Leopoldina
Nationale Akademie
der Wissenschaften

Curriculum Vitae Prof. Dr. Christof Paar

Name: **Christof Paar**
Geboren: **18. Juli 1963**

Forschungsschwerpunkte: angewandte Kryptografie, Hardware-Sicherheit, Sicherheit für das Internet der Dinge, menschliche Aspekte in der IT-Sicherheit, Sicherheit in eingebetteten Systemen

Christof Paar ist Informationswissenschaftler und beschäftigt sich mit den Ingenieuraspekten der modernen Cybersicherheit. Seine Forschungen reichen von Schutzmaßnahmen gegen bösartige Manipulation von Computer-Hardware über die Absicherung von Geräten, die zum Internet der Dinge (IoT) gehören (bspw. Smartphones, Autos oder medizinische Implantate) bis hin zum Verstehen von Kognitionsvorgängen bei Angreifern.

Akademischer und beruflicher Werdegang

seit 2019	Direktor am Max-Planck-Institut für Cybersicherheit und Schutz der Privatsphäre, Bochum
2014 - 2016	Forschungsprofessor, University of Massachusetts Amherst, USA
2008 - 2009	Forschungsprofessor an der University of Massachusetts Amherst, USA
2001 - 2019	Professor für embedded Security, Ruhr-Universität Bochum
1995 - 2001	Assistant und später Associate Professor (tenured), Worcester Polytechnic Institute, Massachusetts, USA
1994	Promotion auf dem Gebiet der Computerarithmetik für endliche Körper, Institut für Experimentelle Mathematik, Universität Duisburg-Essen
1991 - 1994	Wissenschaftlicher Mitarbeiter, Institut für Experimentelle Mathematik, Universität Duisburg-Essen
1989 - 1991	Studium der Elektrotechnik, Universität Siegen

1984 - 1988	Studium der Nachrichtentechnik, Fachhochschule Köln (jetzt Technische Hochschule Köln)
1979 - 1983	Ausbildung zum Fernmeldemechaniker

Funktionen in wissenschaftlichen Gesellschaften und Gremien

2011 - 2017	IACR Board of Directors, International Association for Cryptologic Research
2004 - 2007	Geschäftsführender Direktor, Horst-Görtz-Institut für IT-Sicherheit (erneut 2010 - 2012 und 2016 - 2017)
2004	Gründer, ESCRYPT GmbH - Embedded Security (inzwischen Teil von Bosch)
1999	Mitbegründer, Konferenz CHES - Cryptographic Hardware and Embedded Systems

Projektkoordination, Mitgliedschaft in Verbundprojekten

2019 - 2026	Sprecher DFG-Exzellenzcluster „EXC 2092: Cyber-Sicherheit im Zeitalter großskaliger Angreifer (CASA)“ (mit Th. Holz und E. Kiltz)
2016	ERC Advanced Grant auf dem Gebiet der Hardware-Sicherheit
2016 - 2020	Sprecher des Forschungskollegs „SecHuman - Sicherheit für Menschen im Cyberspace”
2012 - 2017	Sprecher des DFG-Graduiertenkollegs „GRK 1817: Neue Herausforderungen für die Kryptografie in ubiquitären Rechnerwelten“

Auszeichnungen und verliehene Mitgliedschaften

seit 2019	Mitglied der Nationalen Akademie der Wissenschaften Leopoldina
2017	IACR Fellow (International Association for Cryptological Research)
2012	Innovationspreis des Landes Nordrhein-Westfalen
2011	IEEE Fellow (Institute of Electrical and Electronics Engineers)
2010	Deutscher IT-Sicherheitspreis (mit G. Leander und A. Poschmann)
1998	National Science Foundation CAREER Award

Forschungsschwerpunkte

Christof Paar ist Informationswissenschaftler und beschäftigt sich mit den Ingenieuraspekten der modernen Cybersicherheit. Seine Forschungen reichen von Schutzmaßnahmen gegen bösartige Manipulation von Computer-Hardware über die Absicherung von Geräten, die zum

Internet der Dinge (IoT) gehören (bspw. Smartphones, Autos oder medizinische Implantate) bis hin zum Verstehen von Kognitionsvorgängen bei Angreifern.

Unsere moderne Lebenswelt ist bestimmt von vernetzten Geräten. Wir sind von einer Vielzahl von cyber-physikalischen Systemen (CPS) umgeben, wie z. B. elektronischen Ticket- und Bezahlsystemen, Mautsystemen oder Smart Homes. Damit ist die IT-Sicherheit zu einer zentralen gesellschaftlichen Frage geworden. Christof Paar erforscht Sicherheitslücken in diesen Systemen und entwickelt neue Sicherheitslösungen.

Ein Arbeitsschwerpunkt ist der Schutz vor Hardware-Trojanern. Diese bösartigen Manipulationen auf der untersten Hardware-Ebene werden insbesondere von staatlichen Angreifern vorgenommen. Sie sind eine ernsthafte Gefahr für die digitale Gesellschaft. Das zeigen auch Diskussionen über die Vertrauenswürdigkeit von Hardware ausländischer Hersteller. Christof Paar identifiziert Angriffspotenziale und entwickelt Gegenmaßnahmen.

Des Weiteren beschäftigt sich Paar mit Methoden der so genannten Physical-layer Security. Hierbei werden Eigenschaften des Übertragungskanals genutzt, um neue Sicherheitsprimitive umzusetzen, bspw. die digitale Charakterisierung physischer Umgebungen. Damit lassen sich neue Sicherheitslösungen realisieren, wie die sichere Überwachung von Server-Räumen oder Bankautomaten. Solche Techniken sind eine deutliche Erweiterung der bisher rein algorithmischen Datensicherheit.

Christof Paar analysiert in seiner Forschung auch kognitive Prozesse von Angreifern. Das Ziel ist es, dass Regeln für Systeme abgeleitet werden, die eine hohe Resistenz gegenüber Cyberangriffen haben. Hier setzt Paar auf eine enge Kooperation zwischen Sicherheitsingenieuren und Kognitionspsychologen.