

# CURRICULUM VITAE

## Alexios Voulimeneas

Nationality: Greek

Email: [A.Voulimeneas@tudelft.nl](mailto:A.Voulimeneas@tudelft.nl)

Twitter: @systemsgreek

Website: <https://alexios-voulimeneas.github.io/>

Languages: Greek (native), English (fluent), German (basic)

---

## Research Interests

**Cyber Security:** software diversity, memory safety, sandboxing, compartmentalization, exploits, defenses

**Operating Systems:** kernel development, networking, debugging, virtualization, application monitoring, heterogeneous computing, fault tolerance, reliability, record/replay

**Software Protection:** anti tampering, integrity checking, reverse engineering

## Appointments

<b>Assistant Professor</b> TU Delft Proud member of the Cybersecurity (CYS) section in Computer Science, Department of Intelligent Systems, Faculty of Electrical Engineering, Mathematics, and Computer Science. Tenured since March 15 <sup>th</sup> 2025.	2023 – Present
<b>Visitor Researcher</b> European Space Agency	2025 – Present
<b>Postdoctoral Scholar</b> KU Leuven I worked with Professor Stijn Volckaert in the DistriNet research group at KU Leuven's Technology Campus in Ghent, Belgium.	2020 – 2023
<b>Graduate Research Assistant</b> University of California, Irvine I worked with Professor Michael Franz in the Secure Systems Lab at the Donald Bren School of Information and Computer Sciences.	2015 – 2020
<b>Visiting Scholar</b> KU Leuven	Fall 2019
<b>Software Engineering Intern</b> Apple Inc.	Summer 2019
<b>Research Assistant Intern</b> Oracle Labs	Summer 2017
<b>Hellenic Army</b> (mandatory military service) Research and Informatics Directorate	11/2014 – 08/2015
<b>Undergraduate and Graduate Researcher</b> Mobile Multimedia Laboratory/AUEB	2011 – 2014
<b>C and JAVA Software Engineer Intern</b> NCSR Demokritos	Summer 2012

## Education

<b>PhD in Computer Science</b> University of California, Irvine <b>Advisor:</b> Professor Michael Franz <b>Thesis Topic:</b> Building the Next Generation of Security Focused NVX Systems: Overcoming Limitations of N-Variant Execution	2020
<b>MSc in Computer Science</b> University of California, Irvine	2017
<b>Ptychio in Informatics (4-year degree)</b> Athens University of Economics and Business (AUEB)/Department of Informatics, Athens <b>Advisor:</b> Professor George Xylomenos <b>Thesis Topic:</b> Towards an Error Control Scheme for a Publish/Subscribe Network	2012

## Awards, Grants, and Distinctions

2024: ACSAC Distinguished Paper Award with Artifact  
2023: CCS Top Reviewer Award  
2023: ASIA CCS Best Reviewer Award  
2022: Runner-up for the 2022 CNIL-Inria Award for Privacy Protection  
2022: EuroSys Distinguished Reviewer Artifact Award  
2016: ACM CCS Student Travel Grant  
2016: IEEE S&P Student Travel Grant  
2015: ICS Dean's Award, University California, Irvine  
2013: Scholarship for Graduate Studies, Latsis Foundation  
2013: Scholarship for Graduate Studies, Foundation for Education and European Culture  
2012: Valedictorian Graduate, Athens University of Economics and Business

## Publications

### **Clair Obscure: The Light and Shadow of System Call Interposition – From Pitfalls to Solutions with K23**

Jesús María Gómez, Vissarion Moutafis, Antreas Dionysiou, Fernando Kuipers, Georgios Smaragdakis, Bart Coppens, and Alexios Voulimeneas.

(To Appear) *In ACM/IFIP International Middleware Conference (Middleware 2025)*.

**Divide and Conquer: Introducing Partial Multi-Variant Execution.** J. Vinck, A. Jacobs, **A. Voulimeneas**, and S. Volckaert. *In IEEE European Symposium on Security and Privacy (Euro S&P 2025)*.

**Moneta: Ex-Vivo GPU Driver Fuzzing by Recalling In-Vivo Execution States.** J. Jung, J. Jang, Y. Jo, J. Vinck, **A. Voulimeneas**, S. Volckaert, and D. Song. *In Network and Distributed System Security Symposium (NDSS 2025)*.

[211 papers accepted out of 1311 submissions = 16.1%]

**I'll Be There for You! Perpetual Availability in the A<sup>8</sup> MVX.** A. Rösti, S. Volckaert, M. Franz, and **A. Voulimeneas**. *In Annual Computer Security Applications Conference (ACSAC 2024)*.

[83 papers accepted out of 381 submissions = 21.8%] [Distinguished Paper with Artifact Award]

**The Astonishing Evolution of Probabilistic Memory Safety: From Basic Heap-Data Attack Detection towards Fully Survivable Multi-Variant Execution.** A. Rösti, **A. Voulimeneas**, and M. Franz. *In IEEE Security & Privacy 2024*.

**Orbital Shield: Rethinking Satellite Security in the Commercial Off-the-Shelf Era.** N. Yadav, F. Vollmer, A. R. Sadeghi, G. Smaragdakis, and **A. Voulimeneas**. *In IEEE Conference on Security for Space Systems (3S) 2024*.

**System Call Interposition Without Compromise.** A. Jacobs, M. Gülmez, A. Andries, S. Volckaert, and **A. Voulimeneas**. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2024)*. [42 papers accepted out of 203 submissions = 20%]

**A run a day won't keep the hacker away: Inference attacks on endpoint privacy zones in fitness tracking social networks.** K. Dhondt, V. L. Pochat, **A. Voulimeneas**, W. Joosen, and S. Volckaert. In *BlackHat Asia 2023*

**A run a day won't keep the hacker away: Inference attacks on endpoint privacy zones in fitness tracking social networks.** K. Dhondt, V. L. Pochat, **A. Voulimeneas**, W. Joosen, and S. Volckaert. In *ACM Conference on Computer and Communications Security (CCS 2022)*. [218 papers accepted out of 971 submissions = 22.5%]

**You Shall Not (by)Pass! Towards Secure, and Fast PKU-based Sandboxing.** **A. Voulimeneas**, J. Vinck, R. Mechelinck, and S. Volckaert. In *European Conference on Computer Systems (EuroSys 2022)*. [42 papers accepted out of 162 submissions = 25.9%]

**Sharing is Caring: Secure and Efficient Shared Memory Support for MVEEs.** J. Vinck, B. Abrath, B. Coppens, **A. Voulimeneas**, B. De Sutter, and S. Volckaert. In *European Conference on Computer Systems (EuroSys 2022)*. [42 papers accepted out of 162 submissions = 25.9%]

**dMVX: Secure and Efficient Multi-Variant Execution in a Distributed Setting.** **A. Voulimeneas**, D. Song, P. Larsen, M. Franz, and S. Volckaert. In *European Workshop on Systems Security (EuroSec 2021)*

**Distributed Heterogeneous N-Variant Execution.** **A. Voulimeneas**, D. Song, F. Parzefall, Y. Na, P. Larsen, M. Franz, and S. Volckaert. In *Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2020)*. [13 papers accepted out of 45 submissions = 28.9%]

**Secure and Efficient Application Monitoring and Replication.** S. Volckaert, B. Coppens, **A. Voulimeneas**, A. Homescu, P. Larsen, B. De Sutter, and M. Franz. In *USENIX Annual Technical Conference (ATC 2016)*. [47 papers accepted out of 266 submissions = 17.6%]

**A Reliable Multicast Transport Protocol for Information-Centric Networks.** C. Stais, G. Xylomenos, and **A. Voulimeneas**. In *Journal of Network and Computer Applications (JNCA 2014)*

**Towards an Error Control Scheme for a Publish/Subscribe Network.** C. Stais, **A. Voulimeneas**, and G. Xylomenos. In *International Conference on Communications (ICC 2013)*

## Theses

**Building the Next Generation of Security Focused NVX Systems: Overcoming Limitations of N-Variant Execution.** A. Voulimeneas. PhD Thesis, 2020.

**Towards an Error Control Scheme for a Publish/Subscribe Network.** A. Voulimeneas. BSc Thesis, 2012.

## Funding

HONEY-MON: Cyber Deception via N-Variant Execution  
I contributed to the conception/brainstorming/writing of this accepted proposal  
Michael Franz (sole PI)  
Award Amount: +/- 1.65M \$

ONR (2021-2024)

TU Delft Starting Package  
(2023)

TU Delft

Funding for one PhD student for my appointment at TU Delft  
Alexios Voulimeneas  
Award Amount: +/- 375K €

# Professional Scientific Activities

## Conferences Service

(ISSN 2078-2489) Information, Reviewer, [2025]  
(CCS) ACM Conference on Computer and Communications Security, Treasurer [2026]  
(HotOS) SIGOPS ACM Workshop on Hot Topics in Operating Systems, Proceedings Chair [2027]  
(SOSP) ACM Symposium on Operating Systems Principles, Artifact Evaluation Committee Chair [2026]  
(ACSAC) Annual Computer Security Applications Conference, Program Committee [2025]  
(SYSTOR) ACM International Systems and Storage Conference, Program Committee [2025]  
(EuroSys) European Conference on Computer Systems, Proceedings Chair [2025]  
(ACNS) International Conference on Applied Cryptography and Network Security, Program Committee [2025]  
(S&P) IEEE Symposium on Security and Privacy, Program Committee [2025, 2026]  
(ISC) Information Security Conference, Program Committee [2024, 2025]  
(EuroSec) European Workshop on System Security, Program Committee [2024, 2025]  
(USENIX Security) USENIX Security Symposium, Program Committee [2024, 2025, 2026]  
(DIMVA) Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Program Committee [2024]  
(CCS) ACM Conference on Computer and Communications Security, Program Committee [2023, 2024]  
(Middleware) ACM/USENIX/IFIP International Middleware Conference, Program Committee [2023, 2025]  
(USENIX Security) USENIX Security Symposium, Artifact Evaluation Publication Chair [2023]  
(EuroSys) European Conference on Computer Systems, Program Committee [2023]  
(ASIACCS) ACM ASIA Conference on Computer and Communications Security, Program Committee [2023, 2024]  
(ESORICS) European Symposium on Research in Computer Security, Program Committee [2022, 2023]  
(PLDI) ACM SIGPLAN Conference on Programming Language Design and Implementation, Artifact Evaluation Committee [2022]  
(EuroSys) European Conference on Computer Systems, Artifact Evaluation Committee [2022]  
(USENIX Security) USENIX Security Symposium, Artifact Evaluation Committee [2022]  
(EuroSys) European Conference on Computer Systems, External Reviewer [2021, 2022]  
(ROOTS) Reversing and Offensive-oriented Trends Symposium, Program Committee [2020, 2021, 2022]  
(OSDI) USENIX Symposium on Operating Systems Design and Implementation, Artifact Evaluation Committee [2020]  
(S&P) IEEE Symposium on Security and Privacy, Student Program Committee [2018]

## Conferences Attended (+ = I gave a presentation)

(ASPLOS) International Conference on Architectural Support for Programming Languages and Operating Systems [Attended in 2025]  
(ACSAC) Annual Computer Security Applications Conference [Attended in 2024]  
(ESORICS) European Symposium on Research in Computer Security [Attended in 2023]  
(EuroSys) European Conference on Computer Systems [Attended in 2022+, 2025]  
(NDSS) Network and Distributed Systems Security Symposium [Attended in 2016, 2017, 2018, 2025]  
(S&P) IEEE Symposium on Security and Privacy [Attended in 2016]  
(CCS) ACM Conference on Computer and Communications Security [Attended in 2016]  
(DIMVA) Conference on Detection of Intrusions and Malware & Vulnerability Assessment [Attended in 2020+, 2022+]  
(EuroSec) European Workshop on Systems Security [Attended in 2020+]

## Talks

### **Building Secure and Reliable Systems – A Systems Approach**

Invited Talk, Ghent University, Ghent, Belgium April 2025

### **Building Secure and Reliable Systems – A Systems Approach**

Invited Talk, TU Delft, PL Group, Delft, Netherlands, November 2024

### **Building Secure and Reliable Systems – A Systems Approach**

Invited Talk, IMDEA Software Institute, Madrid, Spain, September 2024

### **Tales of Memory-Error Exploits and Defenses**

Invited Talk, TU Delft, Delft, Netherlands, March 2023

### **Tales of Memory-Error Exploits and Defenses**

Invited Talk, AUEB, Athens, Greece, December 2022

### **You Shall Not (by)Pass! Practical, Secure, and Fast PKU-based Sandboxing**

Invited Talk, Telecom SudParis/IP Paris, Online, December 2022

### **You Shall Not (by)Pass! Practical, Secure, and Fast PKU-based Sandboxing**

Invited Talk, Intel Labs, Online, May 2022

### **Distributed Heterogeneous N-Variant Execution**

Invited Talk, DRADS DistriNet Workshop, Leuven, Belgium, July 2021

### **Redundant Execution and Lightweight Monitoring for Security and Performance**

Invited Talk, Mobile Multimedia Laboratory (MMLab), AUEB, Athens, Greece, June 2019

### **Industry and Graduate Studies Opportunities in Greece, Europe, and USA**

Invited Talk, AUEB, Athens, Greece [2015, 2016, 2017, 2019, 2021, 2022]

## **Teaching Experience**

### **Course Developer & Instructor**

Systems Security

TU Delft

2024 – Present

### **Course Developer & Instructor**

Computer Security

TU Delft

2024 – Present

### **Teaching Assistant**

ICS 6B: Boolean Algebra and Logic

University of California, Irvine

Winter 2017

### **Reader**

ICS 46: Data Structure Implementation and Analysis

University of California, Irvine

Spring 2016

### **Lab Assistant**

Computational Mathematics

Athens University of Economics and Business

Summer 2010

# Media Coverage

Article at the Security Management Magazine about our recent ACSAC 2024 paper  
Netherlands

July 2025

## Mentoring, Training, and Advancement of Young Scientists

### Postdoc Mentor:

#### ongoing:

Antreas Dionysiou (2025-Present, TU Delft, Marie Skłodowska-Curie Postdoctoral Fellow Co-Hosting with Georgios Smaragdakis)

### PhD Research and Dissertation Mentor:

#### ongoing:

Vissarion Moutafis (2025-Present, TU Delft)

Jesús María Gómez Moreno (2024-Present, TU Delft)

### External PhD Thesis Reviewer/Evaluator

Alessandro Sanna ([expected 2025], University of Cagliari), "Under The Surface: Analysing Unconventional Malware and Unveiling its Secrets"

### MSc Thesis Mentor:

#### ongoing:

Ali Kahawati (2024-Present, TU Delft)

#### completed:

Vissarion Moutafis (MSc 2025, TU Delft, Present, TU Delft), "MORA: Hunting Space Bugs in your Sleep"

Wouter Jehee (MSc 2024, TU Delft), "WALL-EYE: Taking a look at CubeSat security - Security analysis of CubeSats on a physical testbed"

### MSc Thesis Committee Member:

Mitali Patil (MSc 2025 TU Delft), "Global State Queries in Stream Processing"

Martin Mladenov (MSc 2025, TU Delft), "When Peers Disappear: Protocol Denial of Service Attacks on BGP Routers"

Sergey Datskiv (MSc 2025, TU Delft), "Prompt, Seed, Generate: Seeding For Test Case Generator with LLMs"

Dea Llazo (MSc 2025, TU Delft), "Mitigating Alert Fatigue through Large Language Models - From Alert Enrichment and Prioritization to Full Automation of Incident Investigation"

Weiting Cai (MSc 2024, TU Delft), "1DRep:Automatic Repair for 1-day Vulnerabilities in Reused C/C++ IoT Open-source Software Components"

Daan Prinsze (MSc 2024, TU Delft), " PinDown: Generalized Application Code Identification And Functional Component Analysis In RTOS-based Firmware"

Adriaan Jacobs (MSc 2021, KU Leuven), “Combating address-sensitive behavior in MVEEs”

Michael Poker (MSc 2022, TU Braunschweig), “Techniques for Fast-Forwarding Execution State to Synchronize Software Instances in an MVEE”

*Current as August 22, 2025*