FRANÇAIS ENGLISH

THOR

HARDWARE CYBERATTACKS
USING FAULT INJECTION

WHAT IS THOR

THOR illustrates an "active" hardware attack, bypassing an embedded security mechanism to disrupt a circuit's operation.

Fault injection attacks involve creating faults in electronic circuits via external disruption. This can take place in a number of ways: optically using a laser, electromagnetically, thermally or via the clock in a synchronous circuit or the power supply voltage. The resulting faults disrupt the circuit's operation in order to:

- Bypass security mechanisms: PIN or password checking, access permission management etc.;
- Find secret keys by applying differential cryptanalysis to the embedded cryptography algorithms.

APPLICATIONS

- Game consoles
- PayTV
- Printers
- Coffee machines
- etc.

ABOUT THE DEMONSTRATION

Disruption attacks have been known about for nearly 20 years.
THOR's goal is to show manufacturers a threat source that needs to be taken into account from the development stage of sensitive products.
It demonstrates how a simple, affordable device (hardware costing around €20) on a miniature scale (fitting into a hand) can be used to bypass a PIN check in unprotected electronics.

THOR implements a physical attack by disrupting the power supply.
The targeted system carries out a PIN check. With just a slight physical modification to the circuit, an attacker can gain access to protected functions without knowing the PIN.

WHAT'S NEXT?

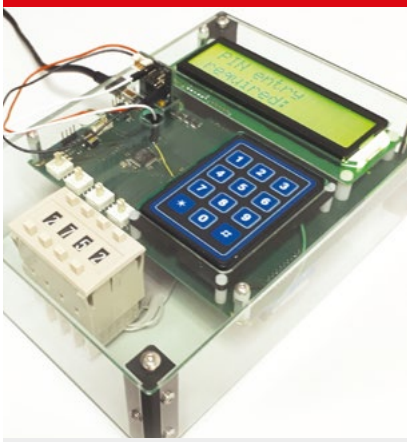
The next version of the demonstrator will illustrate one of the technologies used by CEA-Leti to block this type of attack. One approach relies on the vector instructions provided by some processor cores.

MAIN PUBLICATION

"Thwarting Fault Attacks against Lightweight Cryptography using SIMD Instructions"

Benjamin Lac, Anne Canteaut, Jacques Fournier and Renaud Sirdey

IEEE ISCAS 2018



INTERESTED IN THIS TECHNOLOGY?

Contact:
Marie-Sophie Masselot
marie-sophie.masselot@cea.fr
+33 438 783 830

CEA-Leti, technology research institute
Commissariat à l'énergie atomique et aux énergies alternatives
Minatec Campus | 17 avenue des Martyrs | 38054 Grenoble Cedex 9 | France
www.leti-cea.com
@CEA_Leti CEALeti CEA-Leti