

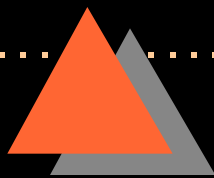
# How to Break a Smartcard

Tom Rowley



# Need for Portable, Secure Tokens

- ◆ Crying need for strong authentication in
  - Health care, entertainment & financial services
- ◆ Face-to-face not possible in e-commerce world
- ◆ Trusted “agents” key part of the value equation

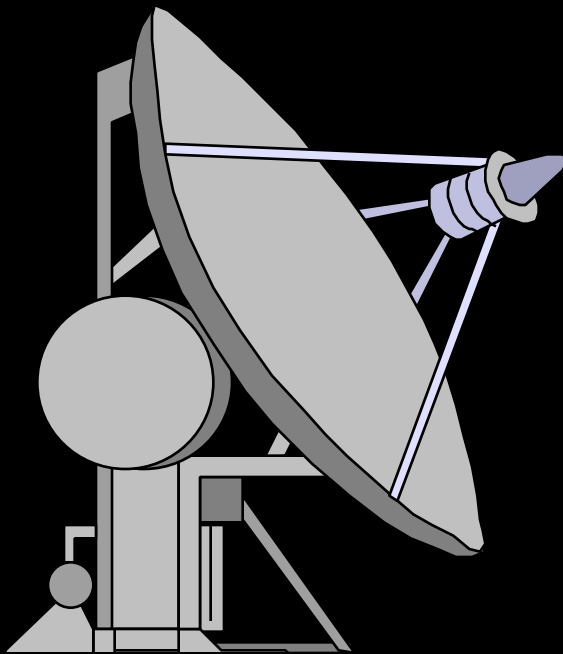


# The Emperor is Naked!



- ◆ Current smartcards are inadequate
- ◆ Vendors deny reality
- ◆ Back to security basics
  - Realistic threat assessment
  - Compromise recovery
- ◆ Appreciate limits of current technology

# Sat-TV - A cautionary tale



- ◆ Unfortunate business model
  - single key compromises the systems
  - long keylife desired
  - low limit on cost
- ◆ 10 compromises in 6 years
- ◆ Substantial lost revenue
- ◆ Dwarfed by banking risk

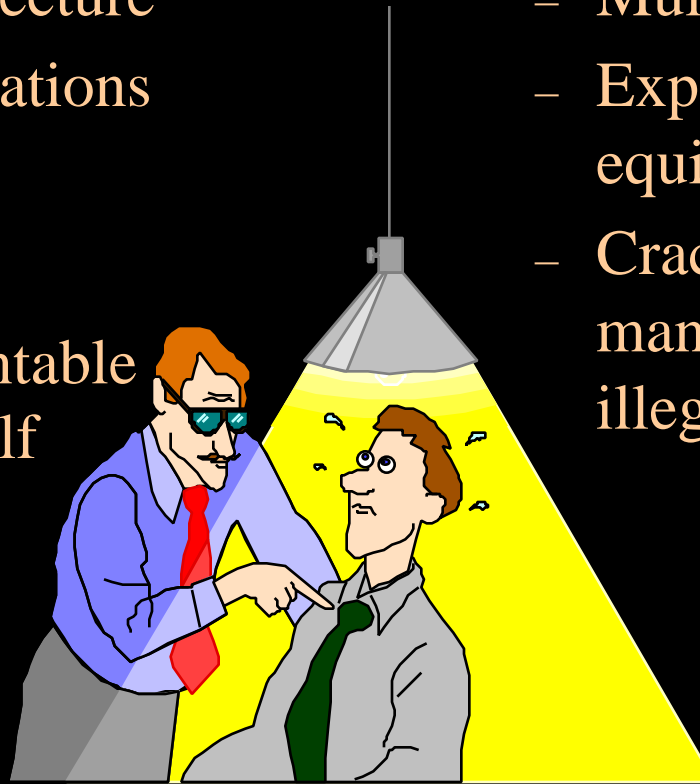
# Attack Methods

## ◆ Exploitive

- Old, slow architecture
- Poor implementations
- Systems flaws
- Trojans
- Crack implementable with off-the-shelf components or software

## ◆ Resource Intensive

- Multi-skill team
- Expensive capital equipment
- Crack requires pirate manufacturing and/or illegal distribution



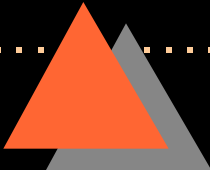
# Exploitable Characteristics



- ◆ Well understood architectures
- ◆ Not designed for tamper-resistance
- ◆ Easily acquired
- ◆ Economic discontinuity
- ◆ Total security implementation
- ◆ Contains a secret key



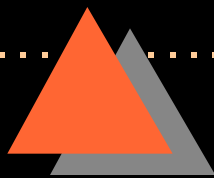
# Exploitable Architectures

- ◆ Old, slow 8-bit “toys”
  - ◆ Large feature sizes ( $\sim 1\mu$ )
  - ◆ Embedded self-test
  - ◆ Exploitable instruction sets
  - ◆ Primitive memory management
  - ◆ Minimal tamper-resistance
- 



# Example, Memory Dumping

- ◆ Most cards have code which copies some portion of memory to the serial port
  - (e.g. answer-to-reset)
- ◆ Changing the pointer or the counter enables the attacker to deliver the contents of memory to the serial port



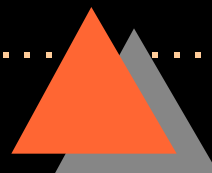
# Physical Attacks



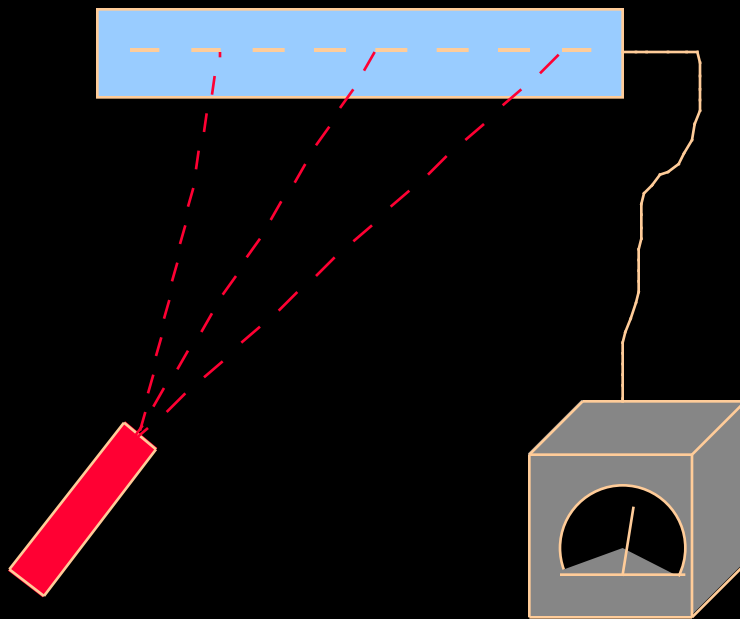
- ◆ Begin by getting access to the chip
  - Chemical solvents remove plastic base
  - Passivation layer removed, plated or bored
- ◆ Use Semiconductor test equipment to analyze to bare device



# ROM Memory Attacks

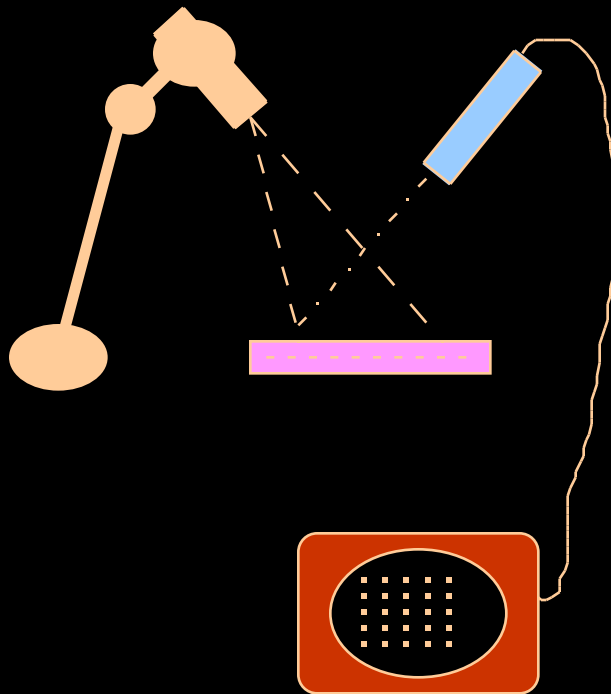
- ◆ Focus of attack is on extracting the smartcard programs & algorithms
  - ◆ Microprobing
  - ◆ Electron Beam scanning
  - ◆ Light Induced Voltage Analysis
- 

# LIVA -Light Induced Voltage



- ◆ Chip is backlapped
- ◆ Scanned by infrared laser
- ◆ Small voltage change depending on transistor state
- ◆ Measured by a precision constant-current source

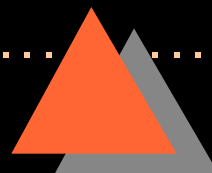
# Electron Beam Scanning



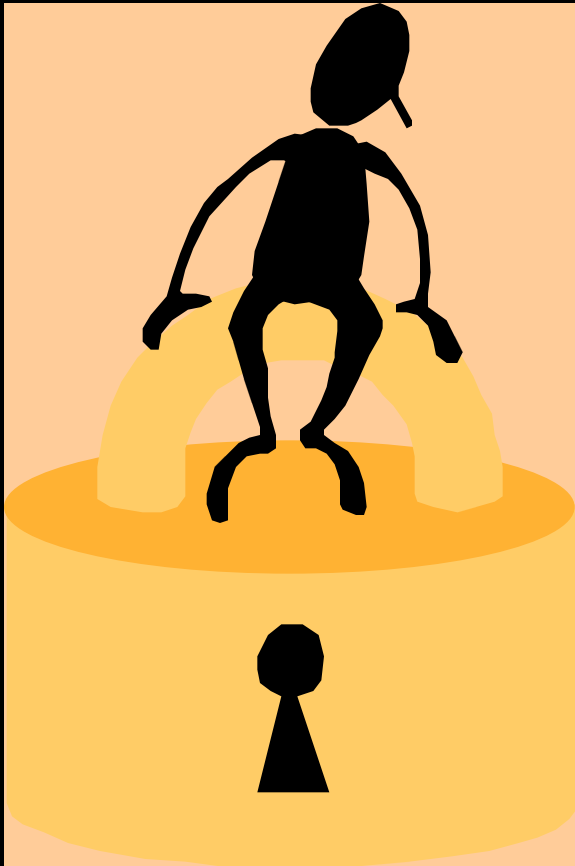
- ◆ Card dissolved and passivation stripped
- ◆ Electron beam directed at area under exam
- ◆ Impact causes release of electrons depending on local potential
- ◆ Layer is image enhanced and displayed



# EEPROM Attacks

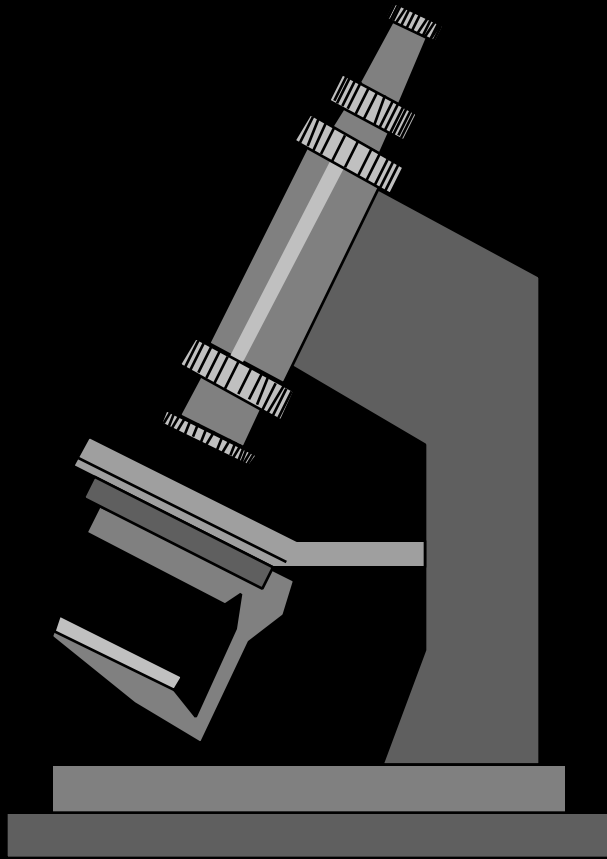
- ◆ Focus of attack is extracting the keys held in EEprom
  - ◆ The data is a charge state on a gate
  - ◆ Read the charge by
    - targeting the row access lines
    - using built-in test circuitry
    - EBT scanning
- 

# Active attacks



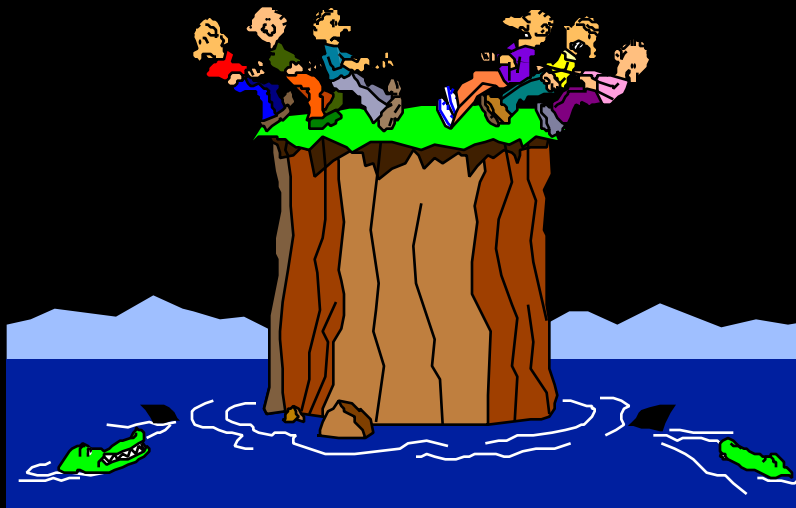
- ◆ Repair protection fuses
- ◆ Modify memory
- ◆ Induce key leakage
  - Bellcore & Shamir results

# Theory or Reality



- ◆ How prevalent are these capabilities?
  - Semiconductor mfg., their suppliers and contractors, major Universities, government labs
- ◆ Well-known cases of reverse-engineering for-hire.

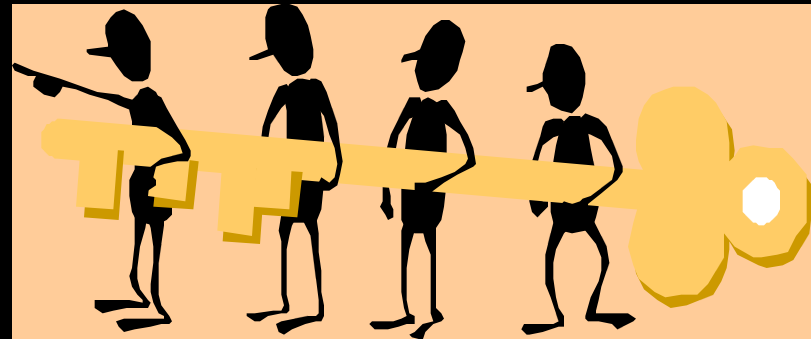
# Infrastructure Attacks



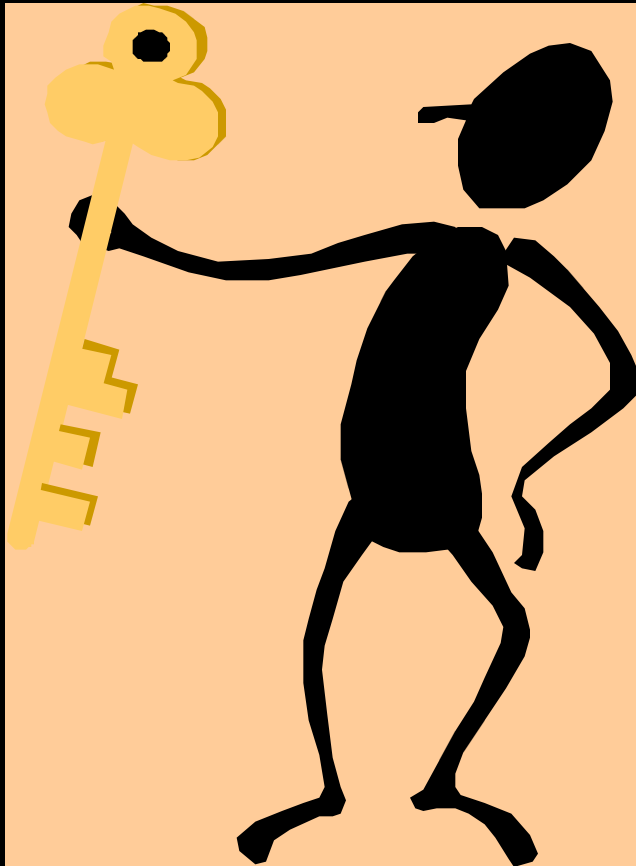
- ◆ Closed implementations without 3rd party review
- ◆ Unknown development environment
- ◆ Unknown manufacturing security

# What to do?

- ◆ Recognize problem
- ◆ Secure microcomputer architectures
- ◆ Tamper-resistant packaging
- ◆ Rapid compromise detection
- ◆ Systems view of security model



# Summary



- ◆ Smartcards **SHOULD BE** an important e-commerce element
- ◆ Current implementations are vulnerable
- ◆ Need realistic expectations of security role
- ◆ Need real crypto-microcomputers