How a voltage glitch attack could cripple your SoC or MCU – and how to securely protect it

- *Hackers and organized crime gangs can make large profits from selling devices which bypass the authentication process in secured electronics products*
- *A voltage glitch attack is one of the simplest and cheapest ways to compromise a product's security*
- *A voltage glitch detector is a simple, low-cost part of the armory which can protect any connected electronics device*

The danger posed to electronics devices by voltage glitch attacks

Hackers and criminals have an array of techniques available to them to intrude into, tamper with, disable or destroy electronics products and services. Some of the techniques are invasive, and call for very expensive equipment and deep engineering expertise to analyze and modify nanoscale electronics circuitry. To justify the cost and effort involved in launching an invasive attack, the target must offer the promise of a very high reward – normally in financial terms – to the attacker.

Hacking, however, does not have to involve complex engineering and racks of specialist equipment. Some attacks can be performed cheaply and easily, which means that almost any connected product is potentially vulnerable to them.

The voltage glitch attack is one such technique. All it requires is sufficient electronics engineering know-how to inject a momentary, high-voltage pulse on to a power rail of the target device, ideally at a precisely timed point in the device's operation. If the hacker succeeds in timing the pulse correctly, the resulting glitch could be enough to:

- jolt a vulnerable device out of its normal security routine, skipping an authentication process which secures the device against unauthorized access;
- corrupt data read from an external memory device;
- induce the system to incorrectly decode instructions in the device's firmware.

The rewards can be rich for successful attacks: for instance, black-market devices which bypass the security of conditional access products such as pay TV set-top boxes can be sold at a large profit to consumers who want to access entertainment services without paying the service provider.

But attempts to perform voltage glitch attacks may be made on almost all kinds of connected device in order to gain access to other devices on a shared network.

Fortunately, it is possible to embed protection against glitching attacks into a silicon chip. Various layers of technology can protect a chip at both the hardware and software level. And one of the most important elements of a chip's defenses, voltage glitch detection, can be implemented with IP provided by INVIA.

Here we explain the operation of a voltage glitch attack, and the ways in which it can be reliably repelled.

What is a voltage glitch attack and how is it performed?

The basic principle of a voltage glitch attack is that a short transient voltage – a spike of a typical magnitude ranging from 1V up to several tens of volts, and lasting just a few nanoseconds – coupled into a device's power supply can be sufficient to disrupt the normal cycle of firmware execution, without doing permanent damage to the circuitry.

This disruptive power event can cause the device to behave in an abnormal way – for instance, to skip a few lines of boot code. If the voltage glitch attack can be timed to force the code to skip at exactly the point at which it would perform user authentication, for instance by asking for a PIN code, it can provide a cheap and simple way to bypass a device's security functions.

The methods of implementing voltage glitch attacks are in the public domain and well known to hackers and cyber-criminals. Successful voltage glitch attacks on early versions of Microsoft's Xbox 360 and Sony's PlayStation3 games consoles are documented in academic literature [1].

The equipment required to design a successful voltage glitch attack on a target device is simple and relatively cheap. Hackers can use a standard, commercial FPGA development board to control the power input to the target board, a hobbyist's breadboard for making connections between the FPGA board and the target, and some basic circuit assembly tools to remove components such as decoupling capacitors from the target.

What does a device manufacturer need to do to protect against glitching attacks?

The key to protecting a device is to know when a glitch attack is being attempted.

Many physical security measures, such as anti-tamper protection on the enclosure of the product, can be disabled or bypassed. After evading or disabling any anti-tamper protection, the attacker has access to the chip's pins and so can launch a glitch attack.

If physical measures to prevent a glitch attack from being attempted are bypassed, how can a chip be reliably protected? The answer is by a combination of **detection** and **resilience**, so that the chip's systems know when an attack is being attempted, and then implement procedures to recover securely from the attack.

As described below, glitch attacks can reliably be **detected** with special circuitry – a voltage glitch detector – provided as IP by INVIA.

Resilience can be achieved by building redundancy into the hardware and software architecture of the chip. This ensures that, on detection of an attack, the chip can automatically resume safe operation by switching to unimpaired redundant hardware and software blocks.

How should I implement voltage glitch detection?

The only way to guarantee the security of the voltage glitch detection circuitry protecting an SoC or microcontroller is to implement the detector on the chip itself. An external device could monitor power levels on the system board, but the interface between the detector and the at-risk IC would itself be vulnerable to tampering and intrusion.

This means that voltage glitch detection should be implemented as an IP block in the chip's circuitry. There are two forms of glitch detection IP: digital and analog.

A digital voltage glitch detector can be implemented within the host system's logic. IC designers should consider, however, that a digital IP block for voltage glitch detection is itself theoretically

vulnerable to attack, for instance by clock glitching. A digital implementation also typically consumes more power than the equivalent analog circuit.

The inherent advantages of analog circuitry in voltage and current sensing applications led INVIA to develop an analog IP block for voltage glitch detection. Compared to a digital detector, an analog voltage glitch detector is more robust and consumes less power. In fact, it is essentially a zero-power block, as its power consumption results only from leakage current. And because it is an analog circuit, it is also intrinsically hardened against any fault injection attack such as clock glitching.

By implementing robust analog detection alongside measures to ensure resilience in the event of an attack, including redundant logic and software blocks, the IC designer can maintain safe operation of the device even in the face of a sustained attempt to perform glitching attacks.

The Voltage Glitch Detector IP from INVIA provides comprehensive protection against power glitching attack. It detects positive and negative supply voltage glitches, and has a slope detection range between 100 MV/s and 2 GV/s.

The detection threshold may be adjusted to suit the requirements of the application at the design stage. On detection of a glitch attack, the detector provides a latched alarm signal.

The INVIA Voltage Glitch Detector is silicon-proven in CMOS processes at 150 nm, 130 nm, 110 nm, 65 nm and 55 nm. It occupies a typical silicon area smaller than 0.02 mm^2.

Conclusion

Voltage glitching is a simple, cheap way for hackers and criminals to perform fault injection exploits on any accessible device. Protection against this attack technique requires layered security: a combination of fast, reliable detection of transient voltage events on the target device's power supply, and redundant hardware and software to ensure the system is resilient to attack.

The Voltage Glitch Detector from INVIA, an analog IP block, provides fast, low-power and secure glitch detection which is intrinsically fault-tolerant. INVIA, a specialist in security and circuit protection IP, provides system integration expertise to support customers in implementing the detector in standard CMOS fabrication processes.

[1] Modern Game Console Exploitation, a paper by Eric DeBusschere and Mike McCambridge