Cybersecurity Attack using High Speed Clock Glitch

Santosh Desiraju, G.Nigamantha Chakravarthi and Dr.Chansu Yu
Department of Electrical Engineering and Computer Science
Washkewicz College of Engineering, Cleveland State University

Goal	Creating a dedicated set-up for clock glitch attacks that develops a high speed clock using custom FPGA bit-streams to inject faults through clock glitching on complex High Speed Microcontrollers (MCUs).

Introduction

In recent times, **hardware secu**rity has drawn a lot of interest in research community. With physical proximity to the target devices, various hardware attack methods have been proposed and tested to alter their functionality and trigger behavior not intended by the design.

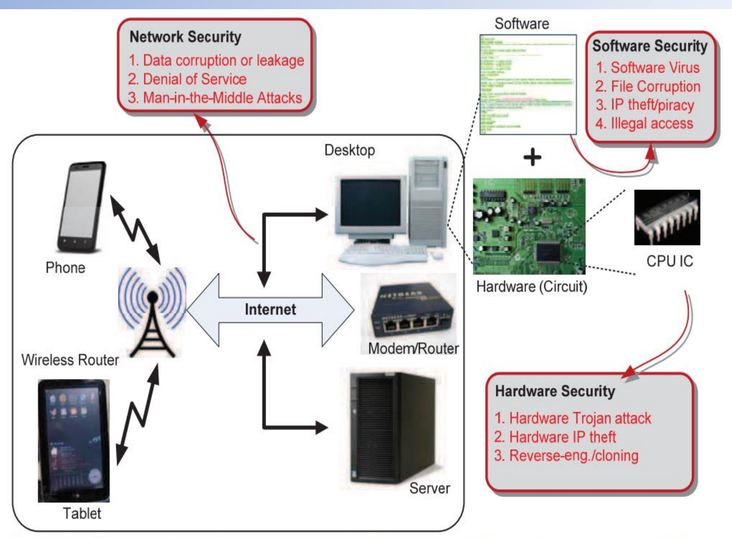
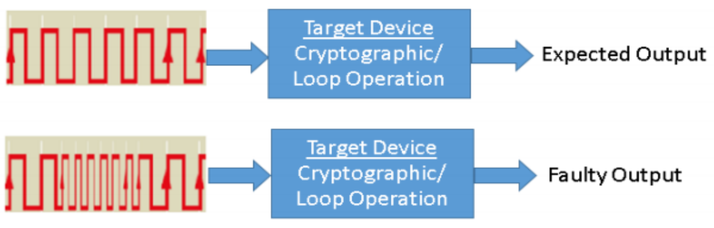


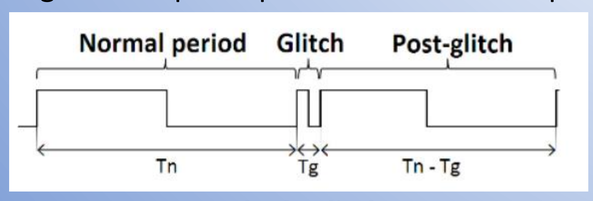
Figure 1: The spectrum of security issues in the connected computer systems, which include information security, software security and hardware security.

One of the cost effective form of hardware security attack is **clock glitching** and is preferred due to controllability and temporary effect on the target device. **Analysis of system behavior under stress** may reveal the attacker the security code.

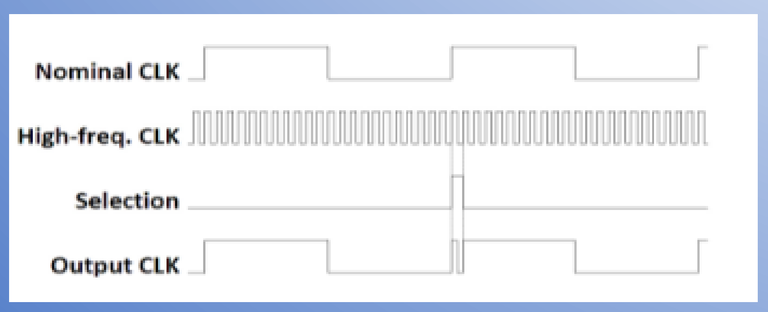


Motivation

The utilization of a high speed clock in digital electronics has become more prevalent in recent times. Various types of attacks have to be tried and tested which will indirectly result in the development of secure hardware in the future. This research intends to implementing the **experimental setup involved in creating high speed clock glitches** and providing an in-depth explanation on the setup.



Clock glitch

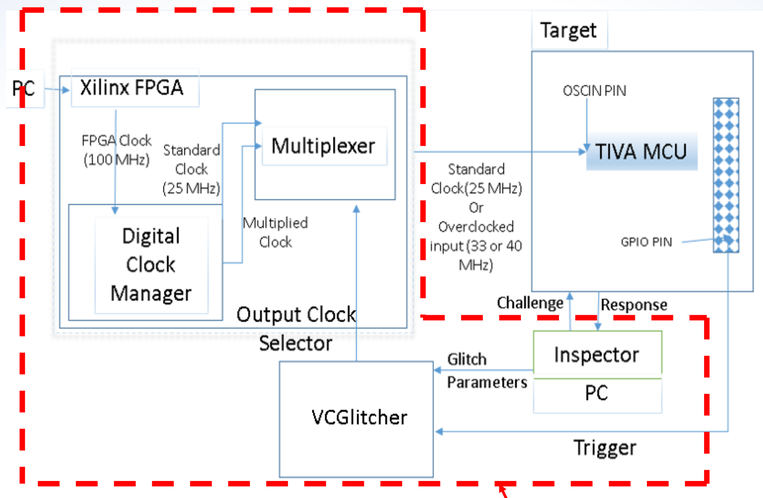


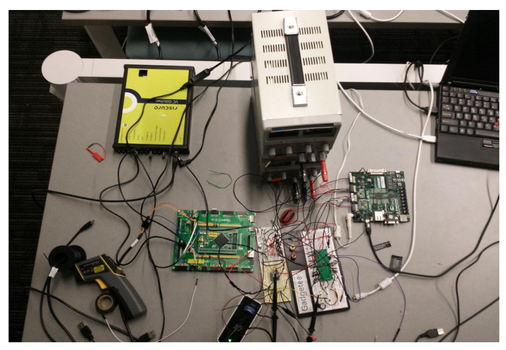
Generation of clock glitch

Methodology

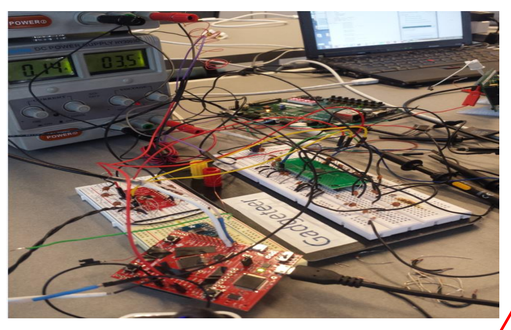
Targets used for this research are:
Tiva C Series Launchpad (Texas Instrument) and
Core 417I Development Board (ST Microelectronics).

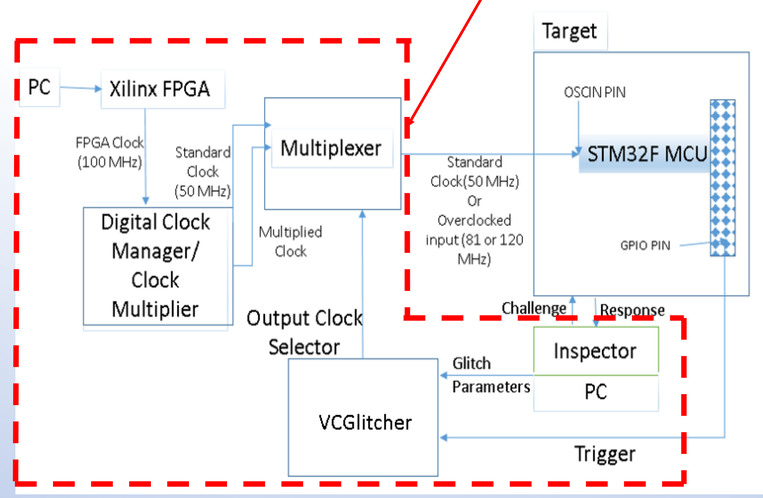
The following two figures show the setup of the on-chip clock glitch generator for the experiment.

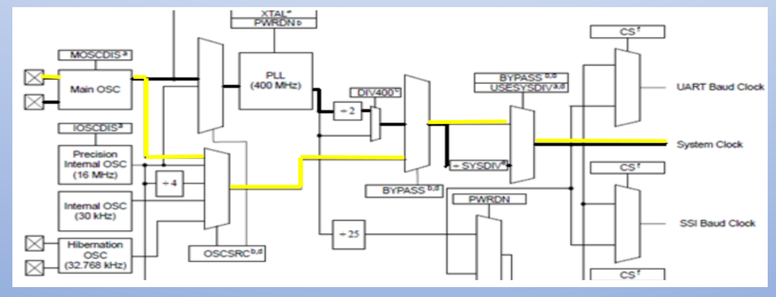




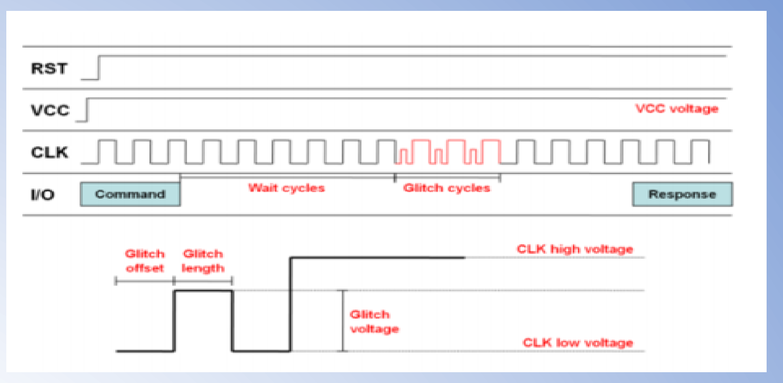
Clock glitch generator







Clock tree of Tiva C System



Clock glitch parameters

Experiments

Setup:

1. DCM (digital clock manager) generates both standard and high-speed clock. The multiplexor can choose either clock based on “VCGlitcher” input.
2. “Inspector” configures glitch parameters.
3. Clock-glitching operations will be embedded into the target algorithm.

Run-time:

1. Execute computationally-intensive security algorithms (e.g., RSA-CRT with modular exponentiation operations)
2. Clock-glitching operations are triggered; Delivered to “VCGlitcher” via GPIO pins.
3. VCGlitcher selects high-speed clock
4. Execution behavior is recorded by “Inspector”

Observations

- Overclock ranges which yielded maximum glitches on the applications running are:
  - 25-33 MHz for TI MCU
  - 50-81 MHz for ST MCU
- When overclocked to certain high speed range, the targets do not respond and need to be reset. The ranges are:
  - 40 MHz for TI MCU
  - 300 MHz and higher for ST MCU

Future Work

- More powerful clock multiplier – With greater range.
- Experimentation on other higher speed externally clocking MCUs or single-board computers.
- PCB Design – To integrate external analog circuitry into a single board for compactness and efficiency in measurement evaluation.
- Controlling FPGA using Inspector – For parameter control or scripting on PC side.

Acknowledgement

This work is supported by **National Science Foundation** and is in collaboration with **Case Western Reserve University** and also supported by **Riscure**.