Investigación en ciberseguridad: Nuevos desafíos para adaptarse a nuevos paradigmas

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 de manera ininterrumpida una línea de investigación en seguridad informática, inicialmente, y en ciberseguridad en la actualidad[1]. Importantes proyectos como el establecimiento del CSIRT académico CERTUNLP[2] y de la autoridad de certificación PKIGRID UNLP[3], así como el afianzamiento del equipo de CTF SYPER[4] plasmado en varios premios obtenidos, son ejemplos concretos de implementaciones que plasman las actividades de investigación que se llevan a cabo.

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 sumando nuevas temáticas como la implementación de monitoreo de seguridad inteligente y el análisis de nuevas amenazas en distintas tecnologías.

Las actividades de investigación presentadas se retroalimentan con el habitual compromiso de trasladar los resultados 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: Ciberseguridad, seguridad inteligente, CTFs, Seguridad en aplicaciones, IoT

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"[5] 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.

1. INTRODUCCIÓN

En un mundo cada vez más conectado y con mayor penetración de la tecnología los problemas se multiplican y profundizan, ya que la superficie de ataque crece día a día y las tecnologías continúan mutando y evolucionando. Estos cambios tecnológicos generan que si bien conceptos tradicionales de seguridad de la información como firewalls, los sistemas de detección de intrusiones, los monitores de seguridad de red o los antivirus

continúen siendo necesarios, los mismos tienen que ser complementados con nuevas técnicas y herramientas que enriquezcan la gestión de la ciberseguridad.

Para citar un ejemplo, si uno analiza tráfico de red se notarán grandes diferencias con lo que ocurría hace unos años; en la actualidad se encontrarán grandes volúmenes de información y mucho uso de protocolos de cifrado. Esto lleva a la necesidad de cambiar de paradigma y se percibe que entre las principales tendencias de ciberseguridad se encuentran una percepción de escasez de recursos capacitados y un cambio en el enfoque hacia la detección y respuesta casi en tiempo real[6].

Estos desafíos requerirán nuevos tipos de habilidades en ciencia de datos y análisis. Dado que resulta imposible mitigar todas las amenazas para evitar su concreción, se debe cambiar el enfoque de la ciberseguridad. El esfuerzo debe dejar de concentrarse únicamente en la protección y prevención, para conducirlo más equitativamente a la detección y respuesta.

El término "seguridad inteligente" que se ha comenzado a difundir en los últimos años, hoy en día toma empuje. Los productos de seguridad inteligentes son herramientas que combinan aspectos del aprendizaje automático y de la inteligencia artificial con las aplicaciones de seguridad tradicionales. Estas cuentan con mayor capacidad para adaptarse a nuevas amenazas y asegurar nuevos tipos de aplicaciones. Tienen la capacidad de identificar comportamiento sospechoso, cambios en el malware existente y monitorear contínuamente el tráfico de red para descubrir eventos anómalos.

En los últimos años se han propuesto enfoques basados en tecnologías de aprendizaje automático para detectar malware, aplicando análisis estático y dinámico. Ambos enfoques presentan algunas desventajas. En el caso del análisis estático, el cifrado y las técnicas de ofuscación dificultan la extracción de características del malware. Por otro lado, el análisis dinámico requiere simular el entorno de operación del malware y observar su comportamiento durante un período largo de tiempo, lo cual resulta costoso.

La evolución del aprendizaje automático tiene a la ciberseguridad como nuevo hogar dentro de la transformación digital, ya que las herramientas lo utilizan junto a las prácticas de monitoreo contínuo para ayudar a defenderse, detectar y remediar las amenazas cibernéticas[7].

Más allá de todos los esfuerzos que se lleven a cabo en pos de la seguridad proactiva, los incidentes seguirán ocurriendo, con lo cual es importante gestionarlos en forma eficiente, de manera de minimizar el impacto de los mismos tanto para la organización, como para los usuarios y la red toda. A través del uso de herramientas que automaticen tareas y procedimientos y que se integren con múltiples fuentes de información que detectan problemas, y de los cuales puedan nutrirse posibilitará una gestión más eficiente de los incidentes de seguridad y permitirá mejorar los niveles de madurez de seguridad en las organizaciones.

En términos de mejorar los niveles de seguridad de las organizaciones, la seguridad de los sistemas críticos constituye una de las principales preocupaciones. Ello debe ser considerado en todo el ciclo de vida de los sistemas, desde su desarrollo a su puesta en producción. Es necesario tener en cuenta por ejemplo la administración de la seguridad de la aplicaciones de forma automatizada, ya que dada la cantidad de aplicaciones que hoy están en línea en cualquier centro de cómputos, es muy difícil tenerlo siempre actualizado si se hace manualmente.

En la misma sintonía, resulta fundamental el desarrollo de competencias específicas en ciberseguridad como son las capacidades para testear la seguridad de un sistema así como de poder implementar las mejoras para que un sistema no sea vulnerable. Investigar las nuevas vulnerabilidades, conocer técnicas y herramientas para detectar las mismas, así como estándares para llevar a cabo el proceso de testeo de seguridad, son tareas que forman parte del desafío de contar con sistemas cada vez más seguros en las organizaciones.
La participación en eventos del tipo CTF favorecen el desarrollo de competencias relacionadas a la seguridad de los sistemas, las redes y los servicios, tanto para nuevos recursos humanos que pasan a formar parte del grupo de investigadores como método de capacitación y actualización para aquellos que forman parte del mismo.

2. LÍNEAS DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

En la actualidad, las principales líneas de trabajo en las que el grupo de investigación en ciberseguridad desarrolla sus actividades incluye:

- Monitoreo de seguridad inteligente.
- Formación y actualización a través del desarrollo de competencias mediante la continua participación en concursos de tipo CTF.
- Detección y análisis de vulnerabilidades en distintos tipos de dispositivos, protocolos y tecnologías.
- Gestión de la seguridad de infraestructura
- Gestión de incidentes de seguridad.
- Forensia Digital.
- Infraestructura de clave pública PKI.
- Desarrollo seguro de software.

3. RESULTADOS OBTENIDOS Y ESPERADOS

Como principales objetivos se plantean:

- Crear un mecanismo alternativo para detectar malware que represente una mejora sobre las herramientas utilizadas actualmente. A su vez éste mecanismo debería aprovechar los resultados del análisis realizado por otras herramientas para aplicar técnicas que permitan tomar la mejor decisión a la hora de determinar si la actividad es maliciosa o no. Dicho mecanismo será integrado al servicio de monitoreo proactivo de seguridad utilizado por CERTUNLP para proteger la red de la UNLP.
- 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 buenas prácticas para 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 distintos proyectos y actividades a los alumnos de las cátedras de grado y postgrado con contenidos afines de nuestra Facultad.

Entre los resultados que se han obtenido en este último tiempo:

- Como parte del proyecto vinculado al

Centro de Excelencia en Ciberseguridad de la ITU[12], del que formamos parte durante el año 2018, se dictaron los cursos "Ciberseguridad: primeros pasos de un gran desafío" y "CSIRT: coordinando prevención, detección, manejo de incidentes, respuesta y mitigación de ciberataques".

- En junio de 2018, los autores de este trabajo formaron parte de la organización junto con la ITU el evento internacional denominado "Ciberseguridad desde el Río de La Plata". El mismo se llevó a cabo en las instalaciones de esta casa de estudios contando con la participación de referentes nacionales e internacionales en diversas temáticas relacionadas con la ciberseguridad. Contó con la participación de más de 150 personas a lo largo de cinco extensas jornadas que involucran disertaciones, workshops y talleres prácticos.
- Desde el año 2017, un grupo de docentes y alumnos trabajan en temáticas relacionadas a las competencias de seguridad, intercambiando experiencias adquiridas en los últimos concursos estudiando nuevas metodologías y nuevas herramientas. Esta actividad que se realiza semanalmente, se enmarca en los grupos de interés definidos por la Secretaría de Innovación de la Facultad de Informática. Entre los logros de esta línea de trabajo se destacan la clasificación a participar en el evento presencial de Cyberex 2018 y la obtención del primer puesto en el CTF llevado a cabo en la conferencia Ekoparty en septiembre de 2018.

4. FORMACIÓN DE RECURSOS HUMANOS

En esta línea de investigación trabaja un grupo de docentes/investigadores del LINTI (Laboratorio de Investigación en Nuevas Tecnologías Informáticas) de la Facultad de Informática de la UNLP (Universidad Nacional de La Plata). Este equipo de trabajo también forma parte de CERTUNLP, el CSIRT Académico de la Universidad Nacional de La Plata [15], ámbito en el cual aplican directamente las temáticas propuestas.

Allí pueden realizarse pruebas y evaluar alternativas en un escenario real; y la experiencia y el desarrollo propuesto enriquece los servicios allí brindados que mejoran la ciberseguridad de la red de la UNLP y de la comunidad en general.

En este marco, se encuentran en desarrollo dos tesis para obtener la Maestría en Redes de Datos: "Detección de ataques de seguridad en redes usando técnicas de ensembling" de la Lic. Paula Venosa y "Optimización del control y administración de la seguridad en una red de servidores. Su implementación como software libre para contribuir con MatFel" del Lic. Einar Lanfranco. También está en curso la tesis del doctorando Ignacio Gallardo Urbini titulada "Estrategia de Ciberseguridad distribuida, aplicando el concepto de operación de inteligencia".

En particular la tesis "Detección de ataques de seguridad en redes usando técnicas de ensembling" sumará también al proyecto SLIPS

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

2 https://academy.itu.int/index.php?option=com_content&view=article&layout=edit&id=249&lang=en

[16] del Stratosphere Laboratory en República Checa, que funciona en el ámbito de la CVUT (Czech Technical University in Prague).

Por otra parte, la tesina de grado de Damián Rubio "Evolución del sistema de gestión de incidentes de seguridad orientado a CSIRT de la UNLP - Ngen" está íntimamente ligada al desarrollo y evolución de NGEN, el sistema de gestión de incidentes actualmente usado en CERTUNLP y liberado como software libre para su uso y contribución por parte de la comunidad.

La tesina en curso "Automatizando la resolución de problemas en competencias de seguridad informática" de los alumnos Jeremías Pretto y Facundo Basso profundiza la investigación y el desarrollo de herramientas utilizables en competencias tipo captura tu bandera.

5. REFERENCIAS

[1] - Díaz, Francisco Javier, Molinari, Lía Hebe, Venosa, Paula, Macia, Nicolás, Lanfranco, Einar Felipe, Sabolansky, Alejandro Javier (2018). WICC 2018 (Workshop de Investigadores en Ciencias de la Computación). UNNE, Corrientes, Argentina. Abril de 2018. Libro de Actas XX Workshop de Investigadores en Ciencias de la Computación. pp1056-1060. ISBN 978-987-3619-27-4.

[2] - CERTunlp: CSIRT académico de la Universidad Nacional de La Plata: http://www.cert.unlp.edu.ar/

[3] - PKIGrid CERTUNLP: https://www.pkigrid.unlp.edu.ar

[4] - Equipo SYPER: https://ctftime.org/team/2003

[5] - Proyecto: F020 - Internet del Futuro. Ciudades Digitales, Inclusivas, Innovadoras y Sustentables, IoT, Ciberseguridad, Espacios de aprendizaje del Futuro. https://cyt.proyectos.unlp.edu.ar/projects/11-f020

[6] - Kasey Panetta. (2017). 5 Trends in Cybersecurity for 2017 and 2018. Diciembre de 2018, de Smarter with Gartner Sitio web: https://www.gartner.com/smarterwithgartner/5-trends-in-cybersecurity-for-2017-and-2018/

[7] - Anna L. Buczak, Member, IEEE, and Erhan Guven, Member, IEEE. (SECOND QUARTER 2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 18, 1153.