

## **PIP 2012 N° 11220110100468: Inlining sobre-la-marcha de monitores dinámicos de dependencias para flujo de información seguro**

**Integrantes:** Bonelli, Eduardo; Bavera, Francisco; Bello, Luciano; Pose, Alberto

**Resumen:** La creciente dependencia en la tecnología ha puesto en evidencia la criticidad del software que le da soporte: gobiernan aplicaciones bancarias, de salud, de transporte, etc. En consecuencia, el concepto de Software Seguro, otrora estudiado en dependencias militares y empresas aeroespaciales, ha pasado a ser analizado en dominios más generales. ¿Qué significa que un programa o sistema sea seguro? La complejidad inherente de los programas y la envergadura del software han dejado en claro que una definición precisa requiere que el concepto se delimite y especialice. Esta propuesta se interesa por la propiedad de seguridad llamada Secure Information Flow Analysis (IFA) en aplicaciones web basándose en técnicas dinámicas. IFA consiste en rastrear a través de un sistema informático el flujo de los datos. Asumiendo que el sistema se alimenta tanto de datos públicos como de datos privados, el análisis de flujo nos permite determinar si valores que son exhibidos en espacios públicos (impresos en pantalla, adosados a formularios web, enviados por la red, etc.) dependen, en alguna medida, de datos sensibles. En los últimos 10 años, el estudio de IFA se ha concentrado principalmente en generar teorías, técnicas y herramientas que permitan garantizar la ausencia de flujos inseguros en lenguajes como Java, ML, Ada, etc. Con el advenimiento de la Web también han comenzado a aparecer resultados que se enfocan sobre lenguajes de programación de aplicaciones web dado que dichas aplicaciones manipulan números de tarjeta de crédito, registros de salud y otros datos sensibles. Gran parte de la literatura que desarrolla estos temas insiste en obtener técnicas de análisis estáticas. Es decir, que no impongan costos en tiempo de ejecución. Sin embargo, hoy en día muchas de las razones (se requiere visión de todas las trazas, escasez de recursos en tiempo de ejecución, etc.) que respaldaban un tratamiento estático han perdido fuerza. IFA puede hacerse con información estática parcial o eventualmente nula, la memoria y tiempo de CPU es barata y abundante, y las técnicas dinámicas son más permisivas y permiten abordar estructuras dinámicas como los objetos. Proponemos considerar técnicas de IFA: \* utilizando un enfoque puramente dinámico, \* en el marco específico de aplicaciones web, y \* que sea escalable.