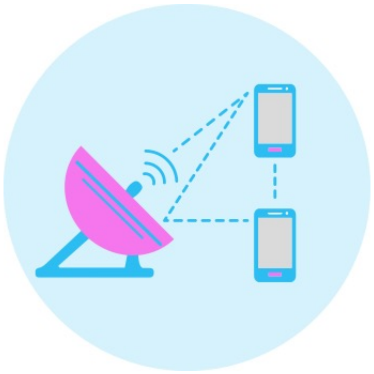
UNIVERSITÀ
DEGLI STUDI
DI PADOVA

UniSMART
Fondazione Università di Padova



Smart device security system

Applicants	Università degli Studi Padova, KU Leuven
Inventors	Mauro Conti, Md Masoom Rabbani, Nele Mertens Jo, Vliegen
Priority Date	30/04/2018
Protection	PCT/EP2019/060382 Ongoing China, Europe, USA

What's needed for?

Smart devices are an important part of today's world, but their security is constantly threatened by a wide array of attacks. This invention uses FPGA (Field Programmable Gate Array) to implement a Remote Attestation as a low-cost, easy to implement alternative to costly tamper-resistant hardware.

The presence of smart devices will continue to grow in all economic sectors. Unfortunately, they are often threatened by attacks to their security system. In order to face such threats, the patented invention uses a remote FPGA attestation to secure devices from attacks. FPGAs are widely used in sectors like aviation, military, cryptography, biomedical and digital-signal processing. For this reason the use of FPGAs instead of costly tamper-resistant hardware to achieve security through remote attestation is a valid, low-cost and easy to implement solution. Through FPGAs, the complete configuration of any architecture can be accessed so that smart devices can be protected from a wide array of attacks.

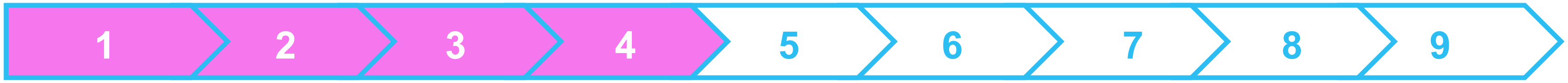
Advantages

- FPGAs can be used in place of tamper-resistant hardware to provide better resiliency against a wide array of attackers
- Improve security in smart device, automated cars or for drones along with sensitive applications like military, aviation, or bio-medical

Applications

- Security measures against both software (i.e. malware) and hardware attackers in various applications

TRL scale



Informatics, Electronics and Communication Systems