ATTACKS AGAINST MICROCONTROLLERS

DIONISIO PEREZ-MAVROGENIS

SUPERVISOR : KLAUS-PETER ZAUNER

MOTIVATION

- MICROCONTROLLERS ARE EVERYWHERE AND STORE PRECIOUS INFO
  - CRYPTO-KEYS
  - PROPIETARY ALGORITHMS
- ACCESS TO THE FIRMWARE COULD HAVE CONSEQUENCES
  - THEFT OF INTELLECTUAL PROPERTY
  - THEFT OF SERVICE
  - LEAKAGE OF SECRET INFORMATION

ATTACK TYPES

- NON-INVASIVE
  - CHEAP, EASY, NO DECAPSULATION
  - CAN REVEAL USEFUL INFORMATION
- SEMI-INVASIVE
  - TRICKIER, REQUIRE DECAPSULATION, TOOLS REQUIRED
  - PROVIDE MORE INSIGHT
- INVASIVE
  - COMPLICATED, EXPENSIVE, LENGTHY, NEED EXPERIENCE
  - YIELD MOST INFO

ATTACK AGAINST ATMEGA644

- HARVARD ARCHITECTURE
- VULNERABLE TO CLOCK-GLITCH ATTACKS (AMONG OTHERS)
  - OPERATES ON EXTERNAL CLOCK, NO CLOCK REGULATOR
  - 2-STAGE PIPELINE
- CAN GLITCH INSTRUCTION FETCH AND DATA FETCH TO :
  - NOP-OUT INSTRUCTIONS
  - REPLACE DATA HANDLED
  - REPLAY INSTRUCTIONS