Christian Doppler Labor für die Verbesserung von Sicherheit und Qualität in Produktionssystemen

(Technologietransfer)

Projektverantwortliche	**Univ.-Prof. Edgar Weippl (edgar.weippl@univie.ac.at)**, Dr. Andreas Ekelhart, Dr.Johanna Ullrich
Projektbeschreibung	In großen Industrieanlagen werden Prozesse zunehmend von Software gesteuert. Diese cyber-physikalischen Produktionssysteme können - wie jede andere Software auch - manipuliert werden. Das Besondere an diesen Produktionssystemen ist, dass sie über Jahrzehnte in Betrieb sind und immer wieder umgebaut werden. Dass mangelnde Security im Sinne von 'Schutz' auch mangelnde Sicherheit für die Firma und die Mitarbeiter*innen bedeutet, muss daher klar kommuniziert werden. Ganz grundsätzlich soll den Industriepartner*innen vermittelt werden, dass heutzutage jede Firma eine Software-Firma ist und man daher auch die entsprechenden Sicherheitsstandards einhalten sollte. Wir versuchen, mögliche Angriffspunkte und geeignete Gegenmaßnahmen für den gesamten Lebenszyklus dieser Produktionssysteme zu betrachten. Die Arbeit des CD-Labors basiert auf anwendungsorientierter Grundlagenforschung. Je nach Größe der Industriepartner*innen (KMU oder GU) werden 40-50% der Förderung von den Firmenpartner*innen, die Mitglieder bei der CD-Gesellschaft sind, und 50-60% vom BMDW und der Nationalstiftung für Forschung, Technologie und Entwicklung getragen.
Schlagworte/Keywords	IoT-Security, Industrie 4.0, Software Quality
Zentrale Ziele der Third-Mission-Aktivität	Die Mission unseres CD-Labors besteht in der Erforschung und Entwicklung von Konzepten zur Verbesserung von Sicherheit und Qualität im Bereich großer Industrieanlagen (Stichwort Industrie 4.0). Das Ziel unserer Forschungsgruppe für Security & Privacy ist die Erforschung von Schwachstellen und Entwicklung von Sicherheitsstrategien für Software-gesteuerte Prozesse. Ein wichtiges Augenmerk liegt hier auf der Mitplanung und Absicherung von Sicherheit und Qualität der Systeme bereits in ihrer Entwicklungsphase, damit Angreifer*innen Schwachstellen nicht gleich von Beginn an miteinbauen können.

Universitätsexterne Kooperations-partner*innen	SMS group GmbH STIWA Automation GmbH EUVIC Software GmbH Ing. Punzenberger COPA-DATA GmbH
Kooperations-partner*innen aus dem Wissenschafts- bzw. Forschungsbereich	TU Wien Otto-von-Guericke-Universität Magdeburg

Fakultät	Fakultät für Informatik / FG Security & Privacy
Projektlaufzeit	01.01.2018 (Start an der TU Wien) 01.04.2020 (Übertragung an die UW) - 31.12.2024
Finanzierung	Christian Doppler Forschungsgesellschaft

Forschungsbasierung	Edgar Weippl forscht seit Jahren im Gebiet der IIoT-Security mit zahlreichen Publikationen und wir organisieren auch 2 Dagstuhl-Seminare zu diesem Thema.
Gesellschaftliche/Wirtschaftliche Relevanz	Prinzipiell soll vermittelt werden, dass heutzutage jede Firma eine Software-Firma ist und man daher auch die entsprechenden Sicherheitsstandards einhalten sollte. Und zwar nicht nur im laufenden Betrieb von Anlagen, sondern eben auch schon bei der Konzeption und Entwicklung derartiger Systeme.
Einbindung der Third-Mission-Aktivität in die Lehre	Nein

Ergebnisse/Wirkung (Impact)	Wir steigern die Awareness, dass Securityüberlegungen schon beim Design und Engineering von Industrieanlagen berücksichtigt werden müssen. Unsere Forschungsergebnisse zeigen Industrieanlagenhersteller*innen Methoden, wie Sicherheitsrisken bewertet werden können und welche Gegenmaßnahmen schon während der Entwicklungsphase sinnvoll sind.
Transferaspekt der Aktivität	Das CD-Labor hat mehrere Industriepartner*innen. Abgesehen von den direkten Firmenpartner*innen profitiert die Allgemeinheit durch unsere Outreach-Aktivitäten, die die Forschungsergebnisse einfach zugänglich machen.

Nachhaltigkeit & Zukunftsorientierung	Das Forschungsgebiet ist langfristig wichtig, weil Industrieanlagen eine lange Lebensdauer haben und über mehrere Jahrzehnte betrieben werden. Bisherige Forschung fokussiert auf die Absicherung „bestehender" Anlagen; unsere Forschung sichert die Entwicklung neuer Anlagen.
Überprüfung der Zielerreichung der Third-Mission-Aktivität	Die wissenschaftliche Qualitätssicherung wird durch Evaluierungen der CDG vorgenommen. Die 2-Jahres-Evaluierung haben wir bereits sehr gut absolviert; die nächste Evaluierung ist die 5-Jahres-Evaluierung. Der wirtschaftliche Nutzen lässt sich leicht an den Partner*innenzahlungen messen. Nur wenn die Partner*innenunternehmen einen Nutzen sehen, werden sie die 50-Co-Finanzierung leisten. In-Kind-Leistungen sind bei CDLs nicht möglich.
Maßnahmen, um die Transferaktivität längerfristig durchzuführen bzw. auszuweiten	Wir planen nach der hoffentlich erfolgreichen 5-Jahres-Evaluierung FFG-Anträge (v.a. Bridge) zu stellen. Außerdem ist die Einreichung eines weiteren CD-Labors geplant.
Sichtbarmachung	Website, Publikationen, Medien
Homepage/Publikationen	• https://www.sqi.at • https://sec.cs.univie.ac.at/cdl-sqi/ • Matthias Eckhart, Andreas Ekelhart, and Edgar Weippl. Automated security risk identication using automationml-based engineering data. IEEE Transactions on Dependable and Secure Computing, 2020. • Matthias Wenzl, Georg Merzdovnik, Johanna Ullrich, and Edgar Weippl. From hack to elaborate technique | a survey on binary rewriting. ACM Computing Surveys (CSUR), 52(3):49:1{49:37, June 2019. http://doi.acm.org/10.1145/3316415. • Philipp Schindler, Aljosha Judmayer, Markus Hittmeir, Nicholas Stifter, and Edgar Weippl. Randrunner: Distributed randomness from trapdoor vdfs with strong uniqueness. accepted for publication at NDSS 2021, Preprint Cryptology ePrint Archive, Report 2020/942, 2021. https://eprint.iacr.org/2020/942