Special Joint University of Virginia ECE/CS Seminar

Karsten Nohl

Founder and Director of Research,
Security Research Labs (Berlin)

University of Virginia
Computer Engineering PhD (2009)

Friday, 1 November
3:30-4:45 pm
Rice Hall, Room 130

reception after talk in 4th Floor Atrium

In-Depth Crypto Attacks
"It always takes two bugs"

Real-world cryptographic systems rarely meet academic expectations, with most systems' being shown "insecure" at some point. At the same time, our IT-driven world has not yet fallen apart, suggesting that many protection mechanisms are "secure enough" for how they are employed. This talk argues that hacks with real-world implications are mostly the result of being able to break security assumptions on multiple design layers. Protection designs that focus on a single security function and neglect complimentary layers are hence more prone to compromise. We look at three widely deployed protection systems – from the cell phone, automotive, and smart-card domains – and show how technology abuse arises from the combination of best-practice deviations on multiple design layers.