

# 宁振宇

博士，计算机科学

广东省深圳市南山区学苑大道 1088 号南方科技大学工学院南楼 441A, 518055

☎ 137-742-19743 | ✉ ningzy@sustech.edu.cn | 🏠 ningzhenyu.github.io

## 研究兴趣

本人的研究专注于安全和隐私的各个领域，包括系统安全、移动安全、物联网安全、交通运输安全、可信执行环境、硬件辅助安全、以及透明恶意软件分析等等。

## 教育经历

韦恩州立大学

博士，计算机科学

密歇根州, 美国

2015 年 8 月 - 2020 年 4 月

同济大学

硕士，计算机科学与技术

上海, 中国

2008 年 8 月 - 2011 年 4 月

同济大学

学术，计算机科学与技术

上海, 中国

2004 年 8 月 - 2008 年 6 月

## 工作经历

研究助理教授，副研究员

南方科技大学

深圳, 中国

2020 年 6 月至今

研究助理或教学助理

韦恩州立大学

密歇根州, 美国

2015 年 8 月 - 2020 年 4 月

高级软件工程师

波罗蜜电子商务有限公司

上海, 中国

2015 年 5 月 - 2015 年 7 月

高级软件工程师

中国银联股份有限公司

上海, 中国

2012 年 9 月 - 2015 年 4 月

助理软件工程师

华为技术有限公司

上海, 中国

2011 年 4 月 - 2012 年 9 月

## 论文发表

\* 表示共同一作.

**[TDSC'22 (CCF A 类期刊, JCR 一区, 中科院一区)] Revisiting ARM Debugging Features: Nailgun and Its Defense**

ZHENYU NING, CHENXU WANG, YINHUA CHEN, AND FENGWEI ZHANG ✉

To Appear in IEEE Transactions on Dependable and Secure Computing, 2022.

**[HASP'21] A Novel Memory Management for RISC-V Enclaves**

HAONAN LI\*, WEIJIE HUANG\*, MINGDE REN, HONGYI LU, ZHENYU NING ✉, AND FENGWEI ZHANG

In Proceedings of the Hardware and Architectural Support for Security and Privacy (HASP'21), in conjunction with the 54th IEEE/ACM International Symposium on Microarchitecture (MICRO'21), October, 2021.

**[ESORICS'20 (CCF B 类会议)] HART: Hardware-assisted Kernel Module Tracing on Arm**

YUNLAN DU\*, ZHENYU NING\*, JUN XU, ZILONG WANG, YUEH-HSUN LIN, FENGWEI ZHANG ✉, XINYU XING, AND BING MAO


In Proceedings of the 25th European Symposium on Research in Computer Security, United Kingdom, September, 2020.

### [DSN'20 (CCF B 类会议)] KShot: Live Kernel Patching with SMM and SGX

LEI ZHOU, FENGWEI ZHANG , JINGHUI LIAO, ZHENYU NING, JIDONG XIAO, KEVIN LEACH, WESTLEY WEIMER, AND GUOJUN WANG

In Proceedings of the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Spain, June, 2020  
(Runner-up Best Paper Award, 3 out of 291 submissions).

### [JCDR'19 (CCF A 类中文期刊)] 基于边缘计算的可信执行环境研究

宁振宇, 张锋巍 , 和施巍松

计算机研究与发展, 第 7 期 56 卷, 1441-1453 页, 2019.

### [DIMVA'19 (CCF C 类会议)] Understanding the Security of Traffic Signal Infrastructure

ZHENYU NING, FENGWEI ZHANG , AND STEPHEN REMIAS

In Proceedings of the 16th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Gothenburg, Sweden, 2019.

### [S&P'19 (CCF A 类会议)] Understanding the Security of ARM Debugging Features

ZHENYU NING AND FENGWEI ZHANG

In Proceedings of the 40th IEEE Symposium on Security & Privacy, San Francisco, California, May, 2019.

### [TIFS'19 (CCF A 类期刊, JCR 一区, 中科院一区)] Hardware-assisted Transparent Tracing and Debugging on ARM

ZHENYU NING AND FENGWEI ZHANG 

In IEEE Transactions on Information Forensics & Security, Vol.14, No.6, pp.1595-1609, 2019.

### [EdgeSP'18] Preliminary Study of Trusted Execution Environments on Heterogeneous Edge Platforms

ZHENYU NING, JINGHUI LIAO, FENGWEI ZHANG, AND WEISONG SHI

In Proceedings of the 1st ACM/IEEE Workshop on Security and Privacy in Edge Computing, in conjunction with the 3rd ACM/IEEE Symposium on Edge Computing (SEC'18), Bellevue, Washington, October, 2018.

### [DSN'18 (CCF B 类会议)] DexLego: Reassembleable Bytecode Extraction for Aiding Static Analysis

ZHENYU NING AND FENGWEI ZHANG

In Proceedings of the 48th IEEE/IFIP International Conference on Dependable Systems and Networks, Luxembourg, June, 2018.

### [Security'17 (CCF A 类会议)] Ninja: Towards Transparent Tracing and Debugging on ARM

ZHENYU NING AND FENGWEI ZHANG

In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, August, 2017.

### [HASP'17] Position Paper: Challenges Towards Securing Hardware-assisted Execution Environments

ZHENYU NING, FENGWEI ZHANG, WEISONG SHI, AND LARRY SHI

In Proceedings of the Hardware and Architectural Support for Security and Privacy, In conjunction with the 44th International Symposium on Computer Architecture (ISCA), Toronto, ON, Canada, June, 2017.

### [In Review] StrongBox: A GPU TEE on Arm Endpoints

YUNJIE DENG, CHENXU WANG, SHUNCHANG YU, SHIQING LIU, ZHENYU NING, FENGWEI ZHANG 

### [In Review] Alligator In Vest: Using Hardware Features for Failure Diagnosis on Arm

YIMING ZHANG, HAONAN LI, YUXIN HU, WENXUAN SHI, XUEYING ZHANG, ZHENYU NING , FENGWEI ZHANG, XIAPU LUO

## 科研项目

---

### 基于 RISC-V 架构的可信执行环境研究

中国自然科学基金青年基金项目, No.62102175

2022 年 1 月-2024 年 12 月, 300,000 RMB, 主持

### Armory: 基于软硬协同的 Arm Enclave 研究

蚂蚁金服 (杭州) 网络技术有限公司

2021 年 10 月-2022 年 10 月, 600,000 RMB, 主持

### Arm 云平台 Secure EL2 研究

蚂蚁智信 (杭州) 信息技术有限公司

2021 年 3 月-2022 年 3 月, 520,000 RMB, 主持

## 基于 RISC-V 架构的软硬件协同数据流分析技术

华为技术有限公司

2020 年 10 月-2021 年 9 月, 1,200,000 RMB, 参与

## Arm 平台核故障检测与处理技术

华为技术有限公司

2020 年 4 月-2022 年 3 月, 1,418,000 RMB, 参与

## 发明专利

---

### 可信执行环境构建方法、系统及存储介质

宁振宇, 张锋巍

审核中, 申请号 202011313471X, 中国

### 基于 ARM 架构的资源访问控制方法、系统、设备及存储介质

宁振宇, 张锋巍, 王晨旭, 陈胤桦

审核中, 申请号 2021111482366, 中国

### 基于 ARM 架构的 GPU 可信执行方法、系统、设备及存储介质

张锋巍, 宁振宇, 邓韵杰, 王晨旭, 于顺昌, 刘世晴

审核中, 申请号 2021111501367, 中国

## 专题演讲

---

### [CRVF'19] SecLabel: Enhancing RISC-V Platform Security with Labelled Architecture

ZHENYU NING, YINQIAN ZHANG, AND FENGWEI ZHANG

In China RISC-V Forum, Shenzhen, China, November, 2019.

### [MOSEC'19] Nailgun: Breaking the Privilege Isolation on ARM

ZHENYU NING AND FENGWEI ZHANG

In Mobile Security Conference, Shanghai, China, May, 2019.

### [DEFCON China'18] Transparent Malware Debugging on x86 and ARM

ZHENYU NING AND FENGWEI ZHANG

In DEFCON China, Beijing, China, May, 2018.

## 展示海报

---

### Poster: SecLabel: Enhancing RISC-V Platform Security with Labelled Architecture

ZHENYU NING, YINQIAN ZHANG, AND FENGWEI ZHANG

In China RISC-V Forum (CRVF), Shenzhen, China, November, 2019.

### Poster: Enhancing ARM Platform Security with Hardware Tags

ZHENYU NING AND FENGWEI ZHANG

In the 40th IEEE Symposium on Security & Privacy, San Francisco, California, May, 2019.

### Poster: Revealing True Behavior via Instruction-level Extraction and Reassembling on Android

ZHENYU NING AND FENGWEI ZHANG

In the IEEE Southeastern Michigan 2016 Spring Conference, Livonia, MI, April, 2016.

## 教学经历

---

### CSC 4111 软件工程实验, 教员

韦恩州立大学计算机系, 2017 年秋季学期.

## CSC 4110 软件工程, 教学助理

韦恩州立大学计算机系, 2017 年秋季学期.

## 专业服务

---

### 程序委员会成员

[CCSW]: ACM Cloud Computing Security Workshop, 2020

### 代码评估委员会成员

[USENIX-Security]: USENIX Security Symposium, 2021

[ACSAC]: Annual Computer Security Applications Conference, 2019, 2020

### 外部审稿人

[CCS]: ACM Conference on Computer and Communications Security, 2017, 2018, 2019

[ACSAC]: Annual Computer Security Applications Conference, 2017, 2018, 2019

[EuroSec]: European Workshop on Systems Security, 2018, 2019

### 审稿人

[TDSC]: IEEE Transactions on Dependable and Secure Computing, 2021

[Computer & Security]: Elsevier Computer & Security, 2020, 2021

[TMC]: IEEE Transactions on Mobile Computing, 2020

[LOCS]: IEEE Letters of the Computer Society, 2018

## 学术奖励

---

2020 **Runner-up Best Paper Award (3/291)**, IEEE/IFIP DSN

2019 **Faculty Competitive for Graduate Research Assistantships Award**, 韦恩州立大学

2019 **Student Travel Grant**, IEEE S&P

2018 **Student Travel Grant**, IEEE/IFIP DSN

# Zhenyu Ning

PH.D. IN COMPUTER SCIENCE

Room 441A, South Tower, CoE Building, SUSTech, 1088 Xueyuan Avenue, Nanshan District, Shenzhen 518055

☎ 137-742-19743 | ✉ ningzy@sustech.edu.cn | 🏠 ningzhenyu.github.io

## Research Interest

My Research interests are in different areas of security and privacy, including system security, mobile security, IoT security, transportation security, trusted execution environments, hardware-assisted security, transparent malware analysis, etc.

## Education

### Wayne State University

PH.D. IN COMPUTER SCIENCE

MI, USA

Aug. 2015 - Apr. 2020

### Tongji University

M.S. IN COMPUTER SCIENCE

Shanghai, China

Aug. 2008 - Apr. 2011

### Tongji University

B.S. IN COMPUTER SCIENCE

Shanghai, China

Aug. 2004 - Jun. 2008

## Employment History

### Research Assistant Professor

SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Shenzhen, Guangdong, China

Jun. 2020 - present

### Graduate Research or Teaching Assistant

WAYNE STATE UNIVERSITY

MI, USA

Aug. 2015 - Apr. 2020

### Senior Software Engineer

BOLOME ELECTRONIC COMMERCE

Shanghai, China

May 2015 - Jul. 2015

### Senior Software Engineer

CHINA UNIONPAY

Shanghai, China

Sep. 2012 - Apr. 2015

### Assistant Software Engineer

HUAWEI TECHNOLOGIES

Shanghai, China

Apr. 2011 - Sep. 2012

## Publications

\* indicates these authors contribute equally to the paper.

### [TDSC'22] Revisiting ARM Debugging Features: Nailgun and Its Defense

ZHENYU NING, CHENXU WANG, YINHUA CHEN, AND FENGWEI ZHANG ✉

To Appear in IEEE Transactions on Dependable and Secure Computing, 2022.

### [HASP'21] A Novel Memory Management for RISC-V Enclaves

HAONAN LI\*, WEIJIE HUANG\*, MINGDE REN, HONGYI LU, ZHENYU NING ✉, AND FENGWEI ZHANG

In Proceedings of the Hardware and Architectural Support for Security and Privacy (HASP'21), in conjunction with the 54th IEEE/ACM International Symposium on Microarchitecture (MICRO'21), October, 2021.

### [ESORICS'20] HART: Hardware-assisted Kernel Module Tracing on Arm

YUNLAN DU\*, ZHENYU NING\*, JUN XU, ZILONG WANG, YUEH-HSUN LIN, FENGWEI ZHANG ✉, XINYU XING, AND BING MAO

In Proceedings of the 25th European Symposium on Research in Computer Security, United Kingdom, September, 2020.

### [DSN'20] KShot: Live Kernel Patching with SMM and SGX

LEI ZHOU, FENGWEI ZHANG ✉, JINGHUI LIAO, ZHENYU NING, JIDONG XIAO, KEVIN LEACH, WESTLEY WEIMER, AND GUOJUN WANG

In Proceedings of the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Spain, June, 2020 (Runner-up Best Paper Award, 3 out of 291 submissions).

### **[JCDR'19] A Study of Using TEE on Edge Computing**

ZHENYU NING, FENGWEI ZHANG , AND WEISONG SHI

In Journal of Computer Research and Development, Vol.56, No.7, pp.1441-1453, 2019.

### **[DIMVA'19] Understanding the Security of Traffic Signal Infrastructure**

ZHENYU NING, FENGWEI ZHANG , AND STEPHEN REMIAS

In Proceedings of the 16th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Gothenburg, Sweden, 2019.

### **[S&P'19] Understanding the Security of ARM Debugging Features**

ZHENYU NING AND FENGWEI ZHANG

In Proceedings of the 40th IEEE Symposium on Security & Privacy, San Francisco, California, May, 2019.

### **[TIFS'19] Hardware-assisted Transparent Tracing and Debugging on ARM**

ZHENYU NING AND FENGWEI ZHANG 

In IEEE Transactions on Information Forensics & Security, Vol.14, No.6, pp.1595-1609, 2019.

### **[EdgeSP'18] Preliminary Study of Trusted Execution Environments on Heterogeneous Edge Platforms**

ZHENYU NING, JINGHUI LIAO, FENGWEI ZHANG, AND WEISONG SHI

In Proceedings of the 1st ACM/IEEE Workshop on Security and Privacy in Edge Computing, in conjunction with the 3rd ACM/IEEE Symposium on Edge Computing (SEC'18), Bellevue, Washington, October, 2018.

### **[DSN'18] DexLego: Reassembleable Bytecode Extraction for Aiding Static Analysis**

ZHENYU NING AND FENGWEI ZHANG

In Proceedings of the 48th IEEE/IFIP International Conference on Dependable Systems and Networks, Luxembourg, June, 2018.

### **[Security'17] Ninja: Towards Transparent Tracing and Debugging on ARM**

ZHENYU NING AND FENGWEI ZHANG

In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, August, 2017.

### **[HASP'17] Position Paper: Challenges Towards Securing Hardware-assisted Execution Environments**

ZHENYU NING, FENGWEI ZHANG, WEISONG SHI, AND LARRY SHI

In Proceedings of the Hardware and Architectural Support for Security and Privacy, In conjunction with the 44th International Symposium on Computer Architecture (ISCA), Toronto, ON, Canada, June, 2017.

### **[In Review] StrongBox: A GPU TEE on Arm Endpoints**

YUNJIE DENG, CHENXU WANG, SHUNCHANG YU, SHIQING LIU, ZHENYU NING, FENGWEI ZHANG 

### **[In Review] Alligator In Vest: Using Hardware Features for Failure Diagnosis on Arm**

YIMING ZHANG, HAONAN LI, YUXIN HU, WENXUAN SHI, XUEYING ZHANG, ZHENYU NING , FENGWEI ZHANG, XIAPU LUO

## **Research Grants**

---

### **A Trusted Execution Environment Based on RISC-V Architecture**

NATIONAL NATURAL SCIENCE FOUNDATION OF CHINA, NO.62102175

2022.01-2024.12, 300,000 RMB, Principal Investigator

### **Armory: Research on Hardware-assisted Arm Enclave**

ANT GROUP

2021.10-2022.10, 600,000 RMB, Principal Investigator

### **Research on Secure EL2 of Arm Cloud Platforms**

ANT GROUP

2021.03-2022.03, 520,000 RMB, Principal Investigator

### **Hardware-assisted Taint Flow Analysis on RISC-V**

HUAWEI

2020.10-2021.09, 1,200,000 RMB, Participant

## Error and Failure Detection of Arm Processors

HUAWEI

2020.04-2022.03, 1,418,000 RMB, Participant

## Patents

---

### Approach, System and Storage for Trusted Execution Environments

ZHENYU NING, FENGWEI ZHANG

In Review, No.202011313471X, China

### Approach, System, Device and Storage for Resource Access Control on Arm

ZHENYU NING, FENGWEI ZHANG, CHENXU WANG, YINHUA CHEN

In Review, No.2021111482366, China

### Approach, System, Device, and Storage for GPU-based Trusted Execution Environments on Arm

FENGWEI ZHANG, ZHENYU NING, YUNJIE DENG, CHENXU WANG, SHUNCHANG YU, SHIQING LIU

In Review, No.2021111501367, China

## Talks

---

### [CRVF'19] SecLabel: Enhancing RISC-V Platform Security with Labelled Architecture

ZHENYU NING, YINQIAN ZHANG, AND FENGWEI ZHANG

In China RISC-V Forum, Shenzhen, China, November, 2019.

### [MOSEC'19] Nailgun: Breaking the Privilege Isolation on ARM

ZHENYU NING AND FENGWEI ZHANG

In Mobile Security Conference, Shanghai, China, May, 2019.

### [DEFCON China'18] Transparent Malware Debugging on x86 and ARM

ZHENYU NING AND FENGWEI ZHANG

In DEFCON China, Beijing, China, May, 2018.

## Posters

---

### Poster: SecLabel: Enhancing RISC-V Platform Security with Labelled Architecture

ZHENYU NING, YINQIAN ZHANG, AND FENGWEI ZHANG

In China RISC-V Forum (CRVF), Shenzhen, China, November, 2019.

### Poster: Enhancing ARM Platform Security with Hardware Tags

ZHENYU NING AND FENGWEI ZHANG

In the 40th IEEE Symposium on Security & Privacy, San Francisco, California, May, 2019.

### Poster: Revealing True Behavior via Instruction-level Extraction and Reassembling on Android

ZHENYU NING AND FENGWEI ZHANG

In the IEEE Southeastern Michigan 2016 Spring Conference, Livonia, MI, April, 2016.

## Professional Services

---

### Program Committee

[CCSW]: ACM Cloud Computing Security Workshop, 2020

### Artifact Evaluation Committee

[USENIX-Security]: USENIX Security Symposium, 2021

[ACSAC]: Annual Computer Security Applications Conference, 2019, 2020

## External Reviewer

[CCS]: ACM Conference on Computer and Communications Security, 2017, 2018, 2019

[ACSAC]: Annual Computer Security Applications Conference, 2017, 2018, 2019

[EuroSec]: European Workshop on Systems Security, 2018, 2019

## Reviewer

[TDSC]: IEEE Transactions on Dependable and Secure Computing, 2021

[Computer & Security]: Elsevier Computer & Security, 2020, 2021

[TMC]: IEEE Transactions on Mobile Computing, 2020

[LOCS]: IEEE Letters of the Computer Society, 2018

## Awards

---

2020 **Runner-up Best Paper Award (3/291)**, IEEE/IFIP DSN

2019 **Faculty Competitive for Graduate Research Assistantships Award**, Wayne State University

2019 **Student Travel Grant**, IEEE S&P

2018 **Student Travel Grant**, IEEE/IFIP DSN