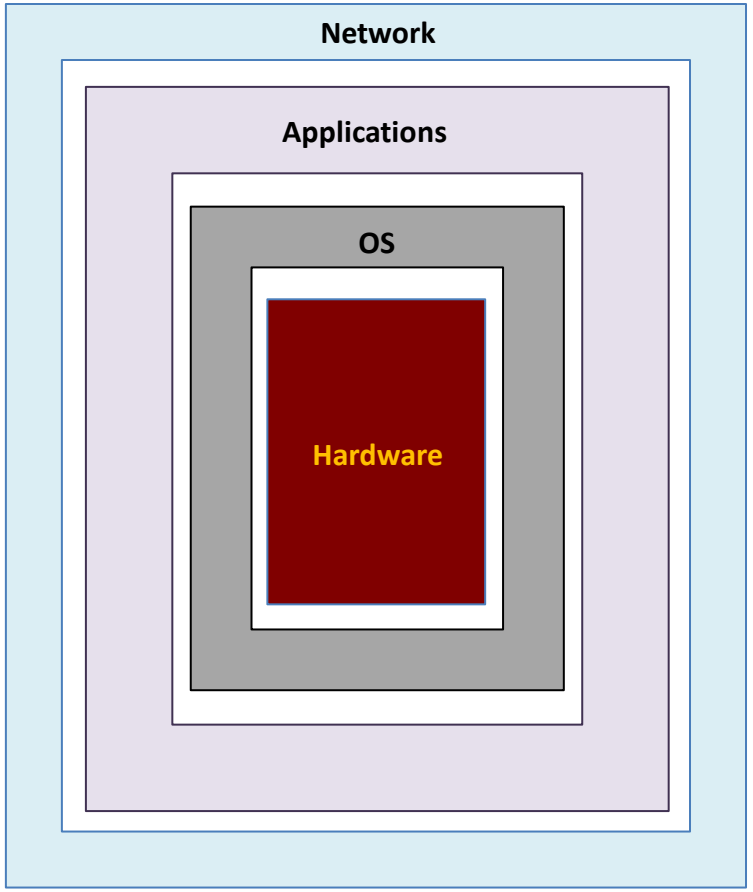
CSE/CEN 598
Hardware Security & Trust

Trusted Digital System Design:
Hardware Watermarking & Random Number Generation

Prof. Michel A. Kinsy

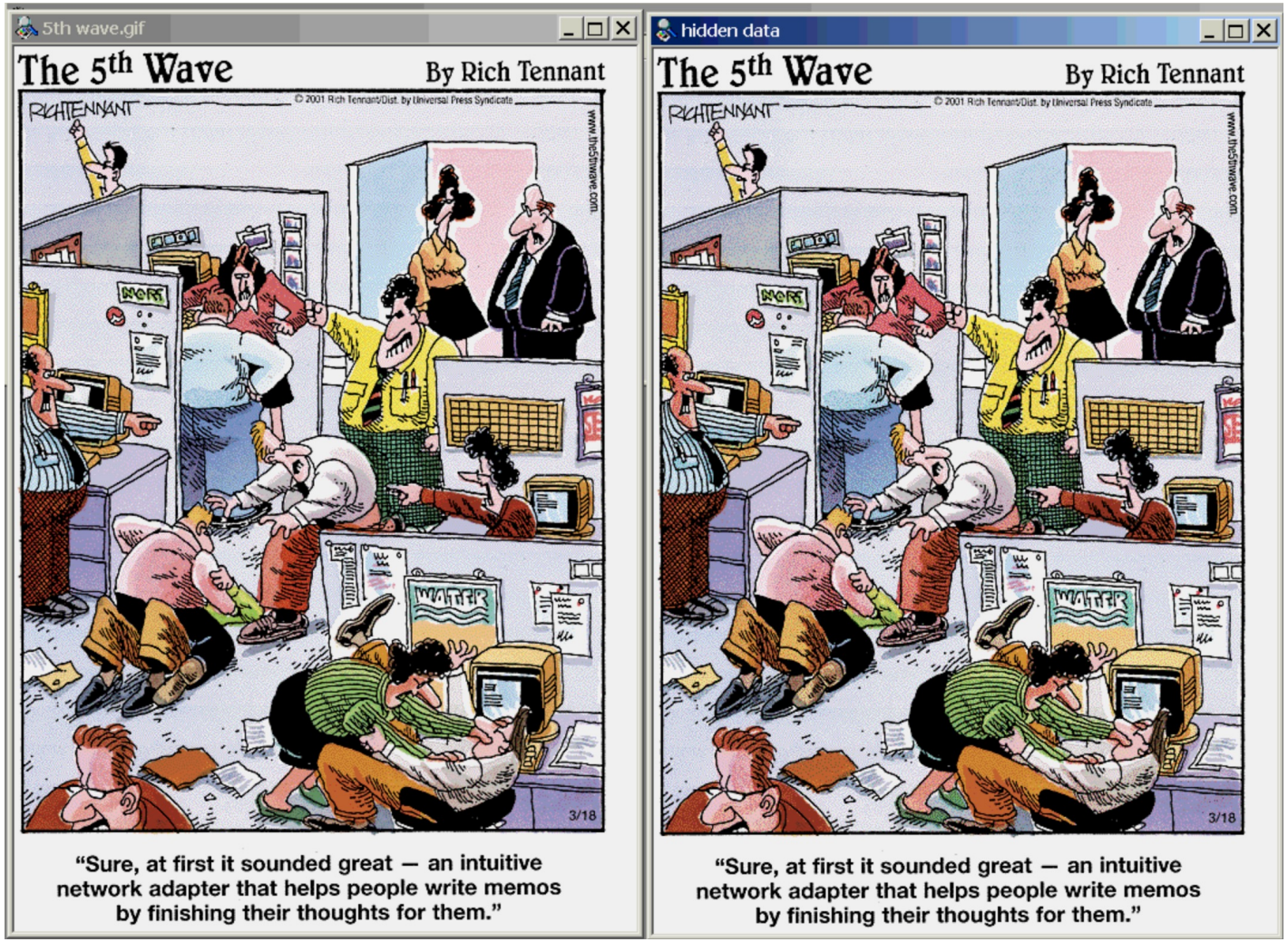
Attacks, Vulnerabilities, and Countermeasures

- Countermeasures
  - Circuit Level
    - Hardware obfuscation
  - Digital Design
    - IC watermarking
  - Datapath & Control
    - Self-repair and regeneration of datapaths
  - Component Level
    - Hardware security primitives (PUF, ORAM, RNG,…)
  - Architecture Level
    - Secure computing architectures
      - Secure heterogeneous system-on-chip (SoC) architectures



Hardware Watermarking

- Hardware/IP watermarking
  - Watermarking can be viewed as an advanced form of Steganography, in which one message is discretely inserted within another, with both messages being linked in some manner.



Hardware Watermarking

- Hardware/IP watermarking
  - Watermarking can be viewed as an advanced form of Steganography, in which one message is discretely inserted within another, with both messages being linked in some manner.
  - Hardware watermarking is a form of digital watermarking
    - Digital watermarking has been around for a while. It is applicable to a diverse range of data types, including images, audio files, and videos.
    - The process entails integrating a specific signature into the data for the purpose of assigning it a distinctive identifier.
  - Hardware watermarking can be visible or invisible and can be invasive or noninvasive

Hardware Watermarking

- Hardware watermarking can be applied to various levels of IP design, such as RTL, Gate level, or GDSII
  - It should not cause any interference with the overall function of the original design
  - It is crucial that any modifications to the data do not result in a change to the intended functionality of the hardware/IP
- Hardware watermarking must be done in a way that:
  - Preserves the functionality of the IP without any noticeable degradation in performance
  - Makes it difficult to detect or remove by unauthorized parties

Hardware Watermarking

- Classes of hardware watermarking approaches
  - Constraint-based watermarking
  - Additive watermarking
  - Others …
- Methodologies for inserting the watermarks
  - Test-based watermarking
  - "Don't Care Condition" watermarking
  - Power Analysis watermarking
  - Placement and Route-based watermarking

Randomness & Random Number Generation

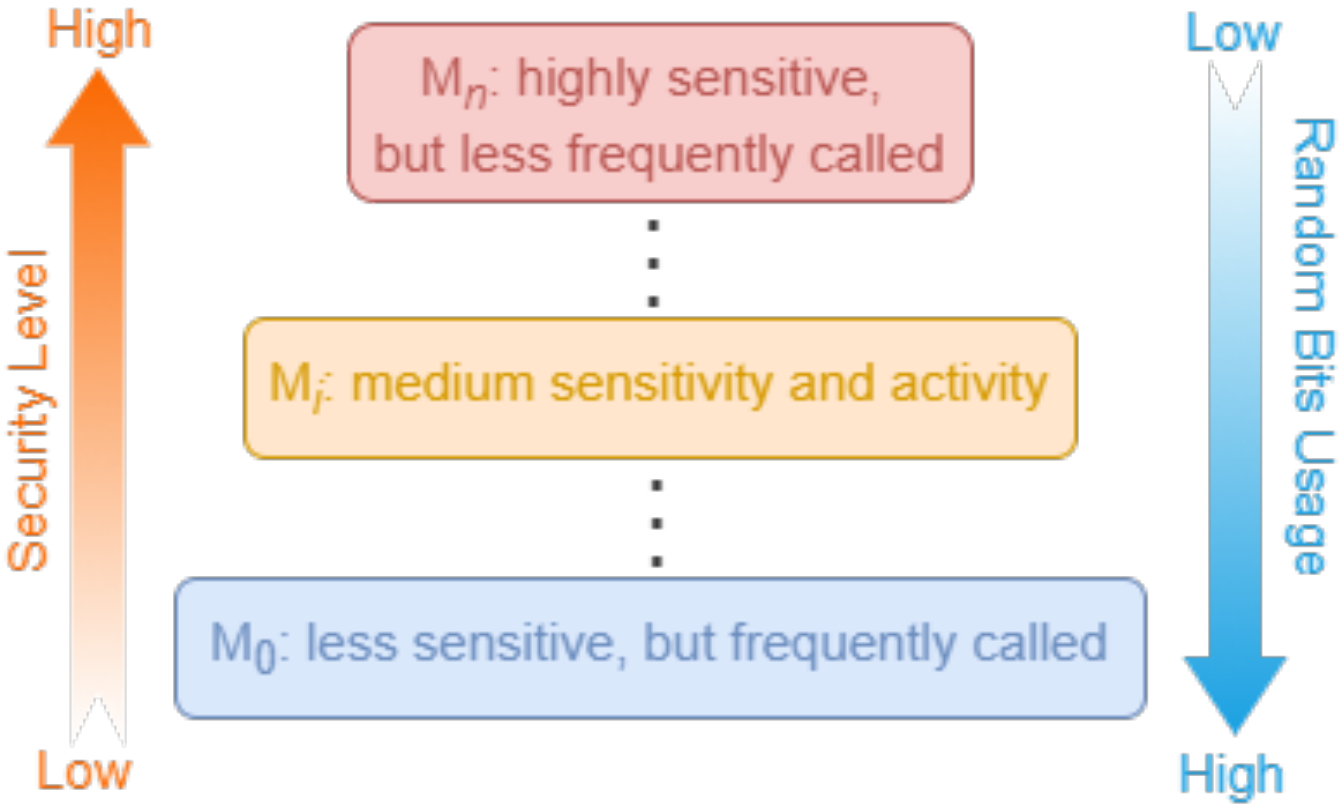
- The importance of random number in computing system security
  - Modern cryptographic applications no longer anchor their trust on the obscurity of algorithms, but instead on the strength of secret vectors (i.e., keys, masks, pads etc.).
  - Randomness and the generation of random numbers is an important building block of designing secure computing systems.
  - What is a random number?
    - Randomness is characterized by the lack of structure or organization and refers to an endless series of numbers that does not adhere to any particular sequence.

Randomness & Random Number Generation

- What is a random number?
  - Randomness is characterized by the lack of structure or organization and refers to an endless series of numbers that does not adhere to any particular sequence.
    - Truly random numbers
      - They are generated as a result of a physical process such as circuit noise.
      - However, truly random numbers face challenges such as being too slow and expensive to generate, low quality, and not reproducible.
    - Pseudo-random numbers
      - Consists of a deterministic sequence with a repeat period but gives the appearance of randomness.
      - This type of random number generation involves the use of a deterministic algorithm to create numbers that seem random.
    - Quasi-random numbers
      - They are almost random in nature.
- RNG hardware security primitive
  - A piece of hardware as a cryptographically secure random number generator (RNG)

Randomness & Random Number Generation

- All these three categories of random numbers are used.
- In certain circumstances, it proves advantageous to replicate a program precisely, utilizing the same sequence of random numbers.
  - Certain cryptography systems rely on PRNG to ensure secure communication between clients and servers, requiring both parties to generate and utilize the same set of random numbers.
  - This is done through properly seeding the number generator.

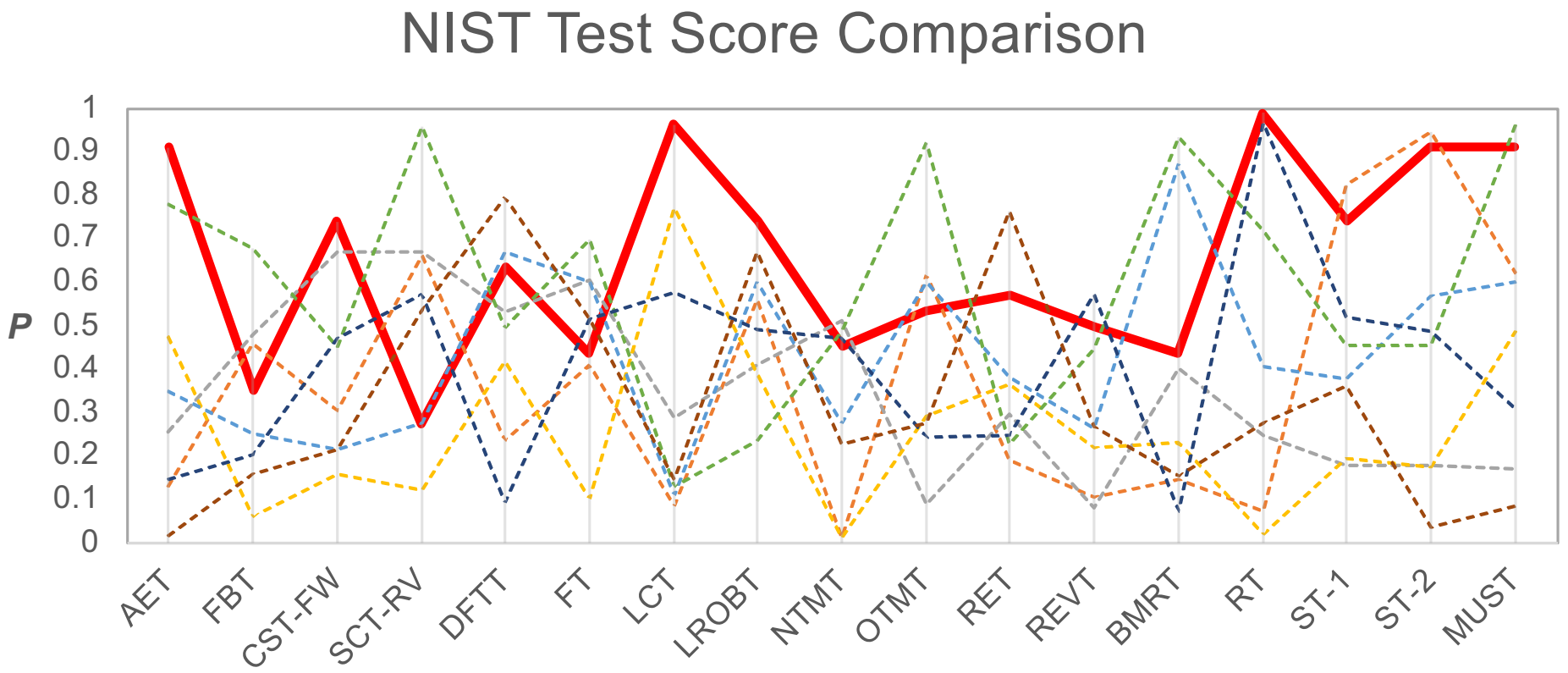


Qualification of Randomness

- National Institute of Standards and Technology (NIST) SP 800-22 Test Suite for Random Number Generators.
- The strict avalanche criterion (SAC) is a formalization of the avalanche effect. It is satisfied if, whenever a single input bit is different, each of the output bits changes with a 50% probability.

Qualification of Randomness

- National Institute of Standards and Technology (NIST) SP 800-22 Test Suite for Random Number Generators.



Upcoming Lectures

- Secure Hardware Primitives
  - Hardware Trojans