RANSOMWARE BASED ON HARDWARE TROJANS

Forget the typical Ransomware, you should start worrying about hardware

H. Martin[1], P. Peris-Lopez[2], L. Entrena[1] and G. Di Natale[3]

[1] Electronic Technology Department, Carlos III University, [2] Computer Sciences, Carlos III University, [3] *Laboratoire d'Informatique, de Robotique et de Microélectronique*, Montpellier University,

DEFINITIONS

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users files unless a ransom is paid.

A **Hardware Trojan** is a malicious intentional modification of an electronic circuit or design, resulting in undesired behaviour under specific conditions.

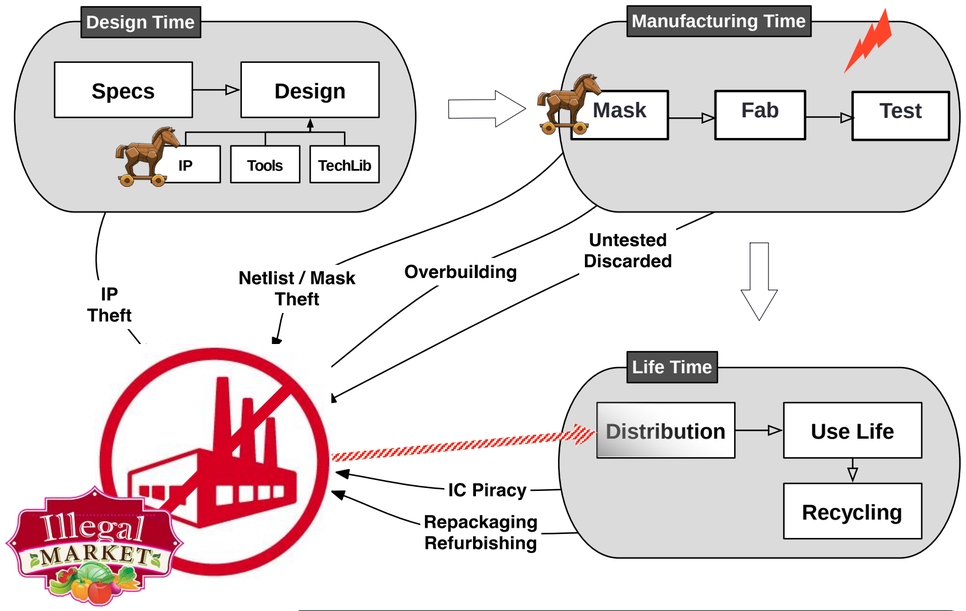
IDEA

Fabless design houses outsource the fabrication to offshore third-party foundries with advanced process technologies. An attacker in the foundry could insert Trojans into a design by manipulating the lithographic masks.

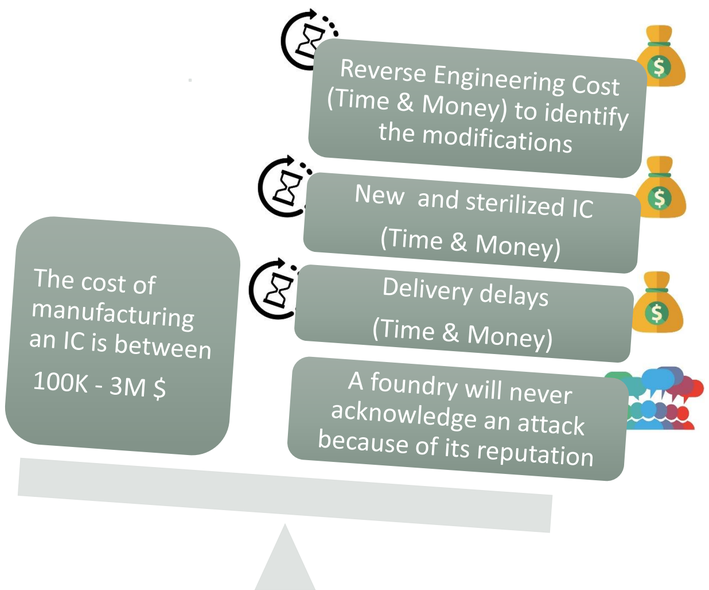
A **rogue employee** at the **foundry** will introduce a HT in the circuit. This HT will lock the operation of the circuit until a key is introduced (malicious logic locking). Unlike typical HTs, the purpose of this HT is **to be detected** during the post-manufacturing tests in order to **claim a ransom** to the foundry.

	Trigger	Payload	Inserted	Physical Charact.
Our HT	Always On	Denial of Service	Manufacturing phase	Don't Care

VULNERABILITIES IN THE DESING/MANUFACTURING PROCESS



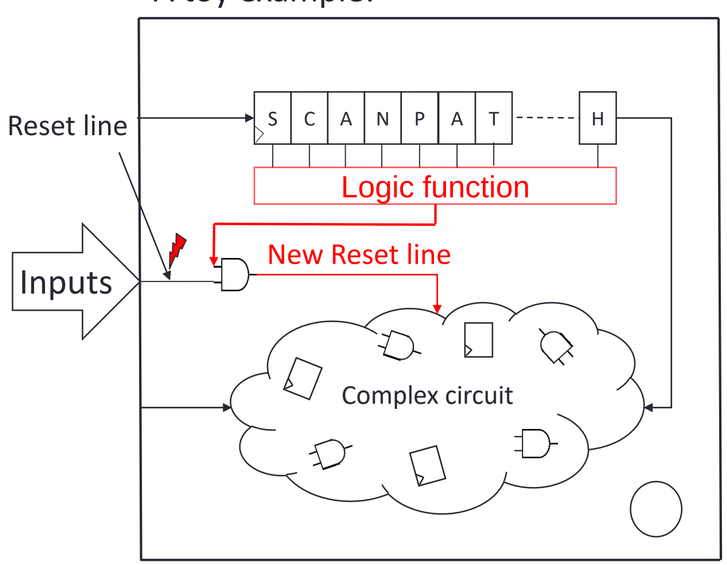
ECONOMICAL IMPACT



A PROOF OF CONCEPT

The target of the attacker will be the reset line of the circuit. Taking advantage of the scan-path registers and a simple logic function, the circuit will be totally functional (no reset) if a key is intruduced through the scan-path.

A toy example:



CONCLUSIONS

After the WannaCry and NotPetya ransomware attacks, many press headlines have been written regarding the danger of these kind of attacks. The move to attacking hardware it is just a matter of time. Unlike software trojans, a HT once is inserted, it cannot be removed. HTs that target IoT devices, fridges, cars or even industrial SCADA systems are a very serious security threat.

From an economic point of view, the hackers not only can extortion the companies but also they can profit by taking advantage of the resulting drop in their stock prices.

K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor. 2016. Hardware Trojans: Lessons Learned after One Decade of Research. *ACM Trans. Des. Autom. Electron. Syst.* 22, 1, Article 6 (May 2016), 23 pages. DOI: https://doi.org/10.1145/2906147

Contact: hmartin@ing.uc3m.es