TU Clausthal

Bachelor-, Master- und Doktorandenseminar
des Instituts für Informatik

Analyse des Datenverkehrs in Zugbeeinflussungssystemen zur vorbereitenden Datenverdichtung für die Intrusion Detection

Pascal Schimkus, TU Clausthal

Zugbeeinflussungssysteme überwachen das Einhalten von Signalen, Geschwindigkeitsbeschränkungen und Sicherheitsabständen im Bahnbetrieb. Der zu Diagnosezwecken aufgezeichnete Datenverkehr ist ohne Kenntnis der genauen Spezifikation für den Menschen unverständlich. Deswegen wurde durch die Siemens AG ein Decoder entwickelt, welcher diese Daten decodiert und in einer lesbaren Form bereitstellt. Die bisher eingesetzte Aufzeichnungsmethode verwendet ein proprietäres Dateiformat und bietet keine Möglichkeit der Erkennung von Netzwerkangriffen (Intrusion Detection). Deswegen findet ein Umstieg bei der Aufzeichnungshardware statt. Die neue Aufzeichnungsmethode verwendet das standardisierte PCAPNG-Dateiformat und bietet die Möglichkeit der tiefergehenden Analyse mit Hilfe von Intrusion Detection Systemen. Im Rahmen dieser Arbeit wurde der Decoder aufgerüstet. Zum einen, um das PCAPNG-Dateiformat der neuen Aufzeichnungsmethode zu unterstützen. Zum anderen, um die Datenverdichtung als Vorbereitung für die Intrusion Detection zu ermöglichen und somit die zu analysierende Datenmenge vorab zu reduzieren.

Mittwoch, den 21.09.2016, 10 Uhr s.t. im Besprechungsraum 106, IfI, Julius-Albert-Straße 4

Technische Universität Clausthal • Institut für Informatik • Julius-Albert-Straße 4 • 38678 Clausthal-Zellerfeld
Tel +49.(0)5323.72.7100 • Fax +49.(0)5323.72.7139 • http://www.in.tu-clausthal.de • info@in.tu-clausthal.de