LABORATORY FOR
COMPUTER SCIENCE

MASSACHUSETTS
INSTITUTE OF
TECHNOLOGY

APPLIED SECURITY READING GROUP

Power Attacks on Cryptographic Hardware

Jonathan Towle, Intertrust

Monday, April 2, 2001
4-5PM NE43-516

Jonathan Towle, a senior engineer from Intertrust, will discuss attacks on cryptographic hardware.

Abstract:

This will be a broad discussion of methods of attacking cryptographic hardware. Attacks can be separated into three main categories: Physical or probing attacks, fault induction attacks, and eavesdropping attacks. Probing attacks are described in several white papers by Ross Anderson's group, see for example Anderson and Kuhn. Fault induction or glitch attacks are discussed by Kömmerling and Kuhn in "Design Principles for Tamper-Resistant Smart Card Processors." Eavesdropping attacks in the form of TEMPEST attacks have been carried out since the 1950s. Recently Paul Kocher and others have studied electrical power consumption of smart card processors and successfully recovered the internally stored secret keys, this will be the main topic of discussion.

Brought to you by the Applied Security Reading Group

`http://pdos.lcs.mit.edu/asrg/`

`asrg-request@pdos.lcs.mit.edu`