Hannes Hartenstein ist seit April 2017 Bevollmächtigter für die Informationsverarbeitung und -versorgung des KIT (siehe https://www.kit.edu/cio/).

Er studierte Mathematik an der Universität Freiburg. Seine Promotion erlangte er 1998 am dortigen Institut für Informatik. Anschließend arbeitete er im Bereich „Mobile Networks" in der Forschungsabteilung von NEC Europe Ltd. in Heidelberg. Seit 2003 ist er Informatikprofessor an der ehemaligen Universität Karlsruhe, dem heutigen KIT.

Am Institut für Telematik leitet er die Professur Dezentrale Systeme und Netzdienste. Seine Forschungs- und Lehrschwerpunkte liegen in den Themenfeldern Sicherheit und Leistungsfähigkeit vernetzter Systeme. Er ist Principial Investigator im BMBF-geförderten nationalen Kompetenzzentrum für Cybersicherheit KASTEL. Darüber hinaus ist er u. a. Mitglied der ständigen Kommission „Digitale Infrastrukturen" der Hochschulrektorenkonferenz, des Ausschusses für Recht und Sicherheit des Deutschen Forschungsnetzes und des Sprecherkreises des Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen.

ÜBERBLICK UND ALLGEMEINES

Unter dem Begriff „Dezentrale Systeme und Netzdienste" werden verteilte und vernetzte technische Systeme verstanden, die sich über mehr als eine administrative Domäne erstrecken und deren Funktionieren somit an mehreren oder vielen „Parteien" hängt. Im Fokus stehen derzeit:

- Blockchains, Konsensverfahren und Peer-to-Peer-Netze
- Network Security Monitoring
- Sichere und privatsphärengerechte Datenverarbeitung in bedingt vertrauenswürdigen Umgebungen.

Zudem wurden viele Jahre auf den Gebieten der Mobilität (vernetzte Fahrzeuge, „Car-to-X Communication"), der dezentralen Energiesysteme und des föderativen Identitätsmanagement Forschungsbeiträge geleistet.

Die Forschungsgruppe entwirft und analysiert Verfahren insbesondere mit den Schwerpunkten:

- Security: explizite Vertrauensmodellierung und „Tunable Security"
- Performance: Leistungsbewertung durch ereignisdiskrete Modellierung und Simulation (insb. auch parallele Simulation)
- Deployability: die Einsatzfähigkeit ist Teil von Anforderung und Bewertung

In der Lehre werden diese Themen insbesondere durch die Vorlesungen „IT-Sicherheitsmanagement für vernetzte Systeme" und „Access Control Systems: Foundations and Practice" mit Übungen, Praktika und Seminaren vertreten. Erstmalig im WS 2018/19 wurde die Vorlesung „Ausgewählte Themen für das Informatik-Lehramt" als Ringvorlesung mehrerer Dozentinnen und Dozenten durchgeführt.

ERGEBNISSE UND ERFOLGE

Die Sicherheit der Netzwerkschicht von Blockchains wurde intensiv analysiert: Erkenntnisse über Angriffsmöglichkeiten konnten systematisiert werden, sodass ein tiefgehendes Verständnis potentieller Schwachstellen möglich ist. Zudem wurden Designoptionen und Zielkonflikte aufgezeigt, die für die Entwicklung von Blockchains relevant sind. Insbesondere in Bezug auf die Bitcoin-Blockchain wurde gezeigt, dass es durch geschicktes Ausnutzen von Bitcoin-Funktionen möglich ist, Informationen über die Topologie des Peer-to-Peer-Netzwerkes zu gewinnen. Da diese helfen können, gezielte Angriffe auszuführen, wurden Möglichkeiten bewertet, wie man solche Angriffe verhindern kann.

Hinsichtlich Anwendungen auf dezentralen Konsenssystemen wurde die Tauglichkeit von Blockchains zur Sicherung der Integrität von Binaries untersucht. Dabei wurde insbesondere darauf Wert gelegt, dass die Integrität von Binaries auch widerrufen werden kann. Dies ist beispielsweise dann relevant, wenn nach der Veröffentlichung bekannt wird, dass das Binary kompromittiert wurde oder kritische Schwachstellen enthält. Zudem wurde ein Konzept „Atomic Information Disclosure" entwickelt, mit dem mehrere sich gegenseitig misstrauende Parteien die Veröffentlichung von individuell gehaltenen Informationen koordinieren können.

Am 18. und 19. September 2018 fand der erste europäische Bro Workshop, durchgeführt von der Forschungsgruppe „Dezentrale Systeme und Netzdienste" mit Unterstützung des International Computer Science Institute (ICSI), Berkekely, am KIT statt. Bro (heute Zeek) ist ein Open Source Network Security Monitoring Tool und wurde 1995 von Vern Paxson im Lawrence Berkeley National Laboratory (LBL) entwickelt. Seither schreibt die Software eine Erfolgsgeschichte sowohl als Grundlage wissenschaftlicher Veröffentlichungen als auch im produktiven Einsatz in Forschungs- und Unternehmensnetzen. Dieses Werkzeug dient der Forschungsgruppe als Basis für Untersuchungen zu leistungsfähigem Threat Intelligence Matching unter Einsatz aktueller Filterverfahren.

AUSGEWÄHLTE PUBLIKATIONEN

A. Degitz, H. Hartenstein: PATCONFDB: Design and Evaluation of Access Pattern Confidentiality-Preserving Indexes. In: *Transactions on Data Privacy*. S. 81-109, 2018.

T. Neudecker, H. Hartenstein: Network Layer Aspects of Permissionless Blockchains. In: *IEEE Communications Surveys & Tutorials*. S. 1-21, 2018.

J. Grashöfer, F. Jacob, H. Hartenstein: Towards Application of Cuckoo Filters in Network Security Monitoring, In: *14th International Conference on Network and Service Management (CNSM)*. Rom, Italien, 2018.

M. Grundmann, T. Neudecker, H. Hartenstein: Exploiting Transaction Accumulation and Double Spends for Topology Inference in Bitcoin. In: *Financial Cryptography and Data Security*. Curaçao, 2018.

O. Stengele, H. Hartenstein: Atomic Information Disclosure of Off-Chained Computations Using Threshold Encryption. In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology - ESORICS 2018 International Workshops, DPM 2018 and CBT 2018*. Barcelona, Spanien, 2018.

MITARBEITERINNEN UND MITARBEITER

Verwaltungspersonal

Astrid Hopprich

Wissenschaftliches Personal

Jan Grashöfer
Matthias Grundmann
Marc Leinweber
Till Neudecker
Oliver Stengele

Technisches Personal

Christian Dreher