Commercial Microelectronics Security Challenges

Jason Moore
jason.moore@amd.com

AMD
together we advance_

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Challenges as Security Becomes Ubiquitous

Who is your Adversary?

- Question elicits a very interesting response
- Sophisticated Low-cost Attacks are on rise
  - Thermal Laser Stimulation[4] (TLS)
  - Electro-Optical Probing[5] (EOP)
- Emerging Sensing Capabilities
  - PLATYPUS[1], CPAmap[2], Sideline[3]

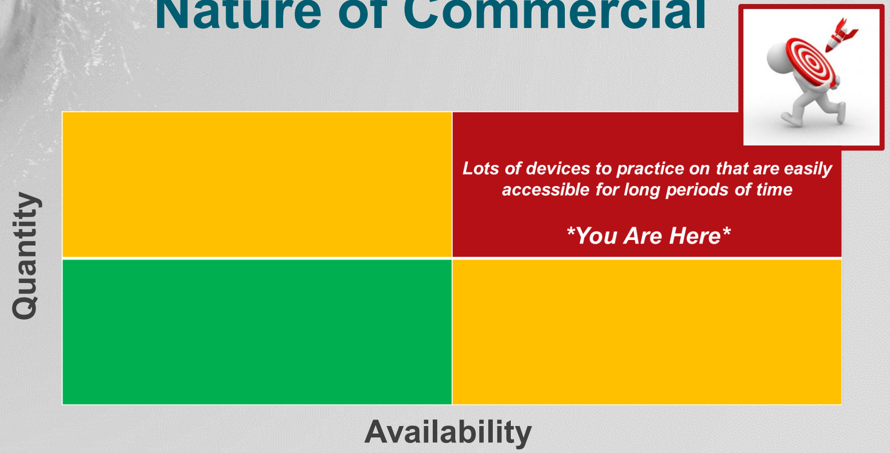
Emerging Requirements

- Multi-Tenancy
- Confidential Compute
- Close Physical Access
- Cost is Rising but how to monetize?

Multiple Standards

- NO Standards
- FIPS 140-3
- PCIe-IDE / TDISP
- Digital Cinema Initiative
- IEEE 802.11
- Payment Card Industry
- ISO21434
- IEC62443
- J3101 / J3201
- Open Compute Platform
- ISO / IEC 15408 Common Criteria
- Trusted Computing Group

Nature of Commercial


Lots of devices to practice on that are easily accessible for long periods of time
You Are Here
Quantity
Availability

Automotive

Communications

Defense

Data Center

Industrial, Vision and Healthcare

References

1. Lipp, Kogler, Oswald, Schwarz, Easdon, Canella, Gruss (2021), PLATYPUS: Software-based Power Side-Channel Attacks on x86, *2021 IEEE Symposium on Security and Privacy (SP)*, https://platypusattack.com/platypus.pdf

2. Krautter, Gnad, Tahoori (2021), CPAmap: On the Complexity of Secure FPGA Virtualization, Multi-Tenancy and Physical Design, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 121-146, https://doi.org/10.13154/tches.v2020.i3.121-146

3. Vravellier, Dutertre, Teglia, Moundi (2020), SideLine: How Delay-Lines (May) Leak Secrets from your SoC, *https://eprint.iacr.org/2020/1127.pdf*

4. Lohrke, H., Tajik, S., Krachenfels, T., Boit, C., & Seifert, J.-P. (2018). *Key Extraction Using Thermal Laser Stimulation: A Case Study on Xilinx Ultrascale FPGAs. IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(3), 573–595. https://doi.org/10.13154/tches.v2018.i3.573-595

5. Tajik, S., Lohrke, H., Seifert, J.-P. and Boit, C. (2017) ‘On the Power of Optical Contactless Probing’, Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM. doi: 10.1145/3133956.3134039.

AMD