Prof. Dr. Theo Ungerer
Lehrstuhl f"ur Systemnahe Informatik
und Kommunikationssysteme
Universit"at Augsburg

Universität
Augsburg
University

Seminar Cyber-Physical Systems

Security Considerations for Cyber-Physical Systems

Maximilian Ammann
Bachelor Informatik

Datum des Vortrags

Kurzfassung

Eine kurze Zusammenfassung der Ausarbeitung mit 10-12 Zeilen Text.

Inhaltsverzeichnis

1 Einführung

Betriebsblindheit beschreibt einen Zustand in dem man sich Aufgrund weitreichendem Prozesswissen nicht über Fehler oder Mängel bewusst ist [GK16, S. 202]. Ist dieser Zustand einmal erreicht, ist es schwer ihm wieder zu entfliehen und beispielsweise Probleme in der Sicherheit[1] eines Systems zu erkennen. Deshalb soll es ein Ziel der Arbeit sein zu Motivieren sich mehr mit Sicherheit auseinander zu setzen und keiner Blindheit zu verfallen. Besonders in Cyber-Physical Systems ist es wichtig sich mit Sicherheit zu befassen, da diese eine erhöhte Angriffsfläche für Angriffe bereitstellen.

Cyber-Physical Systems sind meist eingebettete echtzeit Systeme, welche eine hohe Verfügbarkeit, Robustheit, Widerstandsfähigkeit und Berechenbarkeit aufweisen müssen. Die physische Welt macht hohe Verfügbarkeit allerdings oft schwierig da sie alles andere als berechenbar ist [Lee08]; [Sha+08]. Einsatzorte für diese Systeme könnten intelligente Stromnetze, symbiotische Sensornetzwerke für die Agrarwirtschaft und Katastrophenabwehr, medizinische oder assistierende Geräte, intelligente Verkehrssteuerung und intelligente Gebäude sein [Raj+10]. In all diesen Beispielen spielt ein hohes Maß an Vertrauen eine Rolle [Sha+08]. Zudem unterliegt man konzeptionell bedingt auch einigen Restriktionen wie beispielsweise die Bindung an eine Batterie oder eine leichte Bauweise [Yan+17]. Es existiert also ein Unterschied in den Anforderungen an Cyber-Physical Systems und klassischen Systemen, wie Anwendungsservern oder Heimcomputern.

In Kapitel 2.1 wird zunächst der Begriff Sicherheit speziell für Cyber-Physical Systems definiert. In den Kapiteln 2.2, 2.3, 2.4 werden mögliche Angriffsszenarien beleuchtet um im Kapitel 2.5 adäquate Gegenmaßnahmen darzustellen. Zuletzt soll im Kapitel 3 auf vergangene Vorfälle im Bereich der Security eingegangen werden.

[1] Sicherheit wird in dieser Arbeit (falls nicht anders hingewiesen) äquivalent zu dem englischen Begriff „security“ verwendet

2 Aspekte eines Angriffes

2.1 Security Definition für Cyber-Physical Systems

2.2 Cyber-Physical Systems als Angriffsziel

2.3 Angriffszenarien

2.3.1 Klassische Szenarien

2.3.2 Denial-of-Service Angriff

2.3.3 Man-in-the-Middle Angriff

2.3.4 Täuschungsangriff (Deception)

2.3.5 Lauschangriff (Eavesdropping)

2.3.6 Compromised-Key Angriff

2.4 Angreifergruppen

2.5 Gegenmaßnahmen

2.5.1 Modellierung von Cyber-Physical Systems

Noch nicht sicher.

Um hierbei dem Standard an Sicherheit zu genügen schlägt Lee sogar vor eine neue Grundlage für diese Systeme zu etablieren [Lee08].

2.5.2 Physische Maßnahmen

2.5.3 Organisatorische Maßnahmen

2.5.4 Präventive Maßnahmen

2.5.5 Detektion und Wiederherstellung (Detection and Recovery)

2.5.6 Widerstandsfähigkeit (Resilience)

2.5.7 Abschreckung (Deterrence)

3 Evaluation aktueller Maßnahmen

4 Literatur

[BG11] Radhakisan Baheti und Helen Gill. „Cyber-physical systems“. In: *The Impact of Control Technology*. Hrsg. von T. Samad und A. M. Annaswamy. IEEE Control Systems Society, 2011, S. 161–166.

[Bra14] Jim Brodie Brazell. „The Need for a Transdisciplinary Approach to Security of Cyber Physical Infrastructure“. In: *Applied Cyber-Physical Systems*. Hrsg. von Sang C. Suh u. a. New York, NY: Springer New York, 2014, S. 5–14. ISBN: 978-1-4614-7336-7.

[Car+09] Alvaro Cardenas u. a. „Challenges for securing cyber physical systems“. In: *Workshop on future directions in cyber-physical systems security*. Newark, NJ, USA, Juli 2009.

[CAS08] Alvaro A. Cardenas, Saurabh Amin und Shankar Sastry. „Secure Control: Towards Survivable Cyber-Physical Systems“. In: *The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, Juni 2008. DOI: 10.1109/icdcs.workshops.2008.40.

[Fru+18] M. Frustaci u. a. „Evaluating Critical Security Issues of the IoT World: Present and Future Challenges“. In: *IEEE Internet of Things Journal* 5.4 (Aug. 2018), S. 2483–2495. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2767291.

[GK16] Dieter Gollmann und Marina Krotofil. „Cyber-Physical Systems Security“. In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Springer Berlin Heidelberg, 2016, S. 195–204. ISBN: 978-3-662-49301-4. DOI: 10.1007/978-3-662-49301-4_14.

[Hum+17] Abdulmalik Humayed u. a. „Cyber-Physical Systems Security - A Survey“. In: *IEEE Internet of Things Journal* 4.6 (2017), S. 1802–1831. DOI: 10.1109/JIOT.2017.2703172.

[KC14] Dan Kruger und John N. Carbone. „Radically Simplifying Cyber Security“. In: *Applied Cyber-Physical Systems*. Hrsg. von Sang C. Suh u. a. New York, NY: Springer New York, 2014, S. 51–61. ISBN: 978-1-4614-7336-7.

[Kou+18] Xenofon Koutsoukos u. a. „SURE: A Modeling and Simulation Integration Platform for Evaluation of Secure and Resilient Cyber–Physical Systems“. In: *Proceedings of the IEEE* 106.1 (Jan. 2018), S. 93–112. DOI: 10.1109/jproc.2017.2731741.

[KP14] Md E. Karim und Vir V. Phoha. „Cyber-physical Systems Security“. In: *Applied Cyber-Physical Systems*. Hrsg. von Sang C. Suh u. a. New York, NY: Springer New York, 2014, S. 75–83. ISBN: 978-1-4614-7336-7.

[Lan11] Ralph Langner. „Stuxnet: Dissecting a Cyberwarfare Weapon“. In: *IEEE Security & Privacy* 9.3 (2011), S. 49–51. DOI: 10.1109/MSP.2011.67.

[Lee08] Edward A. Lee. „Cyber Physical Systems: Design Challenges“. In: *11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*. IEEE, Mai 2008. DOI: 10.1109/isorc.2008.25.

[Lin+17] J. Lin u. a. „A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications“. In: *IEEE Internet of Things Journal* 4.5 (Okt. 2017), S. 1125–1142. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2683200.

[Lu+14] Tianbo Lu u. a. „An Analysis of Cyber Physical System Security Theories“. In: *7th International Conference on Security Technology*. IEEE, Dez. 2014. DOI: 10.1109/sectech.2014.12.

[Raj+10] Ragunathan (Raj) Rajkumar u. a. „Cyber-physical Systems: The Next Computing Revolution“. In: *Proceedings of the 47th Design Automation Conference*. DAC '10. Anaheim, California: ACM, 2010, S. 731–736. ISBN: 978-1-4503-0002-5. DOI: 10.1145/1837274.1837461.

[SFJ17] Houbing Song, Glenn A. Fink und Sabina Jeschke. „Overview of Security and Privacy in Cyber-Physical Systems“. In: *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*. IEEE, 2017. ISBN: 9781119226079. DOI: 10.1002/9781119226079.ch1.

[Sha+08] Lui Sha u. a. „Cyber-Physical Systems: A New Frontier“. In: *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*. Hrsg. von Mukesh Singhal u. a. Taichung, Taiwan: IEEE Computer Society, Juni 2008, S. 1–9. DOI: 10.1109/SUTC.2008.85.

[Sin+16] J. Singh u. a. „Twenty Security Considerations for Cloud-Supported Internet of Things“. In: *IEEE Internet of Things Journal* 3.3 (Juni 2016), S. 269–284. ISSN: 2327-4662. DOI: 10.1109/JIOT.2015.2460333.

[SJT08] Karen Scarfone, Wayne Jansen und Miles Tracy. „Guide to general server security“. In: *NIST Special Publication* 800 (2008), S. 123. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf.

[Wan+10] Eric Ke Wang u. a. „Security Issues and Challenges for Cyber Physical System“. In: *IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*. IEEE, Dez. 2010. DOI: 10.1109/greencom-cpscom.2010.36.

[Yan+17] Y. Yang u. a. „A Survey on Security and Privacy Issues in Internet-of-Things“. In: *IEEE Internet of Things Journal* 4.5 (Okt. 2017), S. 1250–1258. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2694844.