Conclusiones

Después de haber estudiado en profundidad el funcionamiento de sigMatch, indagar sobre las posibilidades que pueden ofrecer los adelantes en las nuevas tecnologías, conocer el funcionamiento de Snort a nivel de desarrollador e implementar una técnica de filtrado de tráfico en este IPS, muchas son las conclusiones que se pueden extraer.

sigMatch

En cuanto a sigMatch, se ha estudiado la implementación a tal nivel que se debieron corregir algunos aspectos de la *release* publicada junto al estudio oficial. También, se ha realizado una gran cantidad de pruebas –de las que la mayoría no fueron incluidas en el este documento para evitar escapar demasiado de los objetivos principales del proyecto– que han aportado importantes datos acerca del filtro.

Todo esto ha servido para conocer cada virtud y cada defecto de la propuesta de filtrado desarrollada por el equipo de Jignesh M. Patel. Se trata de una aplicación que realiza muy bien su cometido en condiciones favorables, pero que se vuelve tremendamente deficiente cuando no se dan todas unas determinadas circunstancias.

No obstante, después de un elaborado estudio se ha podido conocer qué factores son los que vuelven a este sistema tan deficiente. Por lo que conociendo la distribución del tipo de datos que circulan en una red y la base de firmas que se usará, se podría estimar si la integración del filtro produciría una mejora considerable. De este mismo estudio se conoce que para cualquier caso desfavorable, en el que se obtenga un decremento del rendimiento, se reduciría la eficiencia hasta llegar a un límite situado entre un 15% y 20% aproximadamente. Aún así, existirán soluciones para que en cualquier caso desfavorable el rendimiento no disminuya un ápice.

Todos estos factores hacen que el uso de sigMatch en Snort resulte especialmente ventajoso para redes internas, en las que el porcentaje de alertas sea muy bajo, lo que significará que la tasa de candidatos también lo será –sobre un 20%–, y por tanto se podrá conseguir una mejora de rendimiento importante.

Nuevas tecnologías

En este proyecto se ha abierto una puerta importante al aprovechamiento de las últimas capacidades ofrecidas por los nuevos procesadores. Este campo se consideró muy importante al comenzar el proyecto, puesto que muy pocas aplicaciones –entre las que no se incluye Snort– aprovechan los últimos avances de los procesadores más recientes en el mercado.

Se pensó en las librerías IPP de Intel, que proporcionaban funciones que aprovechaban al máximo el conjunto de instrucciones SSE (Streaming SIMD Extensions). Había funciones relacionadas con

la búsqueda de patrones en las librerías IPP. El único problema es que estas funciones estaban dedicadas a la búsqueda de patrones simple. El diseño realizado de un algoritmo de búsqueda multi-patrón basado en dichas funciones no obtuvo un buen rendimiento, por lo que este camino se descartó. No obstante, el conocimiento de la existencia de estas funciones permite desarrollar en un futuro otras implementaciones que puedan mejorar el rendimiento de Snort.

Snort

Por último, y no menos importante, se ha adquirido un gran conocimiento de Snort en general, pero sobre todo del motor de búsqueda de patrones (MPSE). De esta forma, si en un futuro se desea desarrollar para Snort cualquier implementación o modificación, resultará mucho más eficiente por el hecho de conocer muy bien el funcionamiento a nivel de código fuente.