Saal: Project 18:30 00:30 Day: 4 Track: Security & Hacking nA 2501

Title: **Hardware attacks: hacking chips on the (very) cheap**

Subtitle: How to retrieve secret keys without going bankrupt

Speaker: **Ramiro Pareja & Rafa Boix**

Short: *Hardware attacks are becoming more and more common. Attacks like Power Analysis or Fault Injection are spread and well known nowadays and the recent hacks to gaming consoles or payment systems are a proof of it. Despite the increasing popularity of these attacks, the cost of the required tools has been unaffordable for most security enthusiasts. Projects like Chipwhisperer have significantly decreased the price of a hardware-hacking setup even below the 1000 barrier, but it still can be too high for hackers that only wants to experiment for fun. We want to prove that money is not a concern if you want to introduce yourself to hardware hacking. Is it possible to perform side channel analysis or fault injection attacks with only 30 euros?*

Long: In our lecture we will introduce the audience to advanced hardware attacks like side channel analysis or fault injection. We will also show how it is possible to perform those attacks using a cheap setup based on a 20 microcontroller board and some spare hardware parts. Some of the attacks we will show include Voltage and Clock Glitching to modify the application flow control, Differential Fault Analysis to retrieving the RSA keys stored in a microcontroller and Differential Power Analysis to break DES. All these while spending less money than a night of beers! In addition to the lecture, we will also run a workshop where we will show you more advanced techniques to break into microcontrollers using professional tools. For more information about the workshop check "Hacking hardware like a pro" workshop