los precios cada vez más accesibles de los dispositivos de conexión a Internet han permitido su uso masivo, y han pasado a ser un accesorio imprescindible en la vida de las personas y las organizaciones. Ubicuo, instantáneo, actualizado, son adjetivos que acompañan el anuncio de los servicios tecnológicos.

No sólo el abaratamiento de los dispositivos ha contribuido a esa apropiación: la facilidad de uso, que no requiere un alto grado de especialización (el período entre la adquisición y la puesta en funcionamiento es cada vez más corto), la posibilidad de almacenamiento en la

nube terminó con las restricciones de espacio y la oferta de aplicaciones en diferentes "stores" invitan a la instalación entusiasta.
Ya no sólo se conectan personas y máquinas: Internet de las cosas (Internet of Things, IoT) habilita la conexión de las máquinas entre sí, sin la intervención de humanos.
No obstante, todas estas ventajas y beneficios pueden transformarse en una verdadera amenaza para quienes no tienen recaudos. Robo de identidad, grooming, carding, entre otras, son situaciones no deseadas que llegaron junto con las TICs.
La promulgación de leyes que contemplan la figura del delito informático, ha alimentado la esperanza que se condene a quienes lo cometen. Pero la determinación de responsabilidades en el mundo digital exige un conocimiento especializado y experiencia en una disciplina en constante evolución.
Ante una denuncia de un potencial delito, los diferentes actores que intervienen necesitan recurrir a profesionales con un alto grado de especialización no sólo desde el punto de vista técnico, sino legal y ético. Esto ha generado una demanda de capacidades y competencias que habitualmente no están consideradas en los contenidos de las currículas.
Si bien siempre la normativa surge luego del uso, un alto grado de sensibilización sobre las vulnerabilidades y amenazas en el mundo digital ha generado una importante cantidad de estándares, buenas prácticas y guías para la gestión de la ciberseguridad. Regulaciones y directivas sobre los datos, intentan establecer pautas claras acerca de la garantía de privacidad.
Al mismo tiempo, la enseñanza basada en competencias, tendencia que está presente en las Reformas educativas de fines de los 90 en algunos países como Francia, Bélgica, hoy ya ha alcanzado también a los países latinoamericanos (Spiegel, 2008) (IEEE, 2013). Estas formas de aprender se ponen en práctica en todos los niveles educativos y se aplican fácilmente en la educación superior.
El Laboratorio de Investigación en Nuevas Tecnologías Informáticas (LINTI) de la Facultad de Informática de la Universidad Nacional de La Plata sostiene desde el año 2001 una línea de investigación, docencia, extensión y transferencia en ciberseguridad. La publicación de artículos en congresos nacionales e internacionales, la participación en competencias CTF (Capture the flag) con excelentes resultados, la creación de una Infraestructura de Clave Pública (Public Infrastructure Key, PKI) en el 2006[1] y su continuidad a la fecha, la creación y administración de CERT UNLP[2], la participación en proyectos de Extensión y Transferencia, y la actualización constante de los contenidos de las asignaturas a su cargo, entre otros logros, han permitido contar con un equipo de profesionales con alto grado de especialización tanto en conocimientos como en experiencia, sumado al perfil ético que garantizan una formación integral.
En este contexto de constante desafío se hace necesario incorporar contenidos relacionados con estas tecnologías emergentes y las situaciones de riesgo que conllevan, en docencia, investigación, extensión y transferencia.

Líneas de Investigación y Desarrollo

La ciberseguridad es una temática que es transversal a las diferentes ramas de las TICs. Redes, bases de datos, autenticación, desarrollo de aplicaciones, entre otros, deben dedicar un espacio a la ciberseguridad para poder hablar de "contextos seguros".
La línea de investigación que se describe aborda, entre otros:

1. Tendencias en incidentes de seguridad y su gestión. Como integrantes del Centro de Respuesta a Incidentes de Seguridad de la Información de la Universidad Nacional de La Plata (CERTUNLP), a

[1] www.pkigrid.unlp.edu.ar
[2] www.cert.unlp.edu.ar

la hora de gestionar los incidentes resulta fundamental conocer cuáles son los problemas más críticos a los que las organizaciones se enfrentan hoy en día (Venosa P.,2014), las técnicas que se utilizan para llevar a cabo los ataques y cómo mitigar los mismos (Francisco Javier Díaz,2017).

2. Forensia digital. La forensia digital constituye una etapa fundamental en el proceso de gestión de incidentes a la hora de investigar las características de un incidente, permitiendo obtener los detalles de lo que ocurrió y aprender de ello. Resulta de gran importancia investigar las técnicas utilizadas en el análisis forense y seleccionar herramientas que den soporte para automatizar las tareas asociadas. (Diaz J., 2016)
3. Infraestructura de clave pública PKI. En el marco de Americas Grid Policy Management Authority[3] (TAGPMA), la prestación del servicio de emisión de certificados digitales a través de PKIGrid UNLP, incluye el estudio de vulnerabilidades que surgen en relación al manejo de claves, algoritmos, etc, así como el análisis de los protocolos, procedimientos y herramientas que se utilizan a fin de garantizar que la gestión de certificados cumple con los requisitos de seguridad exigidos.
4. Seguridad en IoT. La aparición y evolución de IoT que trae consigo la posibilidad de conectar todo tipo de objeto doméstico a las redes, no ha requerido grandes cambios en la estructura de Internet, ya que varios protocolos del stack TCP/IP se reutilizan en IoT (IPv6, UDP, TCP, HTTP, entre otros). En este marco, es necesario que las aplicaciones aseguren la confidencialidad, integridad y autenticidad de los datos que almacenan y se envían entre las diferentes componentes. En consecuencia, debe proveerse seguridad tanto en dichas componentes como en el proceso de comunicación entre las mismas, teniendo en cuenta las diferentes capas de red y la sensibilidad de los datos que las mismas manejan. (Diaz J., 2017)
5. Desarrollo seguro de software. Para entender cómo desarrollar de forma menos insegura es necesario conocer cuáles son los problemas de seguridad que afectan al software, cuáles son las consecuencias de que alguien explote esos problemas y cuáles son las mejores técnicas y herramientas disponibles para evitar desarrollar explotable.
6. Entrenamientos de seguridad. Los CTF (Capture the flag)(Vigna, 2014) son competencias de seguridad informática donde un equipo puede poner en práctica sus habilidades para descubrir vulnerabilidades, explotarlas así como también resolver problemas. Hay dos tipos de competencias:
    - CTF – Capture The Flag: Competencias de tipo ataque / defensa
    - Jeopardy: Competencias tipo pregunta / respuesta, donde se presentan distintas categorías de desafíos, como ser: forensia, esteganografía, criptografía, redes, explotación web, etc.
7. Normativa, marcos referenciales y buenas prácticas. Es sabido que la normativa se define luego del uso. Los estándares genéricos son la base para la elaboración de normativa en general, políticas y estrategias. Enunciadas tendencias acerca de regular la privacidad se hacen realidad como es el caso de European General Data Privacy Regulation (EU - GDPR)[4], con fecha de

[3] www.tagpma.org

[4] https://www.eugdpr.org/

aplicación en Mayo del corriente año. Conceptos como anonimización (anonymization) y pseudo-anonimización (pseudo-anonymization) empiezan a preocupar a los administradores de big data. Evidencia del interés es esta línea de trabajo son varios artículos publicados (Díaz, Molinari, 2017).

Resultados obtenidos/esperados

Como principales objetivos se plantean:

- Consolidar la línea de investigación en ciberseguridad y su aplicación en la docencia y la extensión, trabajando sobre los temas emergentes asociados a las metodologías y paradigmas que surgen día a día.
- Promover las prácticas en lo que hace a tener en cuenta la seguridad en todas las etapas del ciclo de vida del desarrollo, de los servicios y de la gestión de la organización.
- Transmitir la experiencia adquirida en los distintos proyectos y actividades a los alumnos de las cátedras de grado y postgrado con contenidos afines de nuestra Facultad.
- Realizar actividades de difusión, capacitación y sensibilización en el uso del espacio digital con la comunidad, relacionados con las problemáticas actuales que los involucran.
- Conformar un equipo interdisciplinario para el análisis de situaciones que trascienden lo del mundo de las TICs, para evaluar tendencias y propuestas de sensibilización en el uso del espacio digital.

Partiendo de esos objetivos y dentro de las temáticas y proyectos descritos en secciones anteriores se ha arribado a los siguientes resultados:

- Como parte del proyecto vinculado al Centro de Excelencia en Ciberseguridad de la ITU5, del que formamos parte, se han diseñado los cursos “Ciberseguridad: primeros pasos de un gran desafío” y “CSIRT: coordinando prevención, detección, manejo de incidentes, respuesta y mitigación de ciberataques”, que son parte de la oferta de formación para el año 2018. En mayo de 2018 se realizará el Cyberdrill6 de la ITU y la UNLP será anfitrión. El equipo de Ciberseguridad de la UNLP será el organizador.
- También a partir de la investigación en esta línea se han armado y dictado varias iniciativas en 2017: un taller de seguridad en IoT en el marco del curso de Postgrado “Internet de las cosas”; un taller de seguridad Informática en la UNNOBA, dirigido a docentes, graduados y alumnos avanzados; y se ha organizado una jornada de seguridad en la Facultad de Informática de la UNLP en el marco de la semana de la seguridad informática en noviembre de 2017.
- Desde el año 2017 se planificaron y realizaron encuentros semanales en los que un grupo de docentes y alumnos trabajan en temáticas relacionadas a las competencias de seguridad, intercambiando experiencias adquiridas en los últimos concursos en los que hubo participación y estudiando nuevas metodologías. Esta actividad se enmarca en los grupos de interés definidos por la Secretaría de Innovación de la Facultad.

Formación de Recursos Humanos

El equipo de trabajo que lleva adelante estas líneas forma parte del LINTI. El mismo está formado por docentes/investigadores de la Facultad de Informática de la UNLP. En el marco de sus actividades, tiene entre sus funciones la dirección de tesis relacionadas con las temáticas en las que trabaja.
Ese equipo ha dirigido varias tesinas de grado

5

https://academy.itu.int/index.php?option=com_content&view=article&id=154&Itemid=588&lang=en

6 https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2018/20577.aspx

en la presente línea de investigación. Aquéllas que se han finalizado en el último año han sido: "Análisis y mejoras de seguridad a una aplicación prototipo en IoT" del alumno Bruno Pertini, "Análisis e implementación de RPZ" del alumno Matías Ferrigno, "Uso de smartphones para auditar la seguridad de redes inalámbricas" de los alumnos Juan Ignacio Bernal y Alejandro Zurita (Venosa P.,2017) y "Ampliación y mejora de servicios en la infraestructura de clave pública para e-ciencia de la UNLP (PKIGrid UNLP)". de los alumnos Guido Celada y Juan Manuel Filandini.
Además como trabajo final de la cátedra Seguridad y Privacidad en Redes de la cual dos docentes de este grupo forman parte, dos alumnos han investigado sobre el protocolo LORA y el análisis de su seguridad, continuando con temáticas de seguridad en IoT a fin de fortalecer este eje de investigación.
En el marco del proceso de formación continua del equipo, el profesor Nicolás Macia, ha presentado su tesis para obtener el título de Magister en Redes de Datos de la UNLP, realizando el trabajo titulado "Diseño y desarrollo de un mecanismo más seguro de manejo de sesiones web". Finalmente, la profesora Lía Molinari ha expuesto su tesis doctoral titulada "Modelo de Gestión para la Prevención de Lavado de Activos (PLA) en el sector de juegos de azar". Este trabajo plantea un enfoque orientado al riesgo basado en diferentes marcos referenciales y estándares en la gestión de la seguridad de los sistemas de información.

Bibliografía

IEEE (2013). http://ieeexplore.ieee.org/abstract/document/6521304/?reload=true

Venosa P., Díaz J. (2014). Detección de botnets utilizando herramientas Opensource. WICC 2014. ISBN 978-950-34-1084-4

Diaz J., Molinari L., Belalcazar A. Ron M (2017). Towards a Strategic Resilience of Applications through the NIST Cybersecurity Framework and the Strategic Alignment Model (SAM). INCISCOS 2017. Quito, Ecuador.

Javier Dıaz, Paula Venosa, Nicolas Macia, Einar Lanfranco,Alejandro Sabolansky, Damian Rubio, (2016). Análisis digital forense utilizando herramientas de software libre. WICC 2016. ISBN: 978-950-698-377-2

Díaz J., Venosa P., Fava L., Castro N., Vilches D., López F. (2017). Estrategias de IoT para Lograr Ciudades Digitales Seguras, más Inclusivas y Sustentables. WICC 2017. ISBN 978-987-42-5143-5.

Venosa P., Diaz J. (2014). Detección de botnets utilizando herramientas Opensource. WICC 2014. ISBN 978-950-34-1084-4

Venosa P., Macia M., Lanfranco E., Sabolansky A. (2017). Análisis de Seguridad en Redes Wireless Utilizando Dispositivos Móviles. WICC 2017. ISBN 978-987-42-5143-5.

Stiefel, Berta Marco (2008). Competencias básicas: Hacia un nuevo paradigma educativo. Narcea Ediciones.

Francisco Javier Díaz, Alejandro Sabolansky, Nicolás Macia, Paula Venosa, Einar Lanfranco, Mitigación de DDoS en Redes Académicas e IXPs . CIBSI 2017.