Cryptographic Engineering Research Group
Presents

ECE DEPARTMENTAL SEMINAR

Fault Injection on Secure Boot

Friday, September 27th, 2013
2:00 pm — 3:00 pm
Engineering Building Room 2901

Speaker: Jasper van Woudenberg
Chief Technology Officer North America,
Riscure North America

Abstract:

In this presentation, we cover how secure boot is typically implemented, and how fault injection is used to circumvent it. We explain how the different modes of faults work (power, EM, optical). Next, we discuss good and flawed countermeasures against fault injection. Finally, we extrapolate embedded system hardware attack progression by drawing parallels to state-of-the-art attacks on smart cards.

Biography:

Jasper van Woudenberg is CTO of Riscure North America. His interest in security matters was first sparked in his mid-teens by reverse engineering code. During his studies for a MSc degree in both CS and AI, he worked for a penetration testing firm, where he was introduced to a variety of matters regarding reviewing and testing application and network security. At Riscure, Jasper's expertise has grown to include various aspects of hardware security; from design review and logical testing, to side channel analysis and perturbation attacks. He has a special interest in combining AI with security research. Jasper spoke at conferences such as BlackHat and HAR2009, and presented scientific research at conferences including CT-RSA'11 and FDTC'11, and gives invited talks at universities including Stanford.