Elektrotechnik & Informationstechnik (2018) 135/3: 249. https://doi.org/10.1007/s00502-018-0619-2

Cyber-Physical Systems – Security

T. Zseby

Online publiziert am 5. Juni 2018

Univ.-Prof. Dipl.-Ing. Dr.-Ing. Tanja Zseby

Liebe Leserin, lieber Leser,

Cyber-Physical Systems (CPS) verbinden software- und computertechnische Komponenten mit realen physischen Systemen. Sie sind die Basis für eine Vielzahl von Anwendungen in sehr unterschiedlichen technischen Forschungsgebieten. Beispiele sind Smart Grids, E-Health-Anwendungen, neue Entwicklungen im Transportwesen und intelligente Produktionssysteme (Industrie 4.0).

Intelligente Systeme erfordern zunehmend eine Vernetzung, um Informationen von verteilten Teilsystemen auszutauschen und damit eine Einschätzung der aktuellen Lage erstellen zu können. Diese „Situational Awareness" bildet die Grundlage für Entscheidungen im System. Mit der Vernetzung entstehen jedoch oft neue Angriffsmöglichkeiten. Cyber-Physical Systems sind zudem oft Bestandteil kritischer Infrastrukturen und deshalb sehr attraktive Angriffsziele.

Die Erforschung von Sicherheitskonzepten für Cyber-Physical Systems ist daher von hoher Bedeutung. Der hohe Anreiz und die ständige Weiterentwicklung der Angriffstechniken führen dazu, dass auch die Sicherheitsmaßnahmen stets angepasst werden müssen. Die Sicherheit bleibt also ein spannendes Forschungsgebiet.

Die vorliegende e&i-Ausgabe stellt verschiedene Forschungsarbeiten auf dem Gebiet der Cyber-Physical Systems mit dem Schwerpunkt Sicherheit vor. Die ersten drei Beiträge befassen sich dabei mit Smart Grids. Es werden neuartige Angriffsmöglichkeiten aufgezeigt und Konzepte vorgestellt, um sich den neuen Anforderungen in Smart Grid-Umgebungen stellen zu können.

Der Beitrag „Botnets causing blackouts: how coordinated load attacks can destabilize the power grid" zeigt auf eindrucksvolle Weise, welche Auswirkungen koordinierte Angriffe mit kompromittierten Geräten im Internet auf Prozesse in Elektrizitätsnetzen haben können. Die Autoren simulieren dabei Szenarien, in denen eine große Anzahl von Verbrauchern, die mit dem Internet verbunden sind (z.B. IoT-Geräte), übernommen werden und als Teil eines Botnetzes gesteuert werden können. Durch die koordinierte Manipulation des Energieverbrauchs einer hohen Anzahl solcher Geräte lassen sich verschiedene Lastangriffe auf das Elektrizitätsnetz realisieren.

Der Beitrag „Industrial IoT für Smart Grid-Anwendungen im Feld" adressiert den Bedarf nach flexiblen Lösungen, um den hohen Anforderungen in komplexen Internet of Things-Installationen im industriellen Umfeld gerecht werden zu können. In dem Beitrag wird dazu eine IoT-Plattform vorgestellt. Als Anwendungsbeispiel wird die Realisierung einer intelligenten Ortsnetzstation mit Hilfe der IoT-Plattform gezeigt. Das Szenario soll im Rahmen eines Forschungsprojektes im Smart Grid Testbed der ASCR (Aspern Smart City Research) als Machbarkeitsstudie umgesetzt werden.

Der Beitrag „Malware propagation in smart grid monocultures" befasst sich mit der Ausbreitung von verschiedenen Malware-Typen in Smart Grids. Mit einer Simulation wird gezeigt, wie sich Schadsoftware durch die Ausnutzung neuer Sicherheitslücken (zero-day exploits) in einer Smart-Grid-Kommunikationsinfrastruktur ausbreiten kann. Der häufige Einsatz von homogenen Installationen mit identischer Hardware und Software (z.B. Smart Meter eines Herstellers) führt zu hohen Ausbreitungsgeschwindigkeiten und einer schnellen Infektion des gesamten Netzes.

Zwei weitere Beiträge befassen sich mit Sicherheitsherausforderungen von Cyber-Physical Production Systems (CPPS). In beiden Beiträgen werden Systeme vorgestellt, die sich selbst dynamisch an veränderte Umgebungsbedingungen anpassen können.

Der Beitrag „SAMBA – an architecture for adaptive cognitive control of distributed Cyber-Physical Production Systems based on its self-awareness" stellt eine Architektur zur automatisierten Überwachung und Koordination von verteilten intelligenten Systemen vor. In der SAMBA (Self-Aware health Monitoring and Bio-inspired coordination for distributed Automation systems)-Architektur lernen autonome kooperierende Objekte (ACOs) ihre lokale Umgebung kennen und tauschen sich mit anderen ACOs aus, um ein verteiltes intelligentes Produktionssystem zu überwachen und ihre Aktionen miteinander abzustimmen. Dabei können sie sich zu dynamischen Clustern zusammenschließen, um gemeinsam Probleme zu bewältigen.

Der Beitrag „Countering targeted cyber-physical attacks using anomaly detection in self-adaptive Industry 4.0 Systems" stellt ein Konzept zur adaptiven Überwachung von intelligenten Produktionssystemen vor. Dabei werden Verfahren der Anomalieerkennung verwendet, um Abweichungen vom Normalverhalten festzustellen, die durch Fehler oder gezielte Angriffe auf das System verursacht werden können. Als Basis für selbstadaptive Systeme wird der MAPE-K Cycle (Monitor-Analyze-Plan-Execute over a shared Knowledge) aus dem Autonomic Computing verwendet, um die benötigten Funktionen dynamisch an die aktuelle Situation anzupassen. Die Funktionsweise des Konzepts wird anhand eines simulierten industriellen Prozesses demonstriert.

Ich bedanke mich bei allen Autorinnen und Autoren für die spannenden Beiträge, bei den Gutachterinnen und Gutachtern für die kritische Begutachtung der Beiträge und beim Redaktionsteam für die tatkräftige Unterstützung bei der Erstellung des Heftes.

Ich hoffe, das Heft trägt dazu bei, ein stärkeres Bewusstsein für Sicherheitsrisiken zu schaffen, aber auch Lösungsmöglichkeiten aufzuzeigen und wünsche Ihnen viel Freude beim Lesen!

Zseby, Tanja, Institute of Telecommunications, Technische Universität Wien, Gußhausstraße 25-25a, 1040 Wien, Österreich (E-Mail: tanja.zseby@tuwien.ac.at)