RANSOMWARE BASED ON HARDWARE TROJANS
Forget the typical Ransomware, you should start worrying about hardware

H. Martin1, P. Peris-Lopez2, L. Entrena2 and G. Di Natale3
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.

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Payload</th>
<th>Inserted</th>
<th>Physical Charact.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our HT</td>
<td>Always On</td>
<td>Denial of Service</td>
<td>Manufacturing phase</td>
</tr>
</tbody>
</table>

ECONOMICAL IMPACT

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 introduced through the scan-path.

Reverse Engineering Cost (Time & Money) to identify the modifications

New and sterilized IC (Time & Money)

Delivery delays (Time & Money)

A foundry will never acknowledge an attack because of its reputation

The cost of manufacturing an IC is between 100k - 3M $

A toy example:

A PROOF OF CONCEPT

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 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.

Contact: hmartin@ing.uc3m.es