An Introduction to Trusted Execution Environments: Exercise Worksheet

Dr. Carlton Shepherd
carlton.shepherd@ncl.ac.uk

You have seen how trusted execution environments (TEEs) can be used as a hardware-assisted security mechanism on modern computing platforms.

You will now tackle the problems in Sections 1 to 4 and the design challenge in Section 5. Lastly, in Section 6, you will also work to reflect how hardware-assisted security could relate to other topics that you may have encountered, such as privacy-preserving machine learning and post-quantum security.

It is expected that you spend approximately 6–7 minutes on each problem section, i.e. ∼25 minutes in total; 20 minutes on the design problem; and 20 minutes on the final innovation activity. We will discuss the answers in class.

1 Secure Boot

In general, secure boot sequences work by verifying the digital signatures of each boot-time component in a chain. An authenticate-then-load paradigm is typically followed.

Problem 1:

- A secure boot sequence starts with a *root of trust*, which is an inherently trusted component. **What could happen if an adversary is able to gain control over a root of trust?**

Problem 2:

- Discuss some key management problems with secure boot sequences as described. **Which problems do you consider the most important to get right?**

Problem 3:

- Over time, it is usually necessary to update boot-time components in order to address bugs and security vulnerabilities. **What issues might emerge here?**

2 Trusted Computing Bases

Recall that a *trusted computing base* (TCB) is the set of all components relied upon to maintain the security policy of a given system.

Problem 4:

- **Discuss some components that might be included in a typical TCB.**

Problem 5.

- **Discuss why we want to minimise the size of a TCB.** Conversely, think about what happens when the TCB is very large. What issues do we face?

Problem 6:

- **Evaluate the statement:** *"A smaller Trusted Computing Base is inherently more secure."* Discuss the validity and limitations of this assertion.

3 Deployment Challenges

Problem 7:

- A trusted execution environment can be used to prevent users from modifying code and data on their devices. **What ethical issues does this raise?**

Problem 8:

- Many different TEE technologies have been developed, each with their own methods for realising isolated execution, communication protocols, target devices, etc. **Discuss what challenges and constraints this might raise when deploying TEEs in the real world**.

Problem 9:

- **What kind of attacks might be used against a TEE?** Justify your answers.

Problem 10:

- **Evaluate how TEEs might impact modern software development tools. What limitations might need to be overcome?**

4 Applications

Problem 11:

- **How could TEEs be used to enhance the security of data analysis in the cloud?**

Problem 12:

- You are a systems designer employed by an IoT company that manufactures sensors for monitoring industrial control systems (e.g. environmental monitors). **How could TEEs be applied to enhance the security of these sensors?**

5 Design Problem

You have been employed as a security architect for a company developing a new mobile streaming platform. The platform will enable users to play copyrighted movies, TV shows, and music on their personal mobile devices, such as tablets and smartphones.

In groups, create a high-level system design showing how TEEs could be used to provide additional security assurances. In particular, you should consider:

- What assets do we need to protect?
- What adversaries and attack vectors will you consider? What are their capabilities and motivations?
- How will you securely receive copyrighted data over a network?
- How will you securely display received data without relying on any untrusted components?

6 Take Home: Innovation Activity

One method of approaching innovation is to consider how different emerging or advanced topics can be combined to create something new.

In this activity, think about the other topics that you have encountered in this module. Consider ways in which the following topics could be applied, combined or enhanced using TEEs and hardware-assisted security. *(Note: you do not necessarily have to consider every topic; you may want to focus on only one or two).*

- *Privacy-preserving machine learning.*
- *Post-quantum security.*
- *Cloud security.*
- *Blockchain.*
- *Other trusted computing techniques.*

Here are some ideas to help begin your discussions:

- Where could you see TEEs being useful in the context of cloud security? What additional security assurances could they provide?
- What are the potential problems of the privacy-preserving machine learning techniques that you have encountered? How could TEEs be used to mitigate them?
- Consider a blockchain application, such as digital money (e.g. Bitcoin). How could TEEs be applied and to what end?

Further Resources

- *Definitions and basics*: see Sabt et al. [1] and Shepherd et al. [2].
- *Attacks on TEEs*: Nilsson et al. [3] (attacking Intel SGX), Cerdeira et al. [4] (attacking ARM TrustZone), Schwarz & Gruss [5] (micro-architectural attacks), and Shepherd et al. [6] (physical side-channel and fault injections).
- *Applications*: Priebe et al. [7] (databases), Tamrakar et al. [8] (identity verification), Rafi et al. [9] (copyright protection), Schuster et al. [10] (data analytics), Jeon & Kim [11] (mobile gaming), and Li et al. [12] (mobile advertising).

References

[1] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: what it is, and what it is not," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 57–64, IEEE, 2015.

[2] C. Shepherd, G. Arfaoui, I. Gurulian, R. P. Lee, K. Markantonakis, R. N. Akram, D. Sauveron, and E. Conchon, "Secure and trusted execution: Past, present, and future—a critical review in the context of the internet of things and cyber-physical systems," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 168–177, IEEE, 2016.

[3] A. Nilsson, P. N. Bideh, and J. Brorsson, "A survey of published attacks on Intel SGX," *arXiv preprint arXiv:2006.13598*, 2020.

[4] D. Cerdeira, N. Santos, P. Fonseca, and S. Pinto, "SoK: Understanding the prevailing security vulnerabilities in TrustZone-assisted TEE systems," in *IEEE Symposium on Security and Privacy*, pp. 1416–1432, IEEE, 2020.

[5] M. Schwarz and D. Gruss, “How trusted execution environments fuel research on microarchitectural attacks,” *IEEE Security & Privacy*, vol. 18, no. 5, pp. 18–27, 2020.

[6] C. Shepherd, K. Markantonakis, N. van Heijningen, D. Aboulkassimi, C. Gaine, T. Heckmann, and D. Naccache, “Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis,” *Computers & Security*, vol. 111, p. 102471, 2021.

[7] C. Priebe, K. Vaswani, and M. Costa, “EnclaveDB: A secure database using SGX,” in *IEEE Symposium on Security and Privacy*, pp. 264–278, IEEE, 2018.

[8] S. Tamrakar, J.-E. Ekberg, and N. Asokan, “Identity verification schemes for public transport ticketing with NFC phones,” in *Proceedings of the 6th ACM Workshop on Scalable Trusted Computing*, pp. 37–48, ACM, 2011.

[9] A. Rafi, C. Shepherd, and K. Markantonakis, “A first look at digital rights management systems for secure mobile content delivery,” in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, 2023.

[10] F. Schuster, M. Costa, C. Fournet, C. Gkantsidis, M. Peinado, G. Mainar-Ruiz, and M. Russinovich, “Vc3: Trustworthy data analytics in the cloud,” in *Proceedings of the 36th IEEE Symposium on Security and Privacy, S&P*, vol. 15, 2014.

[11] S. Jeon and H. K. Kim, “TZMon: Improving mobile game security with ARM TrustZone,” *Computers & Security*, vol. 109, p. 102391, 2021.

[12] W. Li, H. Li, H. Chen, and Y. Xia, “Adattester: Secure online mobile advertisement attestation using TrustZone,” in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 75–88, ACM, 2015.