Improving the Availability of Secure Space Links through the Partial Reconfiguration of FPGAs

Emmanuel Lesser
Product Assurance and Safety Department
European Space Agency
Noordwijk, The Netherlands
emmanuel.lesser@esa.int

***Abstract*—As an increasing amount of critical infrastructure we rely on daily is enabled by satellite services, the need for secure space and ground segments is now more important than ever. Space missions must be secured end-to-end in order to protect satellite operations, as well as sensitive and proprietary data transmissions. Secure space communication links can become unusable due to the radiation environment they operate in. More specifically, radiation events can corrupt session keys used to secure communication between ground and space. This research investigates the use of an affordable technique for mitigating this risk, ensuring reliable, secure, long-lifetime space missions. By partially reconfiguring FPGAs, corrupted session keys can be restored without any impact on the availability of the secure link, and without the need for expensive radiation-hardened components. An experiment using this technique is currently operating on the ISS.**

I. Introduction

While securing wireless communication links is commonplace in terrestrial applications, this is not always the case for communication links between ground and space segments. However, increasingly, satellite communication links must be secured, causing the success of missions to depend heavily on the reliability of encryption-based links.

In this research, we present an experimental technique, based in-part on the partial reconfiguration of FPGAs, to achieve reliable secure communication links using widely-available Commercial Off-The-Shelf (COTS) components.

II. In-Orbit Radiation Effects on Secure Links

Symmetric-key algorithms, like the Advanced Encryption Standard (AES), use the same cryptographic key for both encryption and decryption in order to achieve secure wireless communication. In case of satellite communications, this cipher key is known only to the satellite and trusted ground stations. The key cannot be renewed between both parties once the satellite is in-orbit, as it could be intercepted by an attacker eavesdropping on the exchange.

If the need arises to renew the cipher key during operations, for example because the key on the satellite was corrupted due to a bit-flip caused by a Single Event Upset, a key recovery protocol like the one proposed by Gebotys [1] can be initiated to securely exchange new keys. However, for this protocol to work reliably, we must ensure that the base key k_0 cannot be irreversibly corrupted during the entire lifetime of the satellite.

III. Two Experiment Setups

In the first setup, we mounted five Digilent Cmod A7-35T boards ($U_{1...5}$) on a custom PCB. Each FPGA contains a MicroBlaze core. $U_{2...4}$ are each running a small C-program to perpetually send k_0 to the voter U_5. The voter evaluates the inputs received from the active tiles. In case of a single discrepancy, the voter powers-off the corrupted tile and brings in the redundant tile (U_1 by default) by powering it on. The inactive tile now becomes the redundant one, as it will be reset and thus repaired in case it is powered on again. U_5 acts as a simple majority voter and sends to its output whichever k_0 it received from either three or two tiles.

In the second setup, we used a Zynq-7000 based board with a Xilinx XC7Z020-1CLG400C SoC, in which a similar configuration as described above was implemented using four reconfigurable partitions (RPs) and the ARM processor to act as the simple majority voter.

IV. The Experiment Cube

Both experiment setups were integrated into an International Space Station (ISS) payload with the form-factor of a $10cm^3$ cube. The experiment cube was launched to the ISS on April 17, 2019.

V. Preliminary Results

Experiment data returned was analysed for the period mid-May 2019 to end of September 2019. Eleven Single Event Effectss were detected. However, none of these radiation events caused the corruption of the session key in either experiment setup. We expect that during the 18-month lifetime of the experiment several session key corruptions will occur due to radiation events.

References

[1] C. H. Gebotys, "Security in Embedded Devices," Springer Science & Business Media, 2009.

2576-2621/20/$31.00 ©2020 IEEE
DOI 10.1109/FCCM48280.2020.00053