Análisis de Autor Referente en Seguridad de Redes

Elmer Ivan Yujra Condori

Ficha Técnica del Autor Referente

Autor Referente:	Wenke Lee
Índice h:	¿80 (Scopus)
Concepto Técnico:	Seguridad de Redes
Afiliación Principal:	Georgia Institute of Technology
Citas Totales:	¿40,000

Área Principal de Trabajo

Descripción General

Wenke Lee es reconocido internacionalmente como pionero en la aplicación de **machine learning y análisis de comportamiento** para la seguridad de redes. Su investigación se centra en desarrollar sistemas inteligentes que puedan detectar y mitigar amenazas de seguridad en tiempo real en infraestructuras de red.

Líneas de Investigación Principales

1. **Detección de Intrusos en Redes (NIDS)**
   - Desarrollo de sistemas basados en anomalías del tráfico de red
   - Análisis de flujos de datos para identificar patrones maliciosos
   - Detección de ataques DDoS y escaneo de puertos
2. **Análisis de Malware y Botnets**
   - Caracterización del comportamiento de malware en red
   - Detección de comunicaciones C&C (Command and Control)
   - Técnicas para desmantelamiento de botnets
3. **Seguridad en IoT y Redes Móviles**
   - Protección de dispositivos IoT conectados a redes
   - Análisis de seguridad en redes 5G y móviles
   - Detección de amenazas en entornos de red heterogéneos
4. **Machine Learning Aplicado a Seguridad**

- Algoritmos de clasificación para tráfico malicioso
- Aprendizaje automático para análisis forense de red
- Detección de amenazas avanzadas persistentes (APT)

Contribuciones Significativas a la Seguridad de Redes

- **Sistemas de Detección Basados en Comportamiento:** Desarrolló algunos de los primeros sistemas NIDS que utilizaban machine learning para identificar anomalías en el tráfico de red.
- **Análisis de Botnets:** Contribuyó significativamente a la comprensión de la infraestructura de botnets y desarrolló técnicas para su detección y desmantelamiento.
- **Seguridad Proactiva:** Promovió el enfoque de seguridad proactiva mediante el análisis continuo del comportamiento de la red, en lugar de dependencia exclusiva de firmas conocidas.
- **Herramientas de Código Abierto:** Varias de sus investigaciones han resultado en herramientas de seguridad de red que se han compartido con la comunidad académica y profesional.

Relación con el Concepto de Seguridad de Redes

El trabajo de Wenke Lee aborda directamente los pilares fundamentales de la seguridad de redes:

- **Confidencialidad:** Mediante detección de fugas de información y análisis de exfiltración de datos.
- **Integridad:** A través de la detección de modificaciones no autorizadas y alteraciones del tráfico.
- **Disponibilidad:** Con sistemas de protección contra ataques DDoS y otras amenazas que afectan la disponibilidad de servicios de red.

"La seguridad de redes moderna requiere enfoques inteligentes que puedan adaptarse a amenazas evolutivas."
- Línea de investigación de Wenke Lee