Tecnológico de Costa Rica

Escuela de Ingeniería en Computación

Seguridad del Software - IC8071

Tarea 2 - Paper CVE

Estudiante:
Axel Alexander Chaves Reyes - 2021099588

Profesor:
Herson Esquivel Vargas

Semestre I

2024

Attack Dynamics: An Automatic Attack Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases

La investigación enviada propone un novedoso marco de trabajo el cual denominaron como *Attack Dynamics*, el cual plantea una generación automática de grafos de ataque en el sector de la ciberseguridad. Asimismo, este marco usa las bases de datos CAPEC, CWE y CVE para reconocer rutas de ataque de forma eficiente.

El objetivo principal de este sistema es brindar visualizaciones, integrarse con herramientas de optimización para poder reducir costes, ser usado como un instrumento de análisis para detectar intrusos potenciales para una variedad de configuraciones de red y ofrecer el servicio a usuarios de cualquier nivel de expertis para el modelado de amenazas con fines educativos.

Los primeros intentos por crear una herramienta de este tipo se datan en el año 1998, donde se propuso una herramienta de ataque semi-automatizado basado en grafos en ciertos archivos de configuración de redes.

De forma muy breve, el funcionamiento del sistema es el siguiente:

Primero, se recibirá un escenario de entrada, el cual entrará en un escenario de razonamiento de máquina, donde comenzará a buscar en su base de datos de CAPEC por una lista potencial de puntos de inicio.

Segundo, se buscará en las rutas de CAPEC para obtener una lista de rutas de ataque potenciales.

Tercero, el sistema calculará los datos dinámicos del atacante para así obtener las máscaras y vectores de ataque.

Cuarto, el sistema determinará la lista de rutas de ataque basado en los datos de CAPEC, lo cual generará un grafo de ataque con metadatos.

Quinto, luego de generar este grafo se enlistan una ruta de debilidades así como su lista de mitigaciones.

Sexto, al obtener la lista de mitigaciones, se realiza una optimización para encontrar un conjunto ideal de mitigaciones.

Finalmente, se crean un conjunto de visualizaciones CAPEC y CWE que muestran las debilidades de la entrada y sus patrones de ataque.

Por otra parte, algunas de las preguntas que realiza el sistema para realizar los pasos anteriores son: “¿Cómo ocurre el ataque?”, “¿Ocurre desde dentro o desde afuera?”, “¿A cuáles son los nodos a atacar?”, “¿Cuáles son los objetivos potenciales de ataque y cuáles nodos están allí?”.

Entre las conclusiones realizadas por el equipo de investigación destacan distintos puntos, por ejemplo, que es la primera herramienta que genera gráficos de ataque que utiliza definiciones de ataque CAPEC en lugar de comportamientos de ataque genéricos. Asimismo, el sistema ha logrado identificar patrones de ataque, debilidades asignadas y mitigaciones.

Por otra parte, la simplificación de la información obtenida del sistema es muy comprensible para los usuarios, lo cual también es un aporte importante. De este modo, dichos datos se pueden utilizar con propósitos educacionales durante el planeamiento y la

evaluación de la seguridad de la red y la configuración de la infraestructura, tanto a nivel de software como de hardware.

Como opinión, quiero destacar que me parece fundamental que existan herramientas automatizadas de detección de debilidades, dado que nuestro software actual es tan inseguro y propenso a vulnerabilidades que es bueno optimizar la carga de trabajo y agilizar el proceso de encontrar estrategias de mitigación.

Asimismo, considero que estas herramientas deberían tener un soporte activo, debido que, aunque se conocen muchos patrones de ataque y muchas debilidades, los atacantes encuentran nuevas formas de penetrar sistemas día con día; en el caso del sistema descrito en la investigación, las redes son sumamente frágiles y una debilidad puede significar un descontrol significativo en todo el entorno.

En síntesis, la automatización de procesos de detección de debilidades es una forma novedosa de manejar la seguridad de nuestro software, optimizando así las labores de los responsables y simplificando la detección en sus distintas etapas.