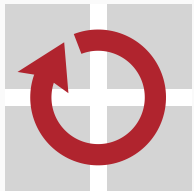
Ausgewählte Kapitel der Systemsoftware

21. November 2022

Rüdiger Kapitza



Lehrstuhl für Verteilte Systeme
und Betriebssysteme

Friedrich-Alexander-Universität
Technische Fakultät

Organisatorisches

Überblick

Rüdiger Kapitza

(Raum 0.048)

ruediger.kapitza@cs.fau.de

Arne Vogel

(Raum 0.041)

vogel@cs.fau.de

- **Termin: TBD**
- **Webseite:** `https://sys.cs.fau.de/lehre/ws22/akss`
- **Mailingliste** an alle Teilnehmer & Betreuer `akss@lists.cs.fau.de`
  - **Anmeldung**: `lists3.cs.fau.de`
- **Mailingliste** an Betreuer `akss-betreuer@lists.cs.fau.de`

Praktische Übung

- Papier: Flicker[1]
- Rezension
  - Kurze Zusammenfassung (max. 5 Sätze)
  - Antworten auf die folgenden Fragen, nicht länger als 10 Sätze
    - Erscheint die Struktur des Artikels sinnvoll?
    - Ist der Beitrag verständlich? Bzw. welche Dinge sind schwer zu erfassen oder unzureichend erklärt?
    - Erscheinen die Ergebnisse plausibel?
    - Gibt es ersichtliche offene Punkte bzw. Schwachstellen?
  - Als PDF bis einschließlich 04.11.2022 an vogel@cs.fau.de
    - Dabei enthält die PDF euren Namen!
- Besprechung in Präsenz in der Woche des 07.11.2022

[1] Jonathan M. McCune et al. „Flicker: an execution infrastructure for tcb minimization“. In: **Proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems 2008**. Eurosys '08. https://doi.org/10.1145/1352592.1352625. New York, NY, USA: Association for Computing Machinery, Apr. 2008, S. 315–328.

Praktische Übung

- Vortrag[2]
- Anschließende Diskussion:
  - Inhalt des Vortrags
  - Aufbau der Präsentation
  - Präsentationsstil
- In Präsenz in der Woche des 14.11.2022

[2] Ines Messadi et al. „SplitBFT: Improving Byzantine Fault Tolerance Safety Using Trusted Compartments“. In: **Proceedings of the 23rd ACM/IFIP International Middleware Conference**. Middleware '22. https://doi.org/10.1145/3528535.3531516. New York, NY, USA: Association for Computing Machinery, Nov. 2022, S. 56–68.

Einarbeitung

- Eigenständiges Bearbeiten eines Themas
- Literaturrecherche: Vorgegebene Papiere als Ausgangsbasis
- Abgabe eines Exposés: **roter Faden**
  - Max. eine Seite!
  - Stichpunktartig: Inhalt der Kapitel der Ausarbeitung
  - Liste der Quellen die zusätzlich aus der Literaturrecherche gekommen sind
  - Abgabe bis (spätestens) zum **21.11.**2022

Ausarbeitung

- Erstellen einer Ausarbeitung (6 Seiten)
- ACM Standard Proceedings Template (ACM SIG style)
- Sprache: Deutsch oder Englisch

The Name of the Title is Hope

Ben Trovato*
G.K.M. Tobin*
trovato@corporation.com
webmaster@marysville-ohio.com
Institute for Clarity in Documentation
Dublin, Ohio, USA

Lars Thørväld
The Thørväld Group
Hekla, Iceland
larst@affiliation.org

Valerie Béranger
Inria Paris-Rocquencourt
Rocquencourt, France

Aparna Patel
Rajiv Gandhi University
Doimukh, Arunachal Pradesh, India

Huifen Chan
Tsinghua University
Haidian Qu, Beijing Shi, China

Charles Palmer
Palmer Research Laboratories
San Antonio, Texas, USA
cpalmer@prl.com

John Smith
The Thørväld Group
Hekla, Iceland
jsmith@affiliation.org

Julius P. Kumquat
The Kumquat Consortium
New York, USA
jpkumquat@consortium.net

ABSTRACT

A clear and well-documented LaTeX document is presented as an article formatted for publication by ACM in a conference proceedings or journal publication. Based on the "acmart" document class, this article presents and explains many of the common variations, as well as many of the formatting elements an author may use in the preparation of the documentation of their work.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

datasets, neural networks, gaze detection, text tagging

ACM Reference Format:

Ben Trovato, G.K.M. Tobin, Lars Thørväld, Valerie Béranger, Aparna Patel, Huifen Chan, Charles Palmer, John Smith, and Julius P. Kumquat. 2018. The Name of the Title is Hope. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX).* ACM, New York, NY, USA, 6 pages. https://doi.org/XXXXXXX.XXXXXXX

*Both authors contributed equally to this research.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
Conference acronym 'XX, June 03–05, 2018, Woodstock, NY
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

ACM's consolidated article template, introduced in 2017, provides a consistent LaTeX style for use across ACM publications, and incorporates accessibility and metadata-extraction functionality necessary for future Digital Library endeavors. Numerous ACM and SIG-specific LaTeX templates have been examined, and their unique features incorporated into this single new template.

If you are new to publishing with ACM, this document is a valuable guide to the process of preparing your work for publication. If you have published with ACM before, this document provides insight and instruction into more recent changes to the article template.

The "acmart" document class can be used to prepare articles for any ACM publication — conference or journal, and for any stage of publication, from review to final "camera-ready" copy, to the author's own version, with very few changes to the source.

2 TEMPLATE OVERVIEW

As noted in the introduction, the "acmart" document class can be used to prepare many different kinds of documentation — a double-blind initial submission of a full-length technical paper, a two-page SIGGRAPH Emerging Technologies abstract, a "camera-ready" journal article, a SIGCHI Extended Abstract, and more — all by selecting the appropriate *template style* and *template parameters*.

This document will explain the major features of the document class. For further information, the *LaTeX User's Guide* is available from https://www.acm.org/publications/proceedings-template.

2.1 Template Styles

The primary parameter given to the "acmart" document class is the *template style* which corresponds to the kind of publication or SIG publishing the work. This parameter is enclosed in square brackets and is a part of the `documentclass` command:

```
\documentclass[STYLE]{acmart}
```

- **Keine** reine Nacherzählung/Übersetzung
- Direkte Übernahme von Abbildungen vermeiden
- Aufgreifen und Vertiefen einzelner Aspekte
- Herausarbeiten eigener Fragestellung
- Eigene Literaturrecherche

Vortrag

- Foliensatz zur Ausarbeitung
- i4-Beamertemplate (`i4neo`)
- Sprache: Deutsch oder Englisch
- Vortrag im Rahmen des Seminars
  - min. 20-minütiger (besser 25-minütiger) Vortrag
  - 10-minütige Diskussion zum Vortrag

Semesterplan

27.10. Organisation, Einführung und Themenvergabe
07.11. Praktische Übung: Lesen & Diskutieren von Papieren
14.11. Praktische Übung: Vortragsdiskussion
21.11. Abgabe Exposé (kein Präsenztermin)

- *Aus* = Abgabe vollständige Version der Ausarbeitung
- *Fol* = Abgabe vollständige Version der Folien
- *Dry* = Abgabe finale Version der Ausarbeitung + Folien und Probevortrag
- *Prä* = Präsentation + (anonyme) Rezension

12.12	19.12	09.01	16.01	23.01	30.01	06.02
$Aus_{1,2}$	$Fol_{1,2}$	$Dry_{1,2}$	$Prä_{1,2}$			
	Aus_3	Fol_3	Dry_3	$Prä_3$		
		Aus_4	Fol_4	Dry_4	$Prä_4$	
			Aus_5	Fol_5	Dry_5	$Prä_5$

Zusätzliche Informationen

Arbeitsmittel

- Verwendung von Git empfohlen
  $\rightarrow$ https://gitlab.cs.fau.de/
- Abgabe der Ausarbeitung/Folien per Git (oder E-Mail)

Zusätzliche Informationen

Arbeitsmittel

- Verwendung von Git empfohlen
  $\rightarrow$ https://gitlab.cs.fau.de/
- Abgabe der Ausarbeitung/Folien per Git (oder E-Mail)

Organisation

- Beim Seminar gilt **Anwesenheitspflicht:**
  Bei Abwesenheit bitte (per E-Mail) Bescheid geben
- **Technikcheck** rechtzeitig vor der Präsentation
- Veröffentlichung der (finalen) Folien und Ausarbeitung auf der Seminarwebseite
  (Falls nicht gewünscht, bitte Bescheid geben)

Themen

Hardware Erweiterungen

Intel Software Guard Extensions[3]: feingranulare Form der vertrauenswürdigen Ausführung

- Welcher Schutzmechanismus wird angeboten?
- Wie kann ich von außen den Zustand der Anwendung überprüfen?
- Wie sieht der Wechsel in und aus der sicheren Umgebung aus?
- (Wie) Können Geheimnisse dauerhaft Gespeichert werden?
- Welche zusätzliche Dienste gibt es?
- Wie entwickelt man eine Anwendung die Intel SGX verwendet?

[3] **Intel® Software Guard Extensions**. en. https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html.

Hardware Erweiterungen

AMD SEV SNP[4] & Intel TDX[5]: vertrauenswürdigen Ausführung auf der Ebene von virtuellen Maschinen

- Welcher Schutzmechanismus wird angeboten?
- Wie kann ich von außen den Zustand der Anwendung überprüfen?
- Wie sieht der Wechsel in und aus der sicheren Umgebung aus?
- (Wie) Können Geheimnisse dauerhaft Gespeichert werden?
- Welche zusätzliche Dienste gibt es?
- Wie entwickelt man eine Anwendung die AMD SEV SNP oder Intel TDX verwendet?

[4] David Kaplan. „AMD SEV-SNP: Strengthening VM Isolation with Integrity Protection and More“. en. In: (), S. 20.

[5] **Intel® Trust Domain Extensions**. en. https://www.intel.com/content/www/us/en/developer/articles/technical/intel-trust-domain-extensions.html.

Hardware Erweiterungen

Keystone[6]: vertrauenswürdige Ausführungsumgebungen auf Basis von RISC-V

- Welcher Schutzmechanismus wird angeboten?
- Wie kann ich von außen den Zustand der Anwendung überprüfen?
- Wie sieht der Wechsel in und aus der sicheren Umgebung aus?
- (Wie) Können Geheimnisse dauerhaft Gespeichert werden?
- Welche zusätzliche Dienste gibt es?
- Wie entwickelt man eine Anwendung die Keystone verwendet?

[6] Dayeol Lee et al. „Keystone: an open framework for architecting trusted execution environments“. In: **Proceedings of the Fifteenth European Conference on Computer Systems**. EuroSys '20. https://doi.org/10.1145/3342195.3387532. New York, NY, USA: Association for Computing Machinery, Apr. 2020, S. 1–16.

ARM CCA[7]: Ein neues Modell des Vertrauens auf der ARM Architektur

- Welcher Schutzmechanismus wird angeboten?
- Wie kann ich von außen den Zustand der Anwendung überprüfen?
- Wie sieht der Wechsel in und aus der sicheren Umgebung aus?
- (Wie) Können Geheimnisse dauerhaft Gespeichert werden?
- Welche zusätzliche Dienste gibt es?
- Wie entwickelt man eine Anwendung die ARM CCA verwendet?

[7] **Arm Confidential Compute Architecture**. en. https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture.

IBM Protected Execution Facility (PEF)[8]: Ergänzung zur vertrauenswürdigen Ausführung für die POWER9 Architektur

- Welcher Schutzmechanismus wird angeboten?
- Wie kann ich von außen den Zustand der Anwendung überprüfen?
- Wie sieht der Wechsel in und aus der sicheren Umgebung aus?
- (Wie) Können Geheimnisse dauerhaft Gespeichert werden?
- Welche zusätzliche Dienste gibt es?
- Wie entwickelt man eine Anwendung die IBM PEF verwendet?

[8] Nicolae Paladi. **Confidential Computing on IBM Protected Execution Facility**. en-GB. https://www.canarybit.eu/2021/paper-review-confidential-computing-for-openpower/. Mai 2021.

Scone[9] & Gramine[10]: Systeme die basierend auf Intel SGX ganze Anwendungen absichern

- Auf welcher Grundlage wird die Anwendung abgesichert?
- Ob und wie wird die zugrunde liegenden Hardware Erweiterung der Anwendung bereitgestellt?
- Welche Limitierungen haben die Ansätze?

[9] Sergei Arnautov et al. „{SCONE}: Secure Linux Containers with Intel {SGX}“. en. In: https://www.usenix.org/conference/osdi16/technical-sessions/presentation/arnautov. 2016, S. 689–703.

[10] Chia-Che Tsai, Donald E. Porter und Mona Vij. „{Graphene-SGX}: A Practical Library {OS} for Unmodified Applications on {SGX}“. en. In: https://www.usenix.org/conference/atc17/technical-sessions/presentation/tsai. 2017, S. 645–658.

Ryoan[11] & AccTEE[12]

- Was ist die Motivation für doppelseitige Sandboxen?
- Was ist das Angreifermodel?
- Welche Technologien werden für die Sandbox der Anwendung verwendet?

[11] Tyler Hunt et al. „Ryoan: A Distributed Sandbox for Untrusted Computation on Secret Data“. en. In: https://www.usenix.org/conference/osdi16/technical-sessions/presentation/hunt. 2016, S. 533–549.

[12] David Goltzsche et al. „AccTEE: A WebAssembly-based Two-way Sandbox for Trusted Resource Accounting“. In: **Proceedings of the 20th International Middleware Conference**. Middleware '19. https://doi.org/10.1145/3361525.3361541. New York, NY, USA: Association for Computing Machinery, Dez. 2019, S. 123–135.

Glamdring[13] & Panoply[14]: Schwierigkeiten bei der teilautomatisierter Partitionierung

- Was ist die Motivation der teilautomatisierten Partitionierung
- Was ist die TCB?
- Welche Probleme werden von den Papieren identifiziert?

[13] Joshua Lind et al. „Glamdring: Automatic Application Partitioning for Intel {SGX}“. en. In: https://www.usenix.org/conference/atc17/technical-sessions/presentation/lind. 2017, S. 285–298.

[14] Shweta Shinde et al. „Panoply: Low-TCB Linux Applications with SGX Enclaves“. en. In: **Proceedings 2017 Network and Distributed System Security Symposium**. https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/panoply-low-tcb-linux-applications-sgx-enclaves/. San Diego, CA: Internet Society, 2017.

EActor[15] & SplitBFT[16]

- Welche Vorteile bieten mehrere vertrauenswürdigen Ausführungskontexte
- Welche Probleme müssen für die verwendung von mehrerer vertrauenswürdigen Ausführungskontexte gelöst werden

[15] Vasily A. Sartakov et al. „EActors: Fast and flexible trusted computing using SGX“. In: **Proceedings of the 19th International Middleware Conference**. Middleware '18. https://doi.org/10.1145/3274808.3274823. New York, NY, USA: Association for Computing Machinery, Nov. 2018, S. 187–200.

[16] Messadi et al., „SplitBFT“.

ROTE[17] & LCM[18]

- Beschreibung des Angriffs
- Welche Gegenmaßnahmen gibt es für den Angriff
  - Wie verändern die Gegenmaßnahmen die Entwicklungsprozesse für Anwendungen?

[17] Sinisa Matetic et al. „{ROTE}: Rollback Protection for Trusted Execution“. en. In: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/matetic. 2017, S. 1289.

[18] Marcus Brandenburger et al. „Rollback and Forking Detection for Trusted Execution Environments Using Lightweight Collective Memory“. en. In: **2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)**. http://ieeexplore.ieee.org/document/8023119/. Denver, CO, USA: IEEE, Juni 2017, S. 157–168.

Foreshadow[19] & SgxPectre[20]

- Beschreibung des Angriffs
- Welche Gegenmaßnahmen gibt es für den Angriff
  - Wie verändern die Gegenmaßnahmen die Entwicklungsprozesse für Anwendungen?
- Wie haben Hardware Erweiterungsanbieter auf Angriffe reagiert?

[19] Jo Van Bulck et al. „FORESHADOW: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution“. en. In: (), S. 19.

[20] Guoxing Chen et al. „SgxPectre: Stealing Intel Secrets from SGX Enclaves Via Speculative Execution“. In: **2019 IEEE European Symposium on Security and Privacy (EuroS&P)**. Juni 2019, S. 142–157.

Malware in the SGX Supply Chain[21]

- Offenes Thema!
- Wie kann der Entwicklungsprozess gesichert werden?
- Wie kann ich sicher sein, dass ich die richtige Anwendung signiere?

[21] Vlad Craciun et al. „Malware in the SGX Supply Chain: Be Careful When Signing Enclaves!“ In: **IEEE Trans. Dependable Secur. Comput.** 19.2 (2022). https://doi.org/10.1109/TDSC.2020.3024562, S. 924–935.

Themenvergabe

- Themen werden nach Windhundverfahren vergeben
  - Intel SGX
  - AMD SEV SNP & Intel TDX
  - Keystone
  - ARM CCA
  - IBM PEF
  - Absicherung ganzer Anwendungen
  - Doppelseitige Sandboxen
  - Teilautomatisierte Partitionierung
  - Nutzung mehrerer vertrauenswürdigen Ausführungskontexte
  - Fork- und Rollback Angriffe
  - Seitenkanalangriffe
  - Abgesicherte Entwicklungsprozesse