Carlton Shepherd
Konstantinos Markantonakis

# Trusted Execution Environments

Springer

# Trusted Execution Environments

Carlton Shepherd • Konstantinos Markantonakis

# Trusted Execution Environments

Springer

Carlton Shepherd
School of Computing
Newcastle University
Newcastle upon Tyne, Tyne and Wear, UK

Konstantinos Markantonakis
Information Security Group
Royal Holloway, University of London
Egham, Surrey, UK

ISBN 978-3-031-55560-2 ISBN 978-3-031-55561-9 (eBook)
https://doi.org/10.1007/978-3-031-55561-9



This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*For James, Henry, and Ellen.*
*— Carlton*

*I would like to dedicate this book to Maria, Eleni, and Georgios, and my grandparents Areti and Kostas, Sofia and Eftyhios.*
*— Kostas*

# Foreword

The need for Trusted Execution Environments (TEE) long predates the invention of computers, as there have always been sensitive activities that need carrying out reliably, protected from imposters, eavesdroppers, thieves, and disruptors. These activities may involve precious things and so protected storage and controlled access falls within the TEE concept.

A castle is a very old example of a TEE. Its strong walls would protect against physical attacks and meetings within an inner keep would resist eavesdropping, with trained guards alert to attackers trying to trick their way inside. Important documents of the time would carry an official wax seal for tamper detection and integrity protection and could be securely stored in a strong box with other valuables. Shared codes would allow ciphered communications for secure messaging beyond the castle. Of course, few people own castles, and they are not designed for our increasingly IT-centric society; but, fast forward to the 1990s, and we had developed smart card chips. These chips mimicked the castle protection on a microscopic and IT-enabled scale, with secure storage, execution, communication, and sophisticated hardware and software defences against physical, side-channel, and fault attacks. Standards also emerged that supported multi-vendor, multi-application compatibility, and internationally recognised security evaluations. Therefore, it might sound like the TEE requirement was satisfied in the 1990s, but sadly no. Real castles served the narrow interests of their owners, and smart cards did the same for the card Issuers. Large vendor organisations have also become so powerful that they adopt proprietary approaches when international standards do not suit them.

Rather than providing an open security foundation for a range of applications, access to security chips was closely guarded by their owners, with policies that, practically or financially, deterred third party access. The Trusted Platform Module (TPM) initiative made use of embedded smart-card style security chips, but they were not mandated and so there is no common hardware security anchor across all device types. If we consider mobile phones as the most ubiquitous user device, a range of hardware-enabled proprietary security solutions exist, which the vendors ask us to trust without disclosure of design and implementation. The vendors also control these solutions for security reasons, but also for business advantage.

So, how is it we have sensitive applications when there is no ubiquitous and accessible hardware-based TEE for developers to exploit? Developers just do their best, with increased error risk from multiple product versions and/or relying solely on software measures when there is no better alternative. Perhaps the risk is manageable for many of the things we do with IT, but what about for cyber-physical systems? Would you reduce your TEE requirements for your medical devices, your driverless car or your smart power-grid? Clearly the need for TEE is as strong as ever, but it has yet to be adequately realised, despite suitable technologies being available. If you are interested in this vital topic and how it is evolving, then I commend you to read this book from authors knowledgeable in the field.

Royal Holloway, University of London, Prof. Keith Mayes
Egham, United Kingdom
May 2023

# Acknowledgements

We would like to thank members of the Smart Card and Internet of Things Centre (SCC) at Royal Holloway, University of London, who painstakingly commented on and corrected early drafts of this book. A big "thank you" is due to Nicola Bates, Amir Rafi, Jan Kalbantner, Zhanyu Sha, and Darren Hurley-Smith for generously volunteering their time and energy. Moreover, we wish to extend our thanks to the SCC's past members who influenced and developed the group's research profile in secure and trusted execution platforms. Particular thanks goes to Raja Naeem Akram, Iakovos Gurulian, Gerhard Hancke, Damien Sauveron, and all the others who are too many to mention in full. We also wish to pay special thanks to Keith Mayes, who led the creation of the SCC and guided the group through good times and challenging ones. Keith has been instrumental in building the group's international reputation in the area of smart cards, secure elements, and related technologies. Lastly, we wish to thank the team at Springer for their flexibility and assistance towards making this book a reality.

# Contents

# About the Authors

**Dr. Carlton Shepherd** (Ph.D., B.Sc.) is a Lecturer (equivalent to Assistant Professor) in Computing at Newcastle University, UK. His expertise lies in mobile and embedded systems security at the interface of hardware and software, including trusted execution environments, side-channel and fault injection attacks, smart cards, secure elements and their applications. He holds a Ph.D. in Information Security from Royal Holloway, University of London, and a B.Sc. in Computer Science from Newcastle University.

**Prof. Konstantinos Markantonakis** (B.Sc., M.Sc., M.B.A., Ph.D.) received his B.Sc. in Computer Science from Lancaster University in 1995, his M.Sc. in Information Security in 1996, and his Ph.D. in 2000 and his MBA in International Management in 2005 from Royal Holloway, University of London. He is currently a Professor of Information Security in the Information Security Group in Royal Holloway University of London. He is also the Director of the Information Security Group Smart Card and IoT Security Centre (SCC). His main research interests include smart card security and applications, IoTs, embedded system security and trusted execution environments, payment, automotive, and avionics system security. He has published more than 200 papers in international conferences and journals. His research has attracted funding from competitive UK/EU funding sources and from industry. He is also the Director of the "Transformative Digital Technologies, Security and Society" Catalyst, at Royal Holloway University of London, responsible for coordinating multidisciplinary research and impact activities. He is the chair of IFIP WG 11.2 Pervasive Systems Security, has experience in the commercialisation of cyber security research, and is an experienced consultant for several technology companies.

# Acronyms

| | |
|---|---|
| ABI | Application Binary Interface |
| AES | Advanced Encryption Standard |
| ALU | Arithmetic Logic Unit |
| AMBA | Advanced Microcontroller Bus Architecture |
| AP | Access Point |
| APB | Advanced Peripheral Bus |
| API | Application Programming Interface |
| ARQC | Authorisation Request Cryptogram |
| AXI | Advanced eXtensible Interface |
| BGA | Ball Grid Array |
| CC | Common Criteria |
| CCRA | Common Criteria Recognition Arrangement |
| CCTL | Common Criteria Testing Laboratory |
| CLK | Clock |
| CMVP | Cryptographic Module Validation Program |
| CPU | Central Processing Unit |
| CRTM | Core Root of Trust for Measurement |
| CSR | Certificate Signing Request |
| CVE | Common Vulnerabilities and Exposures |
| DAA | Direct Anonymous Attestation |
| DAC | Discretionary Access Control |
| DDA | Dynamic Data Authentication |
| DES | Data Encryption Standard |
| DMA | Direct Memory Access |
| DRAM | Dynamic Random Access Memory |
| DRM | Digital Rights Management |
| DRTM | Dynamic Root of Trust for Measurement |
| EAL | Evaluation Assurance Level |
| ECC | Elliptic Curve Cryptography |
| ECDH | Elliptic Curve Diffie-Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |

| | |
|---|---|
| EPROM | Erasable Programmable Read-Only Memory |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| ELF | Executable and Linkable Format |
| eMMC | Embedded MultiMediaCard |
| EMV | Europay, MasterCard, and Visa |
| FEK | File Encryption Key |
| FIPS | Federal Information Processing Standards |
| FIQ | Fast Interrupt Request |
| GIC | Generic Interrupt Controller |
| GID | Group Identifier |
| GND | Ground |
| GPIO | General-Purpose Input/Output |
| GPU | Graphics Processing Unit |
| HCE | Host Card Emulation |
| HDD | Hard Disk Drive |
| HMAC | Hashed Message Authentication Code |
| HUK | Hardware Unique Key |
| I/O | Input/Output |
| I2C | Inter-Integrated Circuit |
| IC | Integrated Circuit |
| ICOM | Inter-Communications |
| IDAU | Implementation-Defined Attribution Unit |
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| IoT | Internet of Things |
| IOMMU | Input/Output Memory Management Unit |
| IPC | Inter-Process Communication |
| IRQ | Interrupt Request |
| ISA | Instruction Set Architecture |
| ISO | International Organization for Standardization |
| JCRE | Java Card Runtime Environment |
| JCVM | Java Card Virtual Machine |
| JTAG | Joint Test Action Group |
| JVM | Java Virtual Machine |
| LLC | Last Level Cache |
| MAC | Message Authentication Code |
| MPU | Memory Protection Unit |
| MLS | Multi-Level Security |
| MOSFET | Metal-Oxide-Semiconductor Field-Effect Transistor |
| NAS | Network-Attached Storage |
| NFC | Near-Field Communication |
| NIST | National Institute of Standards and Technology |
| NS | Non-Secure |

| | |
|---|---|
| NSA | National Security Agency |
| NVIC | Nested Vectored Interrupt Controller |
| OEM | Original Equipment Manufacturer |
| OS | Operating System |
| OTP | One-Time Password |
| PCR | Platform Configuration Register |
| PIC | Programmable Interrupt Controller |
| PID | Process Identifier |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PMP | Physical Memory Protection |
| PoP | Package-on-Package |
| PoS | Point of Sale |
| PP | Protection Profile |
| PRNG | Pseudorandom Number Generator |
| RA | Remote Attestation |
| RAM | Random Access Memory |
| RBAC | Role-Based Access Control |
| REE | Rich Execution Environment |
| RFC | Request for Comments |
| RFID | Radio Frequency Identification |
| RNG | Random Number Generator |
| ROM | Read Only Memory |
| RoT | Root of Trust |
| RPMB | Replay Protected Memory Block |
| RSA | Rivest-Shamir-Adleman |
| RTC | Real-Time Clock |
| RTM | Root of Trust for Measurement |
| RTOS | Real-Time Operating System |
| RTR | Ready to Run |
| RTS | Ready to Send |
| SAR | Security Assurance Requirement |
| SAU | Security Attribution Unit |
| SCI | System Configuration and Integration |
| SCP | Secure Channel Protocol |
| SCR | System Control Register |
| SCS | System Control Space |
| SD | Secure Digital |
| SE | Security Extension |
| SEP | Secure Enclave Processor |
| SFR | Security Functional Requirement |
| SGX | Software Guard Extensions |
| SHA | Secure Hash Algorithm |
| SHS | Secure Hash Standard |
| SiP | System in Package |

| | |
|---|---|
| SMC | Secure Monitor Call |
| SoC | System on Chip |
| SRAM | Static Random Access Memory |
| SRK | Storage Root Key |
| SSD | Solid State Drive |
| SSH | Secure Shell |
| SSK | Secure Storage Key |
| SVM | Secure Virtual Machine |
| TCG | Trusted Computing Group |
| TDX | Trusted Domain Extensions |
| TEE | Trusted Execution Environment |
| TLB | Translation Lookaside Buffer |
| TLS | Transport Layer Security |
| TMF | Trusted Management Framework |
| TOE | Target of Evaluation |
| TPM | Trusted Platform Module |
| TRNG | True Random Number Generator |
| TSK | TA Storage Key |
| TSM | Trusted Service Manager |
| TUI | Trusted User Interface |
| TXT | Trusted Execution Technology |
| TZASC | TrustZone Address Space Controller |
| TZMA | TrustZone Memory Adapter |
| TZPC | TrustZone Protection Controller |
| UEFI | Unified Extensible Firmware Interface |
| UID | User Identifier |
| USB | Universal Serial Bus |
| UTS | Unix Time-Sharing System |
| UUID | Universally Unique Identifier |
| VM | Virtual Machine |
| VMM | Virtual Machine Monitor |

# List of Figures

# List of Tables