*agile*GLITCH

Side Channel Attack Voltage Glitch Detector Core

Application Examples

Version: Issue 1.1
Date: 2021-01-26
Doc Num: AA-000415-MA

1 Introduction

This document outlines a series of example usages for the *agile*GLITCH voltage monitor core, based on existing and expected future requirements.

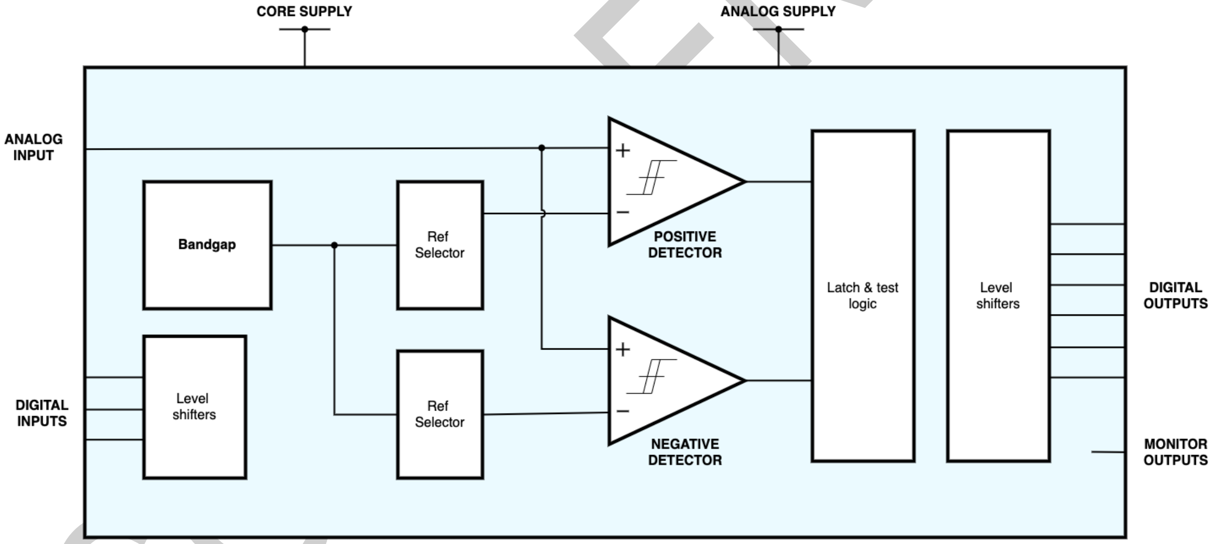
To maintain confidentiality, this information is not directly extracted from any current customer requirements. A number of these attacks have been modelled on attacks that have been documented in public forums, or in white-hack security conferences.

2 About the *agile*GLITCH core

The *agileGLITCH* voltage monitor provides security and protection against voltage side-channel attacks (SCA) and tampering such as supply voltage changes/glitches and power supply manipulation. The sensor provides digital outputs to warn (secure) processors of intrusion attempts, thus enabling a holistic approach to hardware security.

As a key part of the *agile*SCA TVC (Temperature, Voltage, Clock) security sensor, it can be tuned to your specifications and is ideally suited for security and monitoring in applications such as in IoT, Security, Automotive, Medical, AI and general SoCs and ASICs.

The system overview (shown below) includes 4 major components:



2.1 Bandgap

This provides an accurate voltage reference for the other system components, and is designed to operate from a wider voltage range than typical to ensure good coverage of glitch monitoring. The bandgap follows a traditional architecture, based on ratios of current through two different p-n junctions. The bandgap incorporates a bootstrap circuit to ensure reliable turn-on at start up, and has the option for production trim to increase accuracy.

2.2 Comparator

Two configurations of a Comparator are specified, to enable over-voltage and under-voltage glitches to be detected. The thresholds are configurable, and level-shifters are incorporated to allow the IOs to be driven from the core supply.

2.3 Reference selectors

These reference selectors provide configurable input voltages to the programmable comparators, to allow the glitch voltage level to be adjusted. These also allow the thresholds to be adjusted if, for example, the core uses DVFS (Dynamic Voltage and Frequency Scaling).

2.4 Control and test logic and level shifters

From the output of the comparator, the control logic provides the following functions:

- Control of enables based on digital inputs
- Latching of momentary events on the comparator outputs
- Disabling the outputs during test mode
- 3-way majority voting on latched outputs

2.5 (Optional) ADC

An optional SAR ADC can be used to measure the exact value of the supply, which can be used for ongoing monitoring of lifetime issues or performance degradation.

3 Example use cases

3.1 IOT Security – key extraction

Device	Front door wireless lock to a residential house
Scenario	Visitor to house offers to change the batteries in the front door for the owner. Using a voltage-glitching device, the visitor is able to enter debug mode on the lock, and dump out all the authorised keys for the lock.
Result	Malicious person is able to replicate an existing user key for a house, and enter the house, with the audit trail pointing at another user.
Exploit	Voltage glitch allows attacker to enter debug mode and dump out all keys that are authorised by the lock.
Protection	*agile*GLITCH is able to detect voltage glitch events, and records them as suspicious activity. Once repowered, the lock is able to report to the cloud that nefarious activity was suspected, with date and time implicating the nefarious party.

3.2 Home Control Hub – reflash firmware

Device	Camera-enabled home hub device
Scenario	Online trader offers cheap home hub devices for sale in sealed boxes. These devices have been reflashed with firmware that, as well as performing the expected task, also streams a video and audio stream to the trader's server.
Result	Nefarious entity is able to continuously monitor activity in the target house, and use for blackmail or to observe and sell footage of target famous users.

Exploit	Voltage glitch allows attacker to bypass standard boot-signing sequence. This allows the exploiting party to reset the security key to a known value, and reflash unauthorised firmware. Exploiting party downloads firmware, but adds a 'remote monitor' function.
Protection	*agile*GLITCH is able to detect voltage glitch events, and prevents unauthorised code from being installed on the device to reset the boot keys. In addition, the device is able to report to the user and server that it was not new out of the box, and hence user can replace.

3.3 Automotive – performance degradation

Device	Driver assistance solution in modern car
Scenario	Due to device lifetime effects a voltage supply regulator to a car's ADAS system means over time, an increased power supply resistance is seen. This effect is marginal, but is exacerbated at moments of high load, which can cause the voltage to drop below that acceptable for operation.
Result	During highly complex, fast moving manoeuvres, the processing load draws too much power, and the system fails, handing control back to driver at key point.
Exploit	The manufacturing fault is latent, and wasn't detected on the production line, as voltage was within spec. Due to lifetime effects, this degrades over time, and eventually fails during a point of high load.
Protection	*agile*GLITCH is able to detect ongoing voltage degradation ahead of time, and that at times this can spike close to spec values. This is reported by the system back to the car manufacturer, who can identify the fault, and call in cars in priority order to have this patched ahead of a fault causing an accident. The automotive supplier may be able to remotely fix cars through a software patch to increase the supply voltage on faulty cars.

3.4 Satellite TV – bypass fixed link encryption

Device	Satellite TV receiver
Scenario	Nefarious user plans to remove Digital Rights Management (DRM) from films broadcast over satellite channel, and resell.
Result	Content owner discovers that their content is available for rent download, without requisite payment back to them for number of views.
Exploit	Nefarious user installs voltage glitcher on HDMI controller supply to Set Top Box satellite receiver with valid subscription. By voltage glitching, user is able to reset HDMI output to be non-HDCP validated, and decrypted HD content is streamed out to non-secure device. This device then re-encodes the content without protection.
Protection	*agile*GLITCH is able to detect voltage glitching on multiple supplies if desired. This means that glitch attacks on secondary supplies, and analog IP supplies, can also be protected against.

3.5 Hotel safe – bypass safe operation

Device	Hotel electronic safe
Scenario	Service personnel enters hotel room to clean, and is able to open the safe and extract contents without leaving any trace in the access log, and without changing the set code.
Result	Malicious staff member is able to open hotel safe and remove valuables with no trace left.
Exploit	Malicious staff member uses key-code entry device to test all combinations of key code. Before the lockout timer is triggered for each attempt, the supply is glitched to prevent the failed attempt or lockout being recorded.
Protection	*agile*GLITCH is able to detect the power supply being glitched, and is able to flag to the secure microcontroller that semi-regular and suspicious power resets are occurring. This knowledge then triggers a 4-hour lockout, protecting the contents from further attack.

3.6 USB eWallet – access bitcoin private keys

Device	USB key crypto e-wallet
Scenario	User carries all their crypto private keys, plus passwords, on a secure USB key. User loses their USB key, but is not confirmed as USB key is protected by password.
Result	Criminal who acquires the USB key is able to empty user's crypto wallets.
Exploit	Criminal uses voltage glitcher to bypass password check by timing glitch to coincide with password check test Do we want to use this text saying how to bypass password??.
Protection	*agile*GLITCH is able to detect the power supply being glitched, and is able to wipe contents of USB key, thus preventing secrets from being discovered.

3.7 Hardware compromise – disturb workload/trusted boot

Device	Industrial Equipment or Data Centre Server
Scenario	Malicious entity gains access into power supply unit of a complex system ((e.g. server, industrial equipment) though software attack and/or non-trusted hardware.
Result	Remote control of power system allows a third-party to glitch or manipulate the supply, and either disturb workloads, or bypass trusted boot to gain full control of system
Exploit	The power delivery system is infiltrated by a nefarious party, and additional functionality is added which allows the power to be manipulated remotely.

	The system goes to production, and then a malicious entity is able to remotely manipulate the security by resetting/glitching through the power sequence.
Protection	*agile*GLITCH is able to detect the power supply being glitched/modified/manipulated, and is able to signal to the CPU/wider system that nefarious activity is suspected. In separated systems, the device could depower itself, or revert to a safe mode until it is addressed by a maintenance team.

4 Conclusion

There are a very wide variety of exploits available for modern devices. Many vulnerabilities are software related and as these are identified and patched, the physical hardware susceptibilities will become an increasingly important attack vector.

More notable than this, although devices can be remotely patched for software vulnerabilities, hardware vulnerabilities usually require a hardware replacement to address them – thus leaving millions of devices at risk of exploitation.

We have shown that using just the *agile*GLITCH sensor can provide protection from hardware attack vectors. For more comprehensive coverage from suspect activities, the *agile*SCA (Side Channel Attack) monitors and reports Voltage Glitches, Temperature changes and clock manipulation in a single IP core at a very low silicon cost