Intermittent Computing, its vulnerabilities and a protocol to secure its power transitions

Archanaa S. Krishnan

The Bradley Department of Electrical and Computer Engineering

Virginia Tech

Abstract: In the field of Internet of Things, self-powered devices provide a sustainable alternative to battery powered devices, but they suffer from frequent power loss due to lack of input power. Intermittent systems prevent restarting by storing a snapshot of the device state as a checkpoint in non-volatile memory. Upon the next power-up, the device is restored with the most recent checkpoint and resumes application execution. All the security sensitive data from both the system and application state are stored in a checkpoint. An attacker with access to the nonvolatile memory has the ability to view, tamper and replay checkpoints without alerting the device. To overcome these vulnerabilities, we designed the Secure Intermittent Computing Protocol, which provides the following security features to the checkpoints of an intermittent system. First, it provides basic information security to checkpoints. Second, it introduces uniqueness to the checkpoints to detect checkpoint replay. Third, the checkpoints are chained to preserve the order of checkpoints. As the protocol is designed for intermittent systems, it is atomic in design to protect checkpoint generation and restoration process form power loss.

Bio: Archanaa S. Krishnan is a third year Ph.D. student at the Bradley Department of Electrical and Computer Engineering at Virginia Tech. She works in the Secure Embedded Systems Lab with Dr. Patrick Schaumont as her advisor. She received her M.S. in Computer Engineering from Virginia Tech in 2018. Her research focuses on designing and implementing security in embedded devices. Webpage: https://archanaask.github.io/homepage/