MALORI

MALware cOmmunication in cRitical Infrastructures

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2018	**Status**	abgeschlossen
Projektstart	01.01.2020	**Projektende**	30.06.2022
Zeitraum	2020 - 2022	**Projektlaufzeit**	30 Monate
Keywords	Malware; Critical Infrastructure; Communication Network; Anomaly Detection; Machine Learning		

Projektbeschreibung

Im Projekt MALORI werden neue Methoden für versteckte Kommunikation von Malicious Software (Malware) in kritischen Infrastrukturen untersucht mit dem Ziel Verfahren zu entwickeln um diese versteckte Kommunikation zu erkennen und einzudämmen. Diese untersuchten Techniken betreffen vor allem den Bereich der Verschlüsselungsverfahren und Netzwerk–Steganografie (Covert Channels, Subliminal Channels). Dabei werden schwerpunktmäßig auf Machine Learning aufbauende Erkennungsverfahren angewendet, um ein vom Normalzustand abweichendes Kommunikations- oder Systemverhalten festzustellen, mit einem klaren Fokus auf den Möglichkeiten und Herausforderungen, die sich durch den Einsatz von Machine Learning im sicherheitskritischen Umfeld von MALORI ergeben.
Ausgehend von einer strukturierten und detaillierten Analyse der Kommunikation von Malware, einschließlich theoretischer Modelle verborgener Kommunikation entsprechend dem Stand der Technik, werden vorhandene und zukünftige Bedrohungsszenarien als Use Cases ausgearbeitet. Anhand entsprechender Szenarien werden neue Verfahren zur Erkennung und Eingrenzung von Malware in kritischen Infrastrukturen entwickelt. Das Design von Protokollen wird analysiert und Metriken entwickelt, um das Gefährdungspotential neuer Netzwerkprotokolle zu beurteilen und zu minimieren. Die Robustheit der Erkennungsverfahren gegen aktive Manipulationsversuche (Adversarial Machine Learning) wird untersucht und spielt eine entscheidende Rolle bei der Bewertung der Methoden.
Weiterführend wird ein gesamtheitlicher (holistischer) Erkennungsansatz verfolgt, der Daten unterschiedlicher Quellen und Verfahren für eine umfassendere Erkennung zusammenführt. Ziel dieses Ansatzes ist die Zuverlässigkeit der Erkennung mittels Einbeziehung verschiedener Analyseergebnisse, zusätzlichem Kontext und alternativer Perspektiven zu verbessern und auf diese Weise den Anteil fehlerhafter Alarme zu senken. Die wichtigsten Szenarien werden abschließend in einer IoT Security Laborumgebung mit realen Protokollen und Datenströmen aufgebaut und die Angriffs- und Erkennungsverfahren unter realitätsnahen Bedingungen evaluiert.
Die Ergebnisse des Projekts sind vorrangig für kritische Infrastrukturen anwendbar, können aber auch für andere Netze und Anwendungsfälle angepasst werden, wie z.B. weitere Internet-of-Things Szenarien oder klassische IT-Netze. Ziel ist es, die versteckte Kommunikation durch gezielte Auswahl von Protokollen zu erschweren, um die Angriffsfläche zu reduzieren sowie gleichzeitig aktive Maßnahmen anzubieten, um verdeckte Kommunikation frühzeitig zu erkennen und einzugrenzen.

Abstract

The project MALORI investigates new techniques for hidden malware communication in critical infrastructures such as encryption and network steganography (covert and subliminal channels) and explores suitable methods to detect and contain hidden malware communication. In terms of detection methods, MALORI sets particular emphasis on the investigation of opportunities and challenges of machine learning based algorithms. As part of a structured in-depth analysis of malware, including theoretical models for hidden communication according to the state of art, existing and potential future attack possibilities for specific critical infrastructures are defined as use cases. Based on those scenarios new detection and containment methods are developed. Recommendations are formulated to assess and minimize new threats by protocols. A holistic detection approach aims at combining data from various sources for a more comprehensive evaluation and consideration of context to improve classification and detection performance. The developed methods will be also evaluated with regard to their robustness against active manipulation, extending the research in the field of adversarial machine learning.
The most relevant scenarios will be implemented in a security IoT lab environment based on real components, protocols and data to evaluate the developed attack and detection methods in a realistic environment. The project results are targeted towards communication in critical infrastructures, but may be applied and adjusted also to other network domains, like other Internet of Things scenarios or classical enterprise IT networks.
The project aims at reducing the possibilities of hidden communication by a thoughtfully guided selection of protocols and cryptographic methods and at providing methods to detect suspicious communication patterns and to contain hidden malware communication.

Projektkoordinator

- Technische Universität Wien

Projektpartner

- Universität Wien
- IKARUS Security Software GmbH
- illwerke vkw AG
- AIT Austrian Institute of Technology GmbH
- WIENER NETZE GmbH
- Bundesministerium für Inneres