



a-i3/BSI-Symposium 2020

# IT-Sicherheit in IoT, Blockchain und KI

25./26. November 2020

Programm

in Kooperation mit



## Über das Symposium

Fragen der IT-Sicherheit sind brisanter denn je zuvor: Angriffe auf vernetzte Systeme der Industrie 4.0 können – wie der jüngste Fall eines Hackerangriffs auf eine Rettungsinfrastruktur zeigt – eine reale Bedrohung für Menschenleben darstellen. Doch welche Vorkehrungen sind von wem zu treffen, welche sind technisch möglich?

Die Arbeitsgruppe Identitätsschutz im Internet e.V. (a-i3) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) widmen sich auf ihrem 15. interdisziplinären Symposium diesen und anderen Fragen der IT-Sicherheit im Internet der Dinge, in Blockchains und in KI-Systemen.

Die Veranstaltung richtet sich an Entscheidungsträger von Verwaltungsbehörden, Datenschutzbeauftragte in Organisationen und Unternehmen aus den Gebieten IT-Sicherheit, Softwareentwicklung und E-Commerce sowie an Juristen in Justiz, Unternehmen und Verbänden und an spezialisierte Rechtsanwälte sowie Aufsichts- und Datenschutzbehörden.

## Aus den Themen

- Tod durch Hacking – Verantwortlichkeit für Schäden durch Hacking
- Private Blockchains – was unterscheidet sie von Bitcoin & Co?
- Post-Quantum Kryptographie (und Blockchain)
- Rechtliche Aspekte blockchainbasierter Zahlungsabwicklung
- Fuzzing – Maschinelles Lernen von Programmierfehlern

Infos und Anmeldung  
[www.a-i3.org](http://www.a-i3.org)

## Mittwoch, 25. November 2020

- 10.00 Begrüßung und Eröffnung der Tagung  
Prof. Dr. Georg Borges, a-i3 / N.N., BSI
- 10.10 Einführung: Aktuelle Herausforderungen  
in der IT-Sicherheit  
Prof. Dr. Georg Borges, UoS / Prof. Dr. Jörg Schwenk, RUB

### Themenbereich 1

#### Vertraulichkeit und Datenschutz in Blockchain-Anwendungen

Moderation: Prof. Dr. Georg Borges, UoS

- 10.30 Einführung
- 10.35 Private Blockchains – was unterscheidet sie  
von Bitcoin & Co?  
Prof. Dr. Jörg Schwenk, RUB
- 11.20 Projekt 374 – Eine Markt- und Sicherheitsanalyse  
des Blockchain-Ökosystems im Auftrag des BSI  
Dr. Jochen Rill, FZI
- 12.05 Vertraulichkeit in Blockchains  
– Konzepte in Hyperledger Fabric  
Marcus Brinkmann, RUB
- 12.50 Mittagspause
- 14.00 Datenschutzrechtliche Aspekte in der  
Blockchain-Technologie in der Industrie 4.0  
Jonas Baumann, UoS
- 14.40 Pause

### Themenbereich 2

#### IT-Sicherheit in vernetzten Infrastrukturen

Moderation: Prof. Dr. Jörg Schwenk, RUB

- 14.50 Einführung
- 15.00 Lagebild IT-Sicherheit – eine aktuelle Übersicht  
Marco Krambrich, BSI
- 15.45 Angriffe auf TLS – wo stehen wir heute?  
Prof. Dr. Juraj Somorovsky, Uni Paderborn
- 16.20 Tod durch Hacking – Verantwortlichkeit für  
Schäden durch Hacking  
Jun.-Prof. Dr. Dominik Brodowski, UoS
- 17.00 Ende des Tagesprogramms

## Donnerstag, 26. November 2020

### Themenbereich 1 und 2

#### Grundfragen der IT-Sicherheit

Moderation: Prof. Dr. Jörg Schwenk, RUB

- 10.00 Post-Quantum Kryptographie (und Blockchain)  
Dr. Manfred Lochter, BSI

### Themenbereich 3

#### Automatisierte Zahlungssysteme

Moderation: RA Jörg Heidrich

- 10.45 Einführung
- 10.50 Automatisiertes Zahlen mit Paypal, GooglePay und Co.  
Prof. Dr. Jörg Schwenk / Dr. Christian Mainka, RUB
- 11.30 Automatisierter Werttransfer auf Basis von sogenannten  
'smart contracts' – Effiziente Zahlung auf der Basis  
von DLT-Technologie?  
Dr. Alexander Poddey, Bosch
- 12.15 Rechtliche Aspekte blockchainbasierter  
Zahlungsabwicklung  
Dr. Nick Wittek, Jones Day
- 12.55 Mittagspause

### Themenbereich 4

#### IT-Sicherheit und KI

Moderation: Prof. Dr. Jörg Schwenk, RUB

- 14.00 Einführung
- 14.05 Rechtliche Grundlagen des Testens und Auditierens  
von KI-Anwendungen  
Prof. Dr. Georg Borges, UoS
- 14.45 Technische Normen für KI und Sicherheit  
– Wegweiser durch den Normenschwungel  
Dr. Rasmus Adler, Fraunhofer IESE
- 15.25 Pause
- 15.35 Fuzzing – Maschinelles Lernen von Programmierfehlern  
Robert Merget, RUB
- 16.15 State Learning – Maschinell erzeugte Abstraktion  
von Programmcode  
Dr. Dennis Felsch, RUB
- 16.55 Schlusswort  
Prof. Dr. Georg Borges, UoS / Prof. Dr. Jörg Schwenk, RUB
- 17.00 Ende der Tagung

## Referenten

### • Dr. Rasmus Adler

Programm Manager für autonome Systeme am Fraunhofer Institut für Experimentelles Software Engineering (IESE) in Kaiserslautern, 14 Jahre Erfahrung im Bereich Safety in unterschiedlichen Anwendungsdomänen, aktiv in verschiedenen nationalen und internationalen Normungs- und Standardisierungsaktivitäten bezüglich KI und autonome Systeme.

### • Jonas Baumann, LL.M. (UJ)

1. Staatsexamen 2017; LL.M. (University of Johannesburg) 2018; seit 2019 wiss. Mitarbeiter am Lehrstuhl von Prof. Dr. Georg Borges, Universität des Saarlandes; seit 2019 Research Associate am Research Centre for Private International Law in Emerging Countries, University of Johannesburg.

### • Prof. Dr. Georg Borges

Inhaber des Lehrstuhls für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie und geschäftsführender Direktor des Instituts für Rechtsinformatik an der Universität des Saarlandes; Sprecher des Vorstands der a-i3; Mitglied des Verwaltungsrats der Stiftung Datenschutz der Bundesrepublik.

### • Jun.-Prof. Dr. Dominik Brodowski, LL.M. (UPenn)

Juniorprofessor für Strafrecht und Strafprozessrecht an der Universität des Saarlandes. Forschungsschwerpunkte Digitalisierung, Europäisierung & Internationalisierung sowie Grundlagen und Grenzgebiete des Strafrechts.

### • Dr. Dennis Felsch

Postdoktorand am Lehrstuhl für Netz- und Datensicherheit der Ruhr-Universität Bochum. Fachgebiete sind die Sicherheit von Cloud-Plattformen, kollaborativen Web-Anwendungen und Netzwerkprotokollen. Seine Einreichung beim 7. Deutschen IT-Sicherheitspreis 2018 gelangte in den Kreis der Finalisten.

### • Marco Krambrich

Seit 2017 als Referent in der Abteilung "Operative Cybersicherheit" im BSI tätig. Dort insbesondere befasst mit allen Aspekten der Lagebildfeststellung im Bereich "Analysen und Prognosen".

### • Dr. Manfred Lochter

Seit 1994 als Mathematiker beim Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt und hat unter anderem die Einführung der ECC-Kryptografie begleitet. Er beschäftigt sich zur Zeit vornehmlich mit dem Wechsel zu quantensicheren kryptografischen Lösungen, Evaluierungskriterien für QKD-Devices und mit Anwendungen der Blockchain-Technologie. Mitautor der Analyse "Blockchain sicher gestalten. Konzepte. Anforderungen. Bewertungen." Leiter der Studie "Sicherheitsuntersuchung ausgewählter Blockchain-Anwendungen."

### • Dr. Alexander Poddey

Promovierte im Jahr 2008 in theoretischer Physik an der TU Clausthal und begann anschließend als Experte für Machine Learning bei Bosch. Im strategischen Vorausentwicklungsprojekt „Economy of Things“ (EoT) bei Bosch Research leitet er die Forschung in den Themen digitale Sozioökonomie, Kryptologie und künstliche Intelligenz.

### • Dr. Jochen Rill

Dr. Jochen Rill leitet das Themenfeld Kryptographie am Kompetenzzentrum IT-Sicherheit des FZI Forschungszentrums Informatik. Forscht im Bereich der Entwicklung und Analyse von kryptographischen Verfahren.

### • Prof. Dr. Jörg Schwenk

Inhaber des Lehrstuhls für Netz- und Datensicherheit, Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum und Vorstandsmitglied der a-i3; Autor zweier Bücher zu Kryptographie und Internetsicherheit sowie Referent auf (inter-)nationalen Konferenzen.

### • Prof. Dr. Juraj Somorovsky

Juraj Somorovsky ist Professor für Systemischerheit an der Universität Paderborn und Mitgründer der Hackmanit GmbH. Er ist der Hauptentwickler des Analysewerkzeugs TLS-Attacker und Autor zahlreicher Angriffe auf TLS. Dazu gehören u.a. die Angriffe DROWN oder ROBOT, die jeweils mit dem Pwnie Award für den besten kryptographischen Angriff ausgezeichnet wurden.

### • Dr. Nick Wittek

Partner bei Jones Day, laut JUVE eine der Speerspitzen des Beratermarktes für Blockchain-Projekte im Finanzsektor. Sein aktueller Arbeitsschwerpunkt liegt auf der Verwendung von Distributed Ledger Technologie (DLT) und Blockchain für Finanzmarktprodukte und Finanzmarktinfrastrukturen. Nick Wittek wird von JUVE für strukturierte Finanztransaktionen und von Chambers für FinTech Beratung empfohlen.