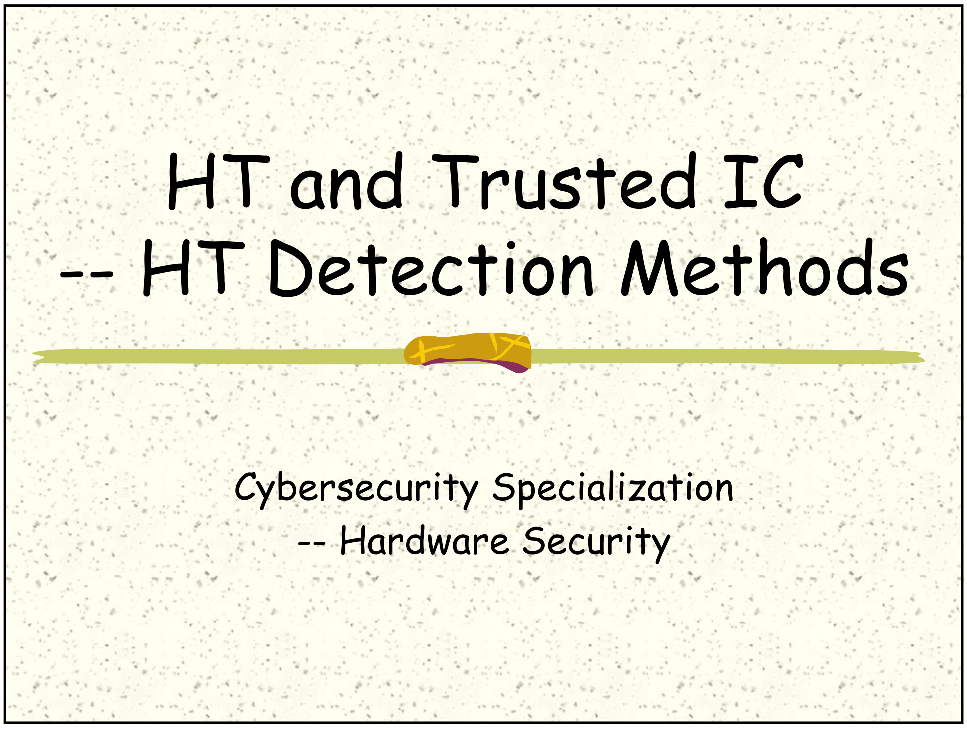
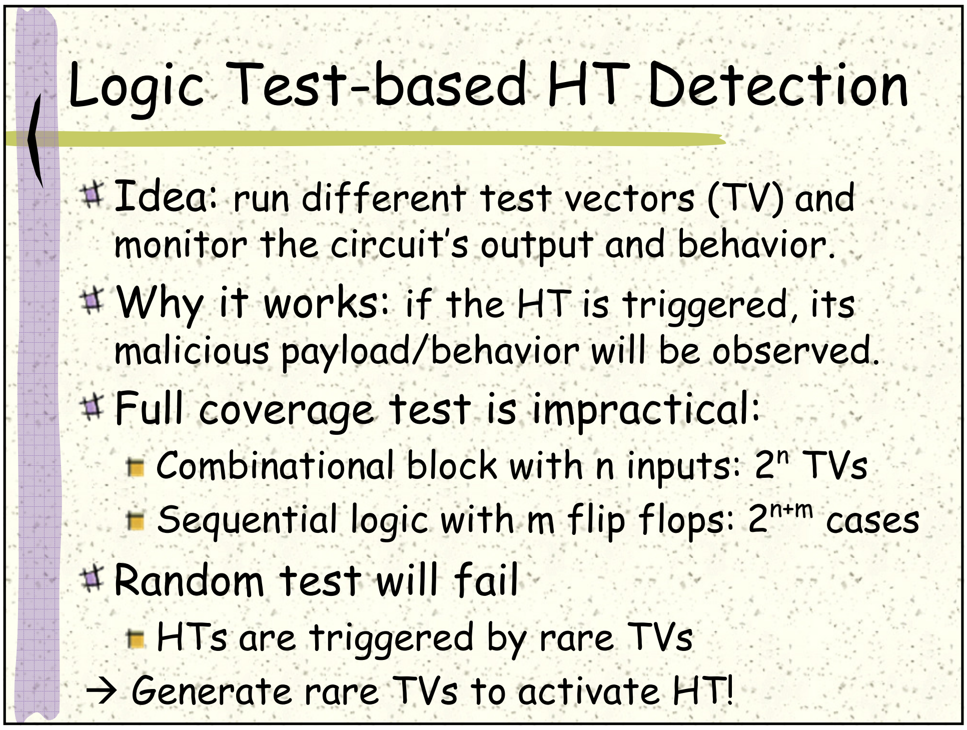


HT and Trusted IC
-- HT Detection Methods

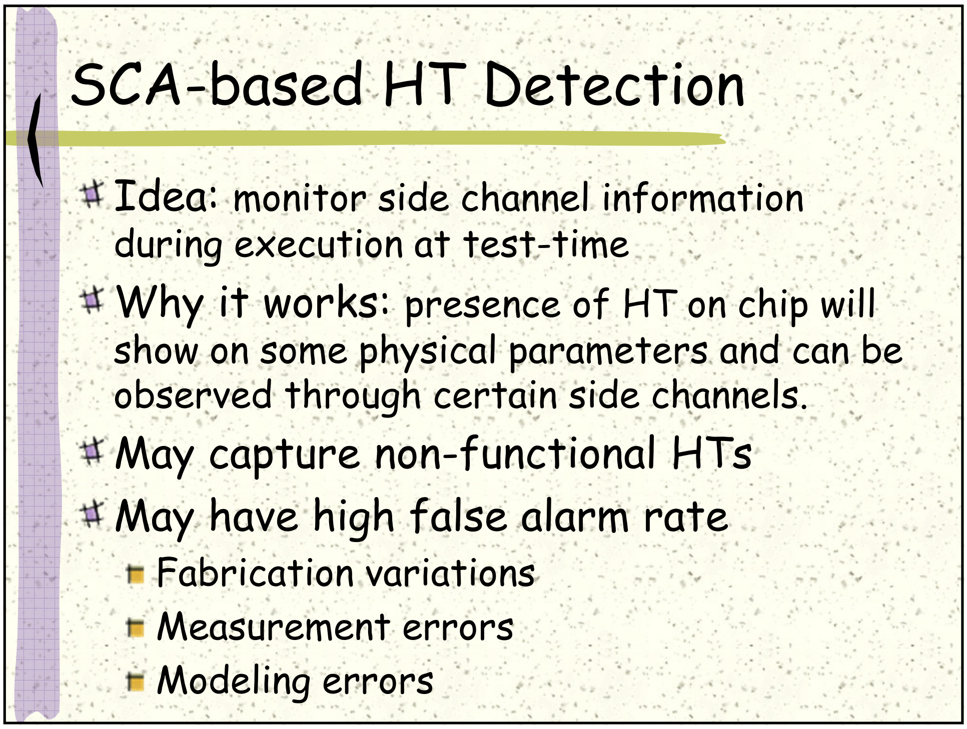
Cybersecurity Specialization
-- Hardware Security



Logic Test-based HT Detection

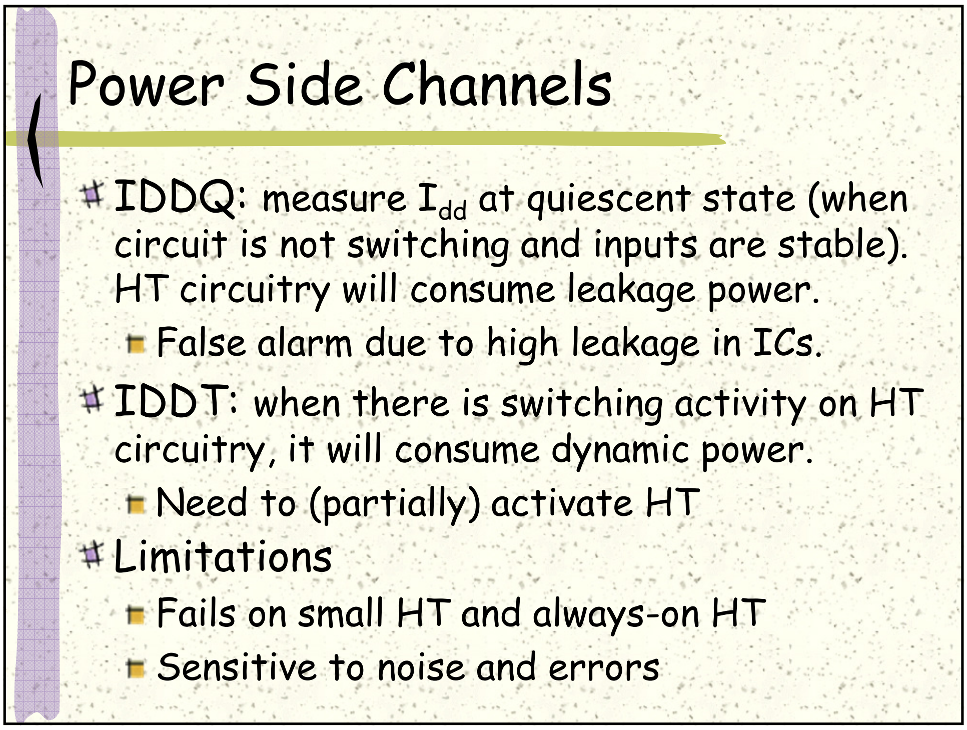
- Idea: run different test vectors (TV) and monitor the circuit's output and behavior.
- Why it works: if the HT is triggered, its malicious payload/behavior will be observed.
- Full coverage test is impractical:
  - Combinational block with n inputs: 2^n TVs
  - Sequential logic with m flip flops: 2^{n+m} cases
- Random test will fail
  - HTs are triggered by rare TVs

→ Generate rare TVs to activate HT!



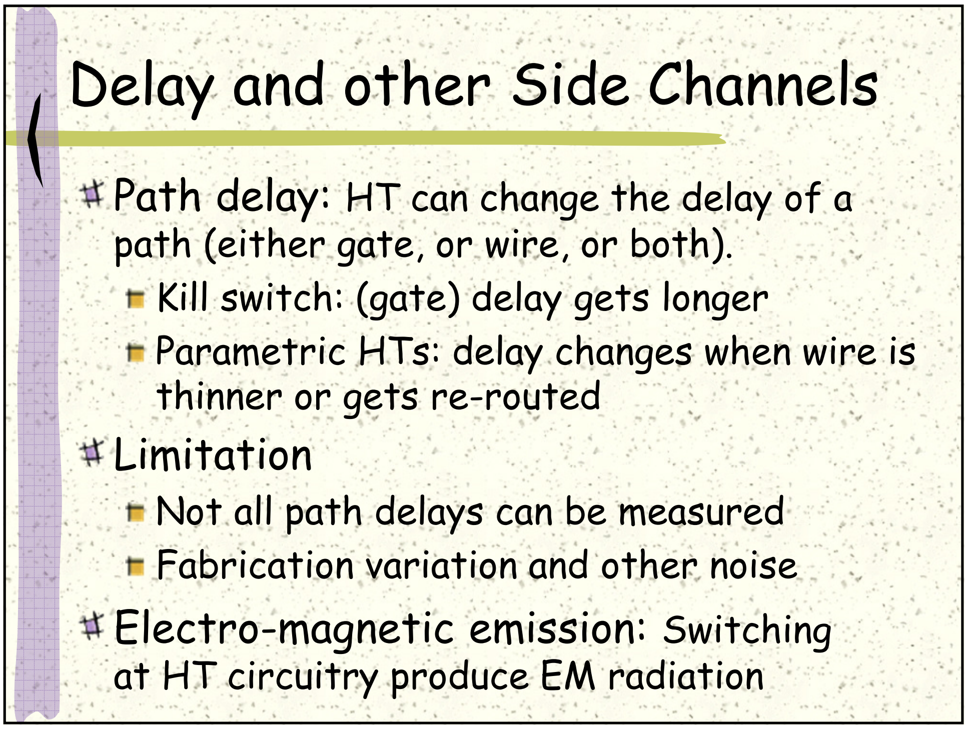
SCA-based HT Detection

- Idea: monitor side channel information during execution at test-time
- Why it works: presence of HT on chip will show on some physical parameters and can be observed through certain side channels.
- May capture non-functional HTs
- May have high false alarm rate
  - Fabrication variations
  - Measurement errors
  - Modeling errors



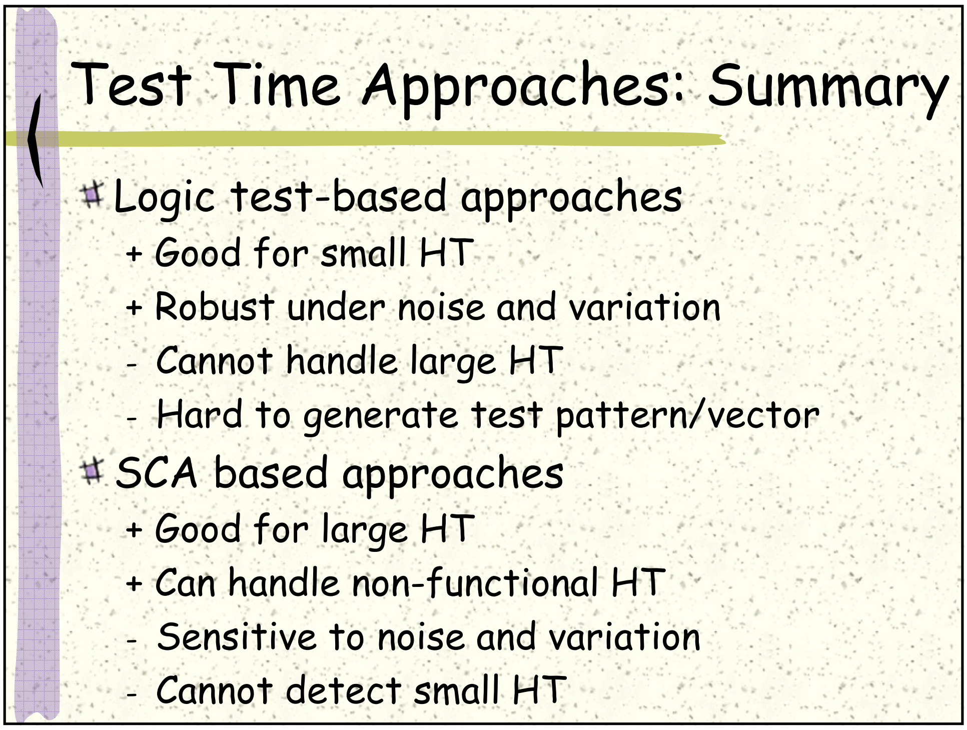
Power Side Channels

- IDDQ: measure I_{dd} at quiescent state (when circuit is not switching and inputs are stable). HT circuitry will consume leakage power.
  - False alarm due to high leakage in ICs.
- IDDT: when there is switching activity on HT circuitry, it will consume dynamic power.
  - Need to (partially) activate HT
- Limitations
  - Fails on small HT and always-on HT
  - Sensitive to noise and errors



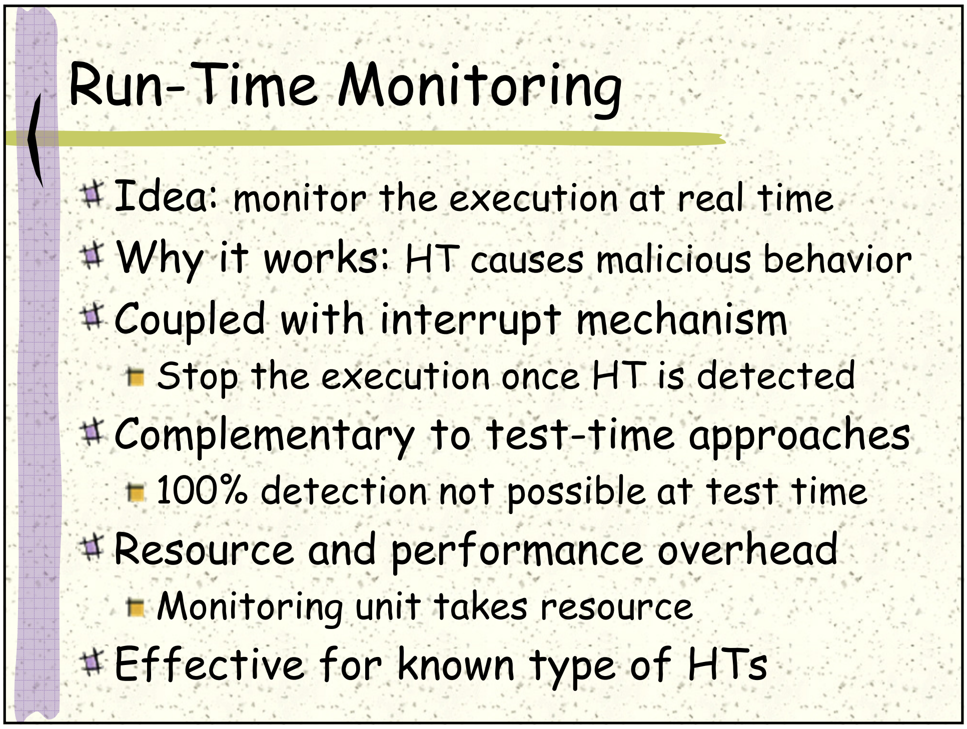
Delay and other Side Channels

- Path delay: HT can change the delay of a path (either gate, or wire, or both).
  - Kill switch: (gate) delay gets longer
  - Parametric HTs: delay changes when wire is thinner or gets re-routed
- Limitation
  - Not all path delays can be measured
  - Fabrication variation and other noise
- Electro-magnetic emission: Switching at HT circuitry produce EM radiation



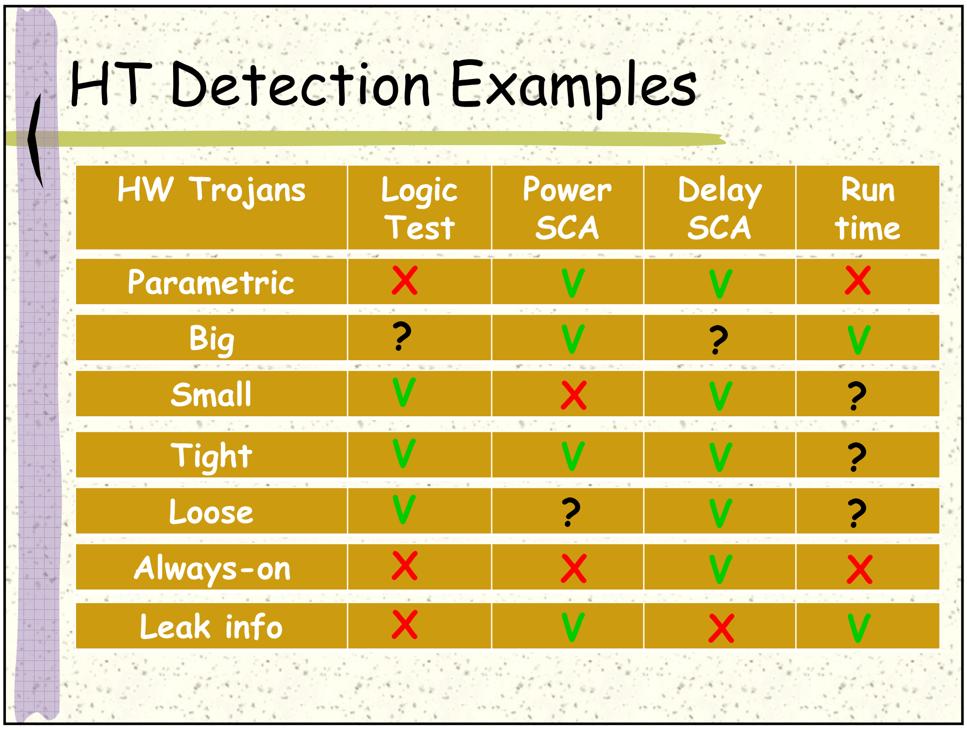
Test Time Approaches: Summary

- Logic test-based approaches
  - + Good for small HT
  - + Robust under noise and variation
  - - Cannot handle large HT
  - - Hard to generate test pattern/vector
- SCA based approaches
  - + Good for large HT
  - + Can handle non-functional HT
  - - Sensitive to noise and variation
  - - Cannot detect small HT



Run-Time Monitoring

- Idea: monitor the execution at real time
- Why it works: HT causes malicious behavior
- Coupled with interrupt mechanism
  - Stop the execution once HT is detected
- Complementary to test-time approaches
  - 100% detection not possible at test time
- Resource and performance overhead
  - Monitoring unit takes resource
- Effective for known type of HTs



HT Detection Examples

HW Trojans	Logic Test	Power SCA	Delay SCA	Run time
Parametric	X	V	V	X
Big	?	V	?	V
Small	V	X	V	?
Tight	V	V	V	?
Loose	V	?	V	?
Always-on	X	X	V	X
Leak info	X	V	X	V