Thwarting Evil Maid Attacks:
Physically Unclonable Functions for Hardware Tamper Detection
** GE-117, 1500-1600, 19 June 2014 **

Abstract: Increasingly, users and their computing hardware are exposed a range of software and hardware attacks, ranging from disk imaging to hardware keylogger installation and beyond. Existing methods are inadequate to fully protect users, particularly from covert physical hardware modifications in the “evil maid” scenario, and yet are very inconvenient. Victims include governments and corporations traveling internationally (e.g. China), anti-government activists in places like Syria, and anyone who is a target of a motivated attacker who can gain physical access. Physically Unclonable Functions, combined with a trusted mobile device and a network service, can be used to mitigate these risks. This talk will describe a novel open-source mobile client and network service which can protect arbitrary hardware from many forms of covert modification and attack, and which when integrated with software, firmware, and policy defenses, can provide greater protection to users and limit potential attack surface.

Biography: Eric Michaud is the Founder and CEO of Rift Recon and Director of Hardware Curation at ExploitHub. Michaud has advised on physical security, lockpicking, and hackerspaces for over a decade. He is a professional physical security advisor; an R&D, test and analysis expert; and specializes in forecast and strategy. Michaud started HacDC and Pumping Station: One, is the author of the How To Start A Hackerspace Series, and advises hackerspaces – bringing the movement to over 900 locations worldwide.