

A U S H A N G

FREIE UNIVERSITÄT BERLIN

Fachbereich Mathematik und Informatik

Promotionsbüro, Arnimallee 14, 14195 Berlin

D I S P U T A T I O N

Montag, 20. September 2021, 10:00 Uhr

Ort: Seminarraum 051* und [WebEx](#)

(Takustr.9, 14195 Berlin)

(* Begrenzte Teilnehmerzahl unter Kontrolle der 3G Regeln – geimpft, genesen, getestet)

Disputation über die Doktorarbeit von

Herrn Michael Witt

Thema der Dissertation:

Generation of Secure Runtime Environments for Untrusted Applications Through Machine Code Analysis

Thema der Disputation:

Möglichkeiten und Limitierungen der Überwachung von Systemaufrufen in verschiedenen Betriebssystemen und Prozessorarchitekturen.

Die Arbeit wurde unter der Betreuung von **Prof. Dr. M. Margraf** durchgeführt.

Abstract: Moderne Betriebssysteme sind Multi-User-Systeme, welche privilegierte und nicht-privilegierte User sowie deren Aktionen voneinander trennen. Diese Trennung und deren Durchsetzung wird ebenfalls durch die Betriebssysteme realisiert. Zusätzlich dazu existieren Techniken und Verfahren auf Ebene der CPU, welche die Betriebssysteme hierbei unterstützen und versuchen, auf Hardware-Ebene den Zugriff auf sensible Daten oder die Ausführung von beschränkten Aktionen zu erschweren bzw. zu verhindern.

Die Schnittstelle zur Ausführung von Systemaufrufen (engl. System Call Interface) ist eine wohldefinierte Schnittstelle. Diese ermöglicht es nicht-privilegierten Anwendungen mit dem Betriebssystem zu interagieren um auf geschützte Ressourcen zuzugreifen. Da diese Ressourcen häufig ebenfalls das Ziel von Angriffen sind ist die Überwachung dieser Schnittstelle von großem Interesse. Dieser Vortrag stellt die unterschiedlichen Konzepte der Umsetzung von Systemaufrufen zwischen verschiedenen Betriebssystemen vor. Außerdem werden Techniken auf CPU-Ebene beschrieben, die das Betriebssystemen bei der sicheren, effizienten und effektiven Abarbeitung von Systemaufrufen unterstützen. Des Weiteren werden unterschiedliche Angriffs-Szenarien vorgestellt, deren Schäden mit Hilfe einer effektiven Überwachung der System Call Schnittstelle verhindert werden können und welche Limitierungen dieser Ansatz nach aktuellem Stand der Forschung besitzt.

Die Disputation besteht aus dem o. g. Vortrag, danach der Vorstellung der Dissertation einschließlich jeweils anschließenden Aussprachen.

Interessierte werden hiermit herzlich eingeladen

Der Vorsitzende der Promotionskommission
Prof. Dr. M. Margraf