COSIC
CRYPTOGRAPHY & CYBER SECURITY

Trust in CPU+FPGA Architectures

Furkan Turan and Ingrid Verbauwhede

CPU+FPGA PLATFORMS

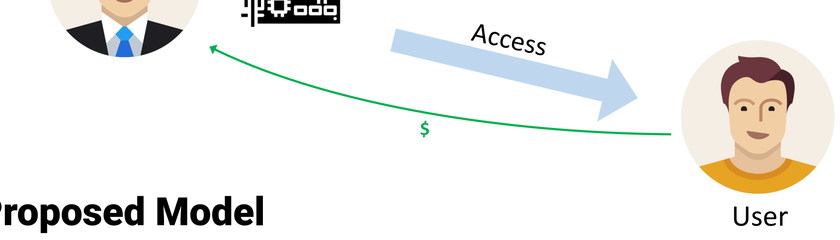
Platform	CPU	FPGA
Xilinx *Zynq*	ARM	Artix7 / UltraScale
Intel *Xeon+FPGA*	Xeon	Arria10
Amazon WS	Intel	Xilinx
Alibaba	Intel	Xilinx / Intel
Huawei	Intel	Xilinx
Baidu	Intel	Xilinx

Anyone can construct a platform with commercial devices and even offer it for cloud use.

TRUST MODELS

Old Model

- Designer wants to protect his IP, he does not trust user.
- Designers can only protect their IP, if it is delivered encrypted to FPGA.
- Key provisioning requires physical access.
- Model is restricted to only two parties.



Related Work for Better Models

[1,2,3] present the FPGA vendor as the trusted party who hides his secret key in FPGA at manufacturing.

[2] also proposes a key establishment protocol between the FPGAs and the accelerator providers, which also requires hiding a secret key in the FPGAs so that MiTM attacks can be avoided.

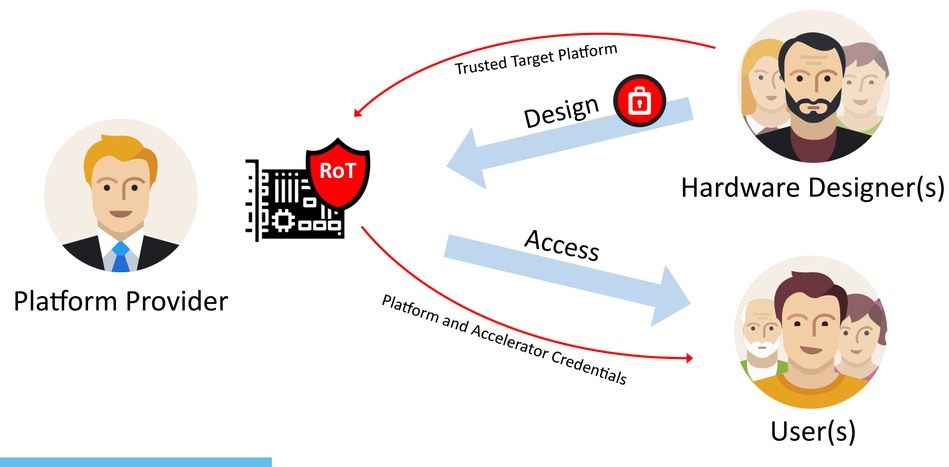
[4] similarly prefers a TTP who receives the FPGA from its vendor, and delivers it to users after installing its own key.

Current Model

- Platform providers do not trust hardware designers and users .
- Designers and users need to trust to the platform provider.
- No cryptography is used.

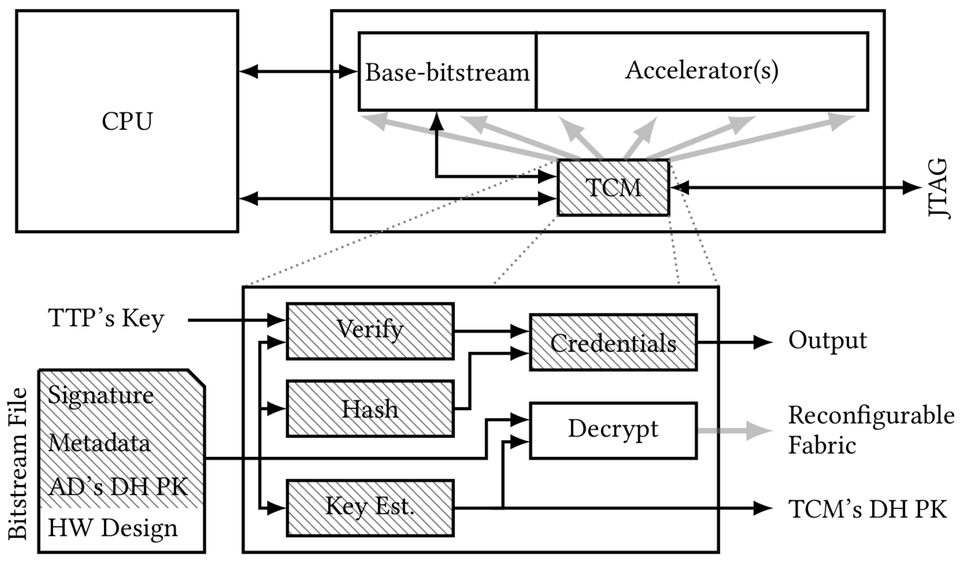
Our Proposed Model

- The trust model accounts the platform providers, HW designers and users.
- Each involved entity is treated with equal importance.
- The platforms allow shared use by multiple designers and users.
- The platforms are provided with a RoT (Root-of-Trust) to enforce the model.
- The entities use the RoT to establish a trust relationship.



TRUSTED CONFIGURATION MODULE (TCM)

TCM is a small unmodifiable RoT added to the FPGA device. It improves the existing FPGA configuration modules and implements our trust model.



- It programs the bitstream for either a base-design or accelerators.
- It supports three basic features:

Bitstream Identification

- Calculates a unique identifier for the bitstream.
- Derives bitstream credentials from metadata and identifier.
- Advertises the credentials to applications.
- Lets accelerators target their base-design.

Building Trust with Authentication

- Relies on TTPs to sign and verify the target bitstreams.
- Lets entities freely/independently pick TTPs to authenticate themselves.
- If entity trusts to the TTPs that the others are authenticated by, then a trust relationship can be established.

Confidentiality

- Avoids permanent keys.
- Supports DH key exchange with online solutions.
- Decrypts the design, only if trust is established to agree on a key.

- The TCM enables entities to establish a trust relationship, relying on cryptographic proofs from freely picked TTPs.
- It avoids claiming an entity as an authority over the others, and abstains from asking manufacturers or TTPs from hiding a secret inside the FPGAs.

Future Work

The TCM can only be successful if it is supported by the FPGA manufacturers. Hence, we plan to turn the design into a prototype to prove its practicality.

References

[1] Saar Drimer, Tim Güneysu, Markus G Kuhn, and Christof Paar. 2008. Protecting multiple cores in a single FPGA design. Draft available at http://www. cl. cam. ac. uk/sd410/, May (2008).

[2] Tim Güneysu, Bodo Moller, and Christof Paar. 2007. Dynamic intellectual property protection for reconfigurable devices. In Field-Programmable Technology, 2007. ICFPT 2007. International Conference on. IEEE, 169–176.

[3] Tom Kean. 2002. Cryptographic rights management of FPGA intellectual property cores. In Proceedings of the 2002 ACM/SIGDA tenth international symposium on Field-programmable gate arrays. ACM, 113–118.

[4] Roel Maes, Dries Schellekens, and Ingrid Verbauwhede. 2012. A pay-per-use licensing scheme for hardware IP cores in recent SRAM-based FPGAs. IEEE Transactions on Information Forensics and Security 7, 1 (2012), 98–108.

Funding

FAU FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
KIT Karlsruhe Institute of Technology
TRR 89
erc

KU LEUVEN

https://www.esat.kuleuven.be/cosic/

@CosicBe

ESAT