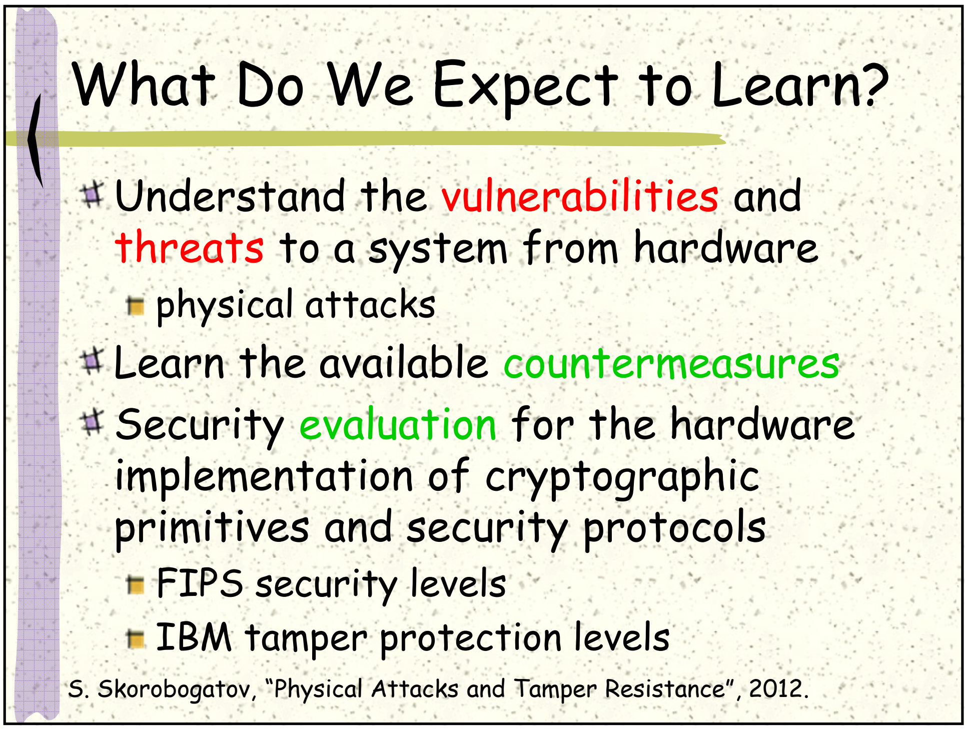
Hardware Security -- Physical Attacks

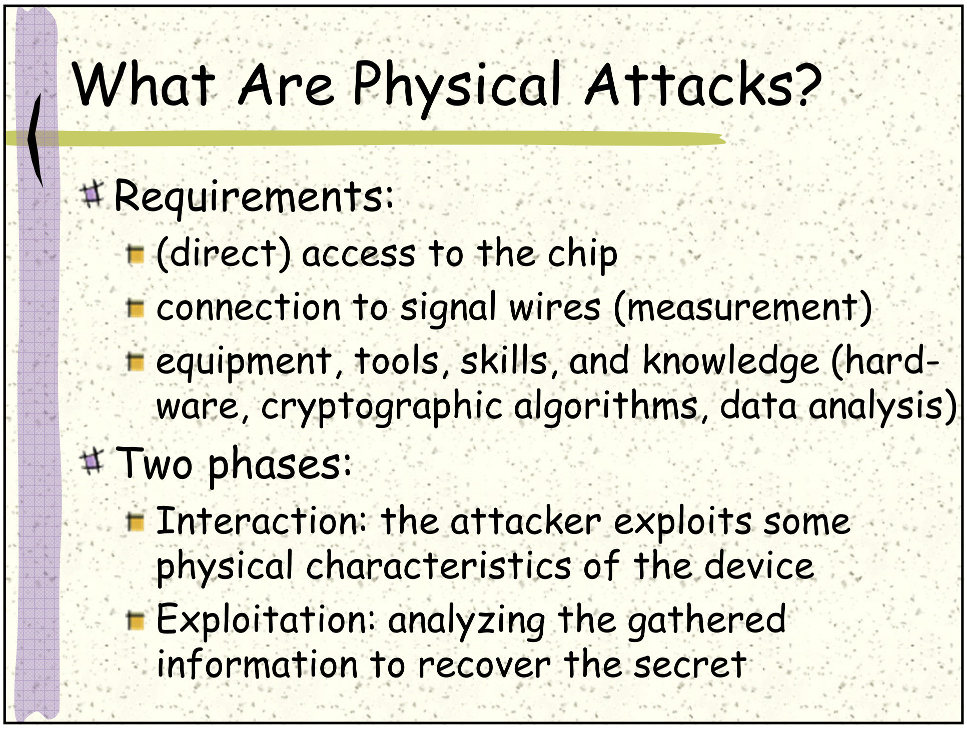
Cybersecurity Specialization



What Do We Expect to Learn?

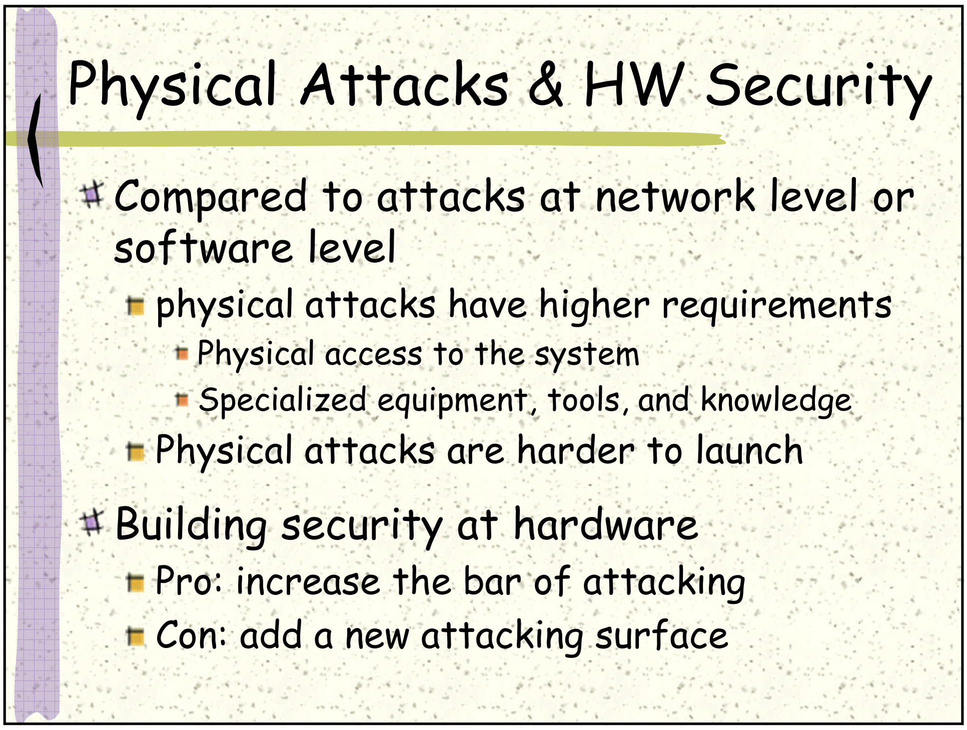
- Understand the vulnerabilities and threats to a system from hardware
  - physical attacks
- Learn the available countermeasures
- Security evaluation for the hardware implementation of cryptographic primitives and security protocols
  - FIPS security levels
  - IBM tamper protection levels

S. Skorobogatov, "Physical Attacks and Tamper Resistance", 2012.



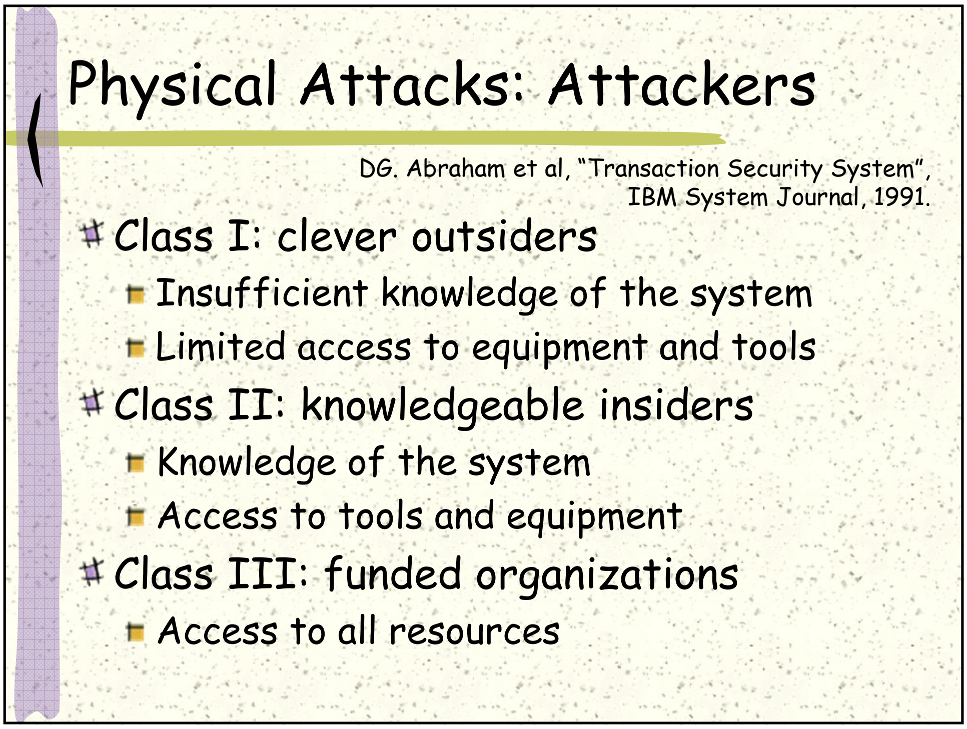
What Are Physical Attacks?

- Requirements:
  - (direct) access to the chip
  - connection to signal wires (measurement)
  - equipment, tools, skills, and knowledge (hardware, cryptographic algorithms, data analysis)
- Two phases:
  - Interaction: the attacker exploits some physical characteristics of the device
  - Exploitation: analyzing the gathered information to recover the secret



Physical Attacks & HW Security

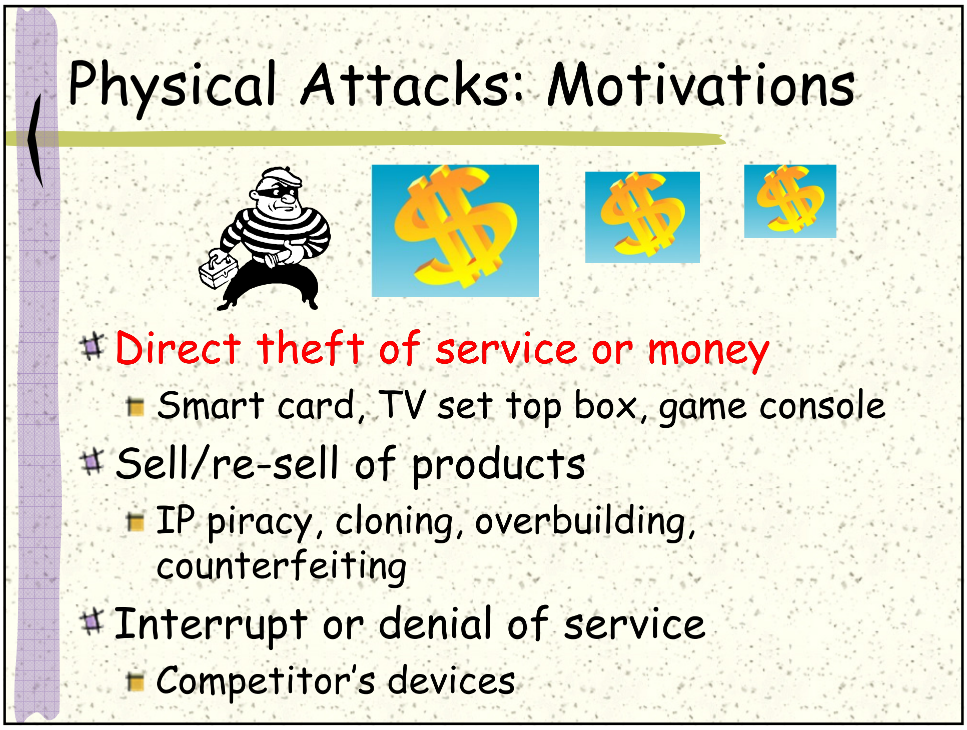
- Compared to attacks at network level or software level
  - physical attacks have higher requirements
    - Physical access to the system
    - Specialized equipment, tools, and knowledge
  - Physical attacks are harder to launch
- Building security at hardware
  - Pro: increase the bar of attacking
  - Con: add a new attacking surface



Physical Attacks: Attackers

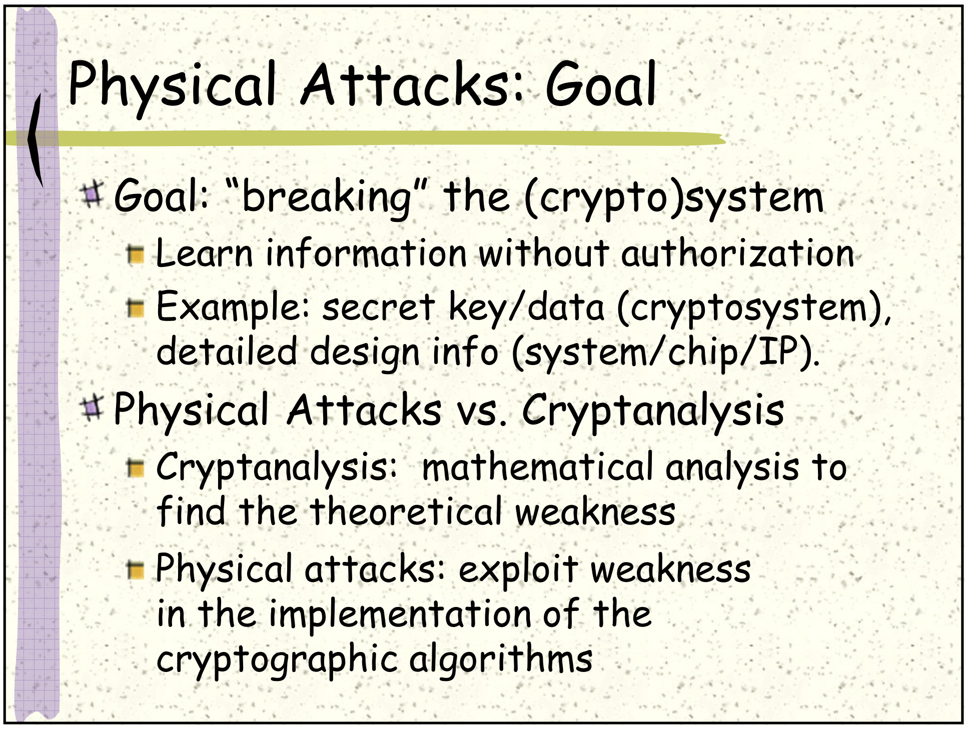
DG. Abraham et al, "Transaction Security System",
IBM System Journal, 1991.

- Class I: clever outsiders
  - Insufficient knowledge of the system
  - Limited access to equipment and tools
- Class II: knowledgeable insiders
  - Knowledge of the system
  - Access to tools and equipment
- Class III: funded organizations
  - Access to all resources



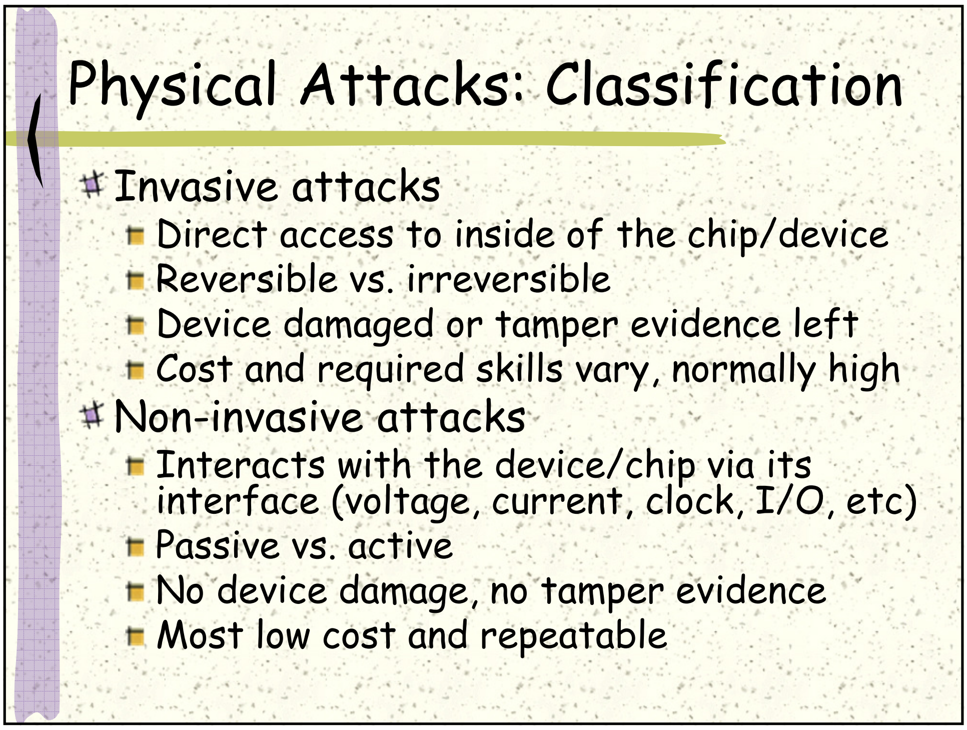
Physical Attacks: Motivations

- Direct theft of service or money
  - Smart card, TV set top box, game console
- Sell/re-sell of products
  - IP piracy, cloning, overbuilding, counterfeiting
- Interrupt or denial of service
  - Competitor's devices



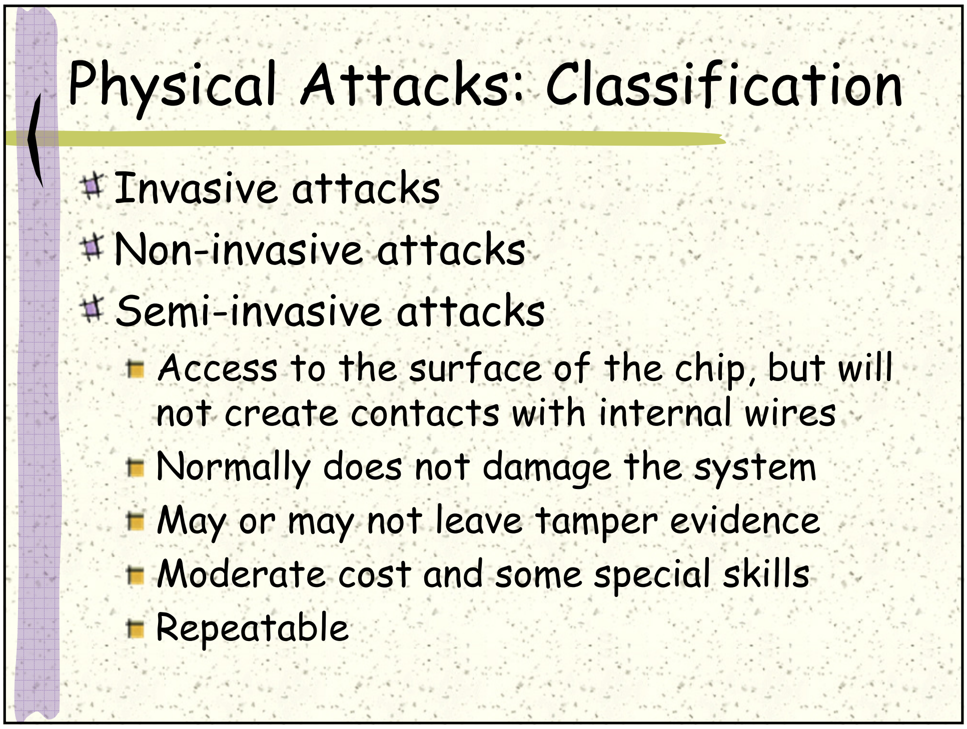
Physical Attacks: Goal

- Goal: “breaking” the (crypto)system
  - Learn information without authorization
  - Example: secret key/data (cryptosystem), detailed design info (system/chip/IP).
- Physical Attacks vs. Cryptanalysis
  - Cryptanalysis: mathematical analysis to find the theoretical weakness
  - Physical attacks: exploit weakness in the implementation of the cryptographic algorithms



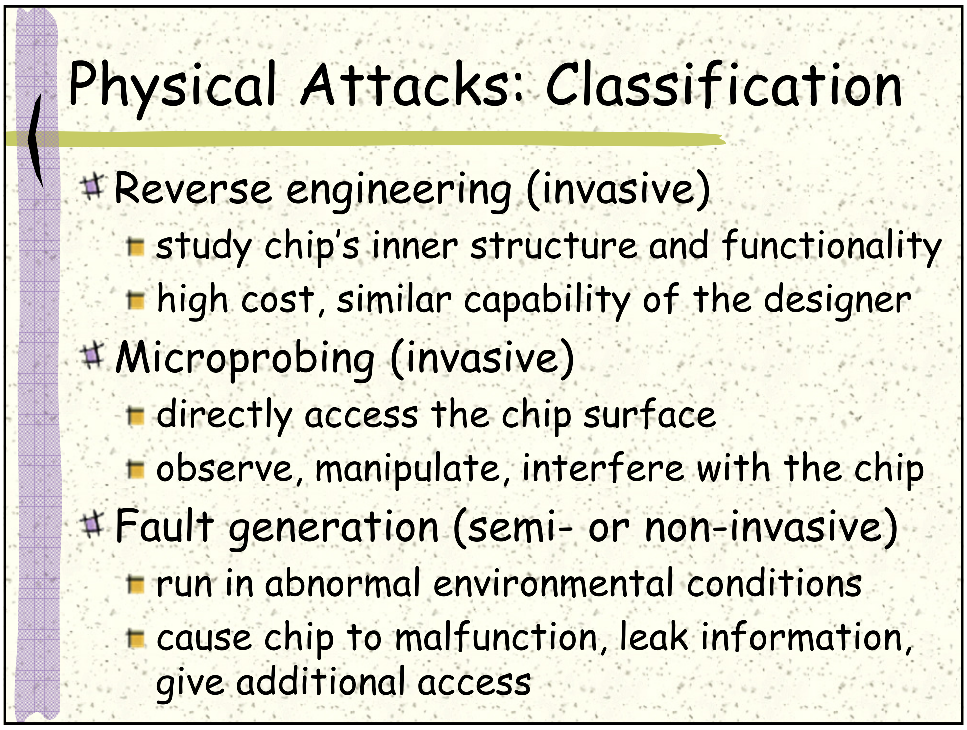
Physical Attacks: Classification

- Invasive attacks
  - Direct access to inside of the chip/device
  - Reversible vs. irreversible
  - Device damaged or tamper evidence left
  - Cost and required skills vary, normally high
- Non-invasive attacks
  - Interacts with the device/chip via its interface (voltage, current, clock, I/O, etc)
  - Passive vs. active
  - No device damage, no tamper evidence
  - Most low cost and repeatable



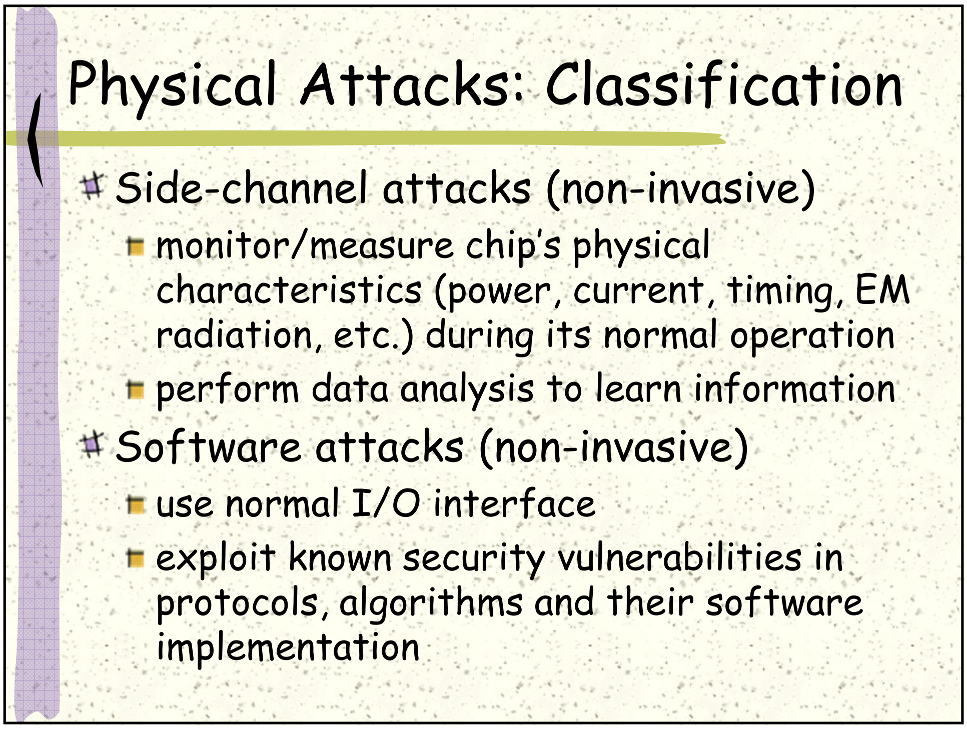
Physical Attacks: Classification

- Invasive attacks
- Non-invasive attacks
- Semi-invasive attacks
  - Access to the surface of the chip, but will not create contacts with internal wires
  - Normally does not damage the system
  - May or may not leave tamper evidence
  - Moderate cost and some special skills
  - Repeatable



Physical Attacks: Classification

- Reverse engineering (invasive)
  - study chip's inner structure and functionality
  - high cost, similar capability of the designer
- Microprobing (invasive)
  - directly access the chip surface
  - observe, manipulate, interfere with the chip
- Fault generation (semi- or non-invasive)
  - run in abnormal environmental conditions
  - cause chip to malfunction, leak information, give additional access



Physical Attacks: Classification

- Side-channel attacks (non-invasive)
  - monitor/measure chip's physical characteristics (power, current, timing, EM radiation, etc.) during its normal operation
  - perform data analysis to learn information
- Software attacks (non-invasive)
  - use normal I/O interface
  - exploit known security vulnerabilities in protocols, algorithms and their software implementation