Anwenderforum für Fernmeldetechnik, AFCEA Computer, Elektronik und Automatisierung

AFCEA Bonn e.V. Studienpreis 2017

Kernthesen der Arbeit

Titel der Arbeit:	**Konzeption und prototypische Implementierung eines Current-Based IDS**
Tag der Einreichung:	01. August 2016
Hochschule:	Universität der Bundeswehr München
Name des Verfassers:	Teo Kühn, Marcel Odenwald
Betreuender Professor:	Prof. Dr. Gabi Dreo Rodosek

*Kurze Beschreibung (1 Seite !) der **Kernthesen**.*

Was ist die Quintessenz der Arbeit?

Industrielle Steuerungsanlagen stehen zunehmend im Visier von Angreifern. Beispiele wie die durch Cyberangriffe verursachten Stromausfälle in der Ukraine im Dezember 2015 sowie Dezember 2016 unterstreichen die tatsächliche Gefährdung. Die resultierende Notwendigkeit einer besseren Absicherung industrieller Steuerungssysteme zeigt in der Praxis jedoch zahlreiche Herausforderungen. Traditionelle Verfahren wie Systeme zur Einbruchserkennung lassen sich nur bedingt, stellenweise auch gar nicht nachträglich integrieren, da zu den Charakteristika von Steuerungsanlagen oft 24/7-Betrieb, Echtzeitfähigkeit und die operative Forderung, auch unter Maximallast gemäß Spezifikation zu arbeiten, gehören.

Die vorliegende Masterarbeit adressiert die Limitierungen bisheriger Detektionssysteme sowie die eingeschränkten Nachrüstmöglichkeiten verschiedener Systeme und Anlagen. Um die bisherigen Limitierungen zu überwinden, wird ein Konzept für ein neues, verhaltensbasiertes System zur Einbruchs- und Innentätererkennung auf Basis von manipulationssicheren Stromverbrauchswerten vorgestellt, prototypisch implementiert und evaluiert. Die vorgestellte Lösung erzielt hohe Detektions- und geringe Fehlalarmraten. Sie basiert auf der Nutzung kostengünstiger Einplatinenrechner und kann auch zur Überwachung und Absicherung eigentlich nicht-nachrüstbarer und proprietärer Systeme genutzt werden. Dabei werden die Kernthesen der Arbeit untersucht, dass einerseits die Charakteristik des Stromverbrauchs eines Systems genutzt werden kann, um Anomalien wie Angriffe oder Manipulationen zu detektieren, andererseits ein auf Stromverbrauch basiertes Detektionsverfahren sich mittels kostengünstiger Einplatinenrechner realisieren lässt. Weiterer Schwerpunkt der Arbeit ist die praktische Anwendbarkeit der Ergebnisse.

Nach einem Abriss des Stands von Wissenschaft und Technik auf dem Gebiet strombasierter Sicherheitsverfahren, welcher in einer vorhergehenden Arbeit umfassend analysiert wurde, wird ein Detektionskonzept auf Basis der Messung von Stromverbrauch entwickelt. Hierbei werden umfassende Untersuchungen angestellt, um eine Meßbasis zu finden, welche die Anforderungen an eine spätere Nutzbarkeit in realen Steuerungssystemen erfüllt. Die nachfolgende Implementierung des Prototypen beinhaltet daher über das eigentliche Meßverfahren hinaus eine komfortable Nutzerschnittstelle und eine Erweiterung der verbreiteten Webschnittstelle Snorby. Während der umfassenden Evaluation des Prototypen werden sowohl zahlreiche Angriffe ausgewertet, als auch Detektionsmöglichkeiten im Falle einer Kompromittierung oder Manipulation des Systems untersucht. In diesem Rahmen werden auch typische Strommuster identifiziert. Abschließend diskutiert die Arbeit praktische Einsatzmöglichkeit und Grenzen des vorgestellten Prototypen.

Das in der Masterarbeit vorgestellte und evaluierte Detektionskonzept stellt einen wichtigen Beitrag zur Verbesserung der Sicherheit industrieller Steuerungssysteme und Anlagen dar. Die Bedeutung der Ergebnisse wird durch eine zugehörige Veröffentlichung bei der Konferenz IEEE Privacy Security & Trust 2016, sowie beim kommenden 15. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik, unterstrichen. Derzeit wird der Prototyp weiterentwickelt und es wurden Gespräche mit Industriepartnern initiiert, um eine umfassende Erprobung des Verfahrens in einer realen Steuerungsumgebung durchzuführen.