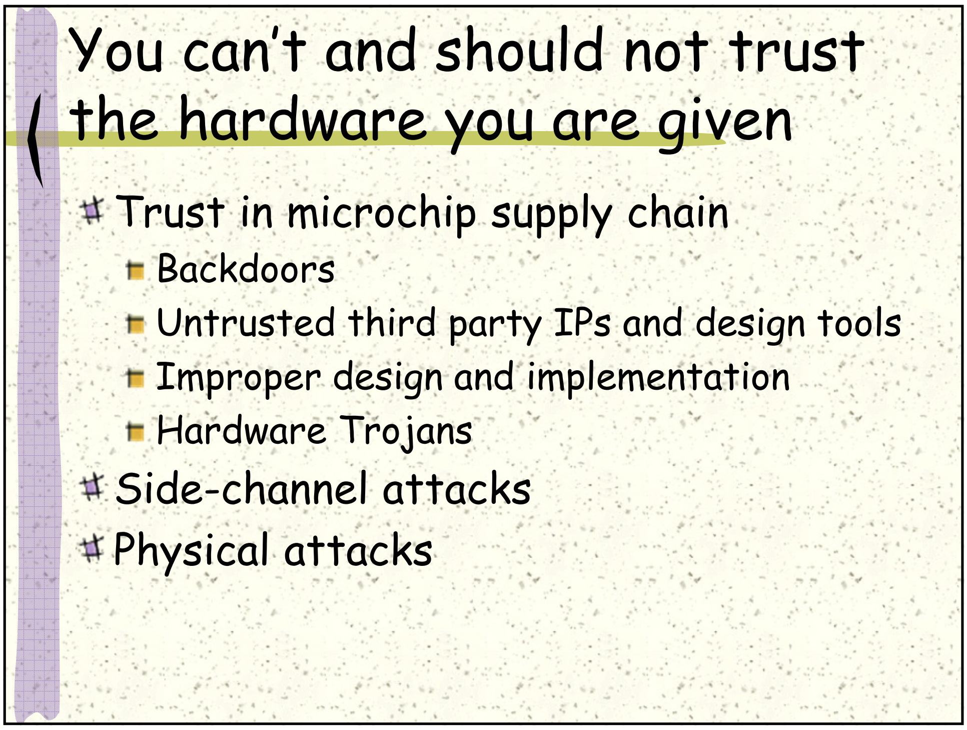
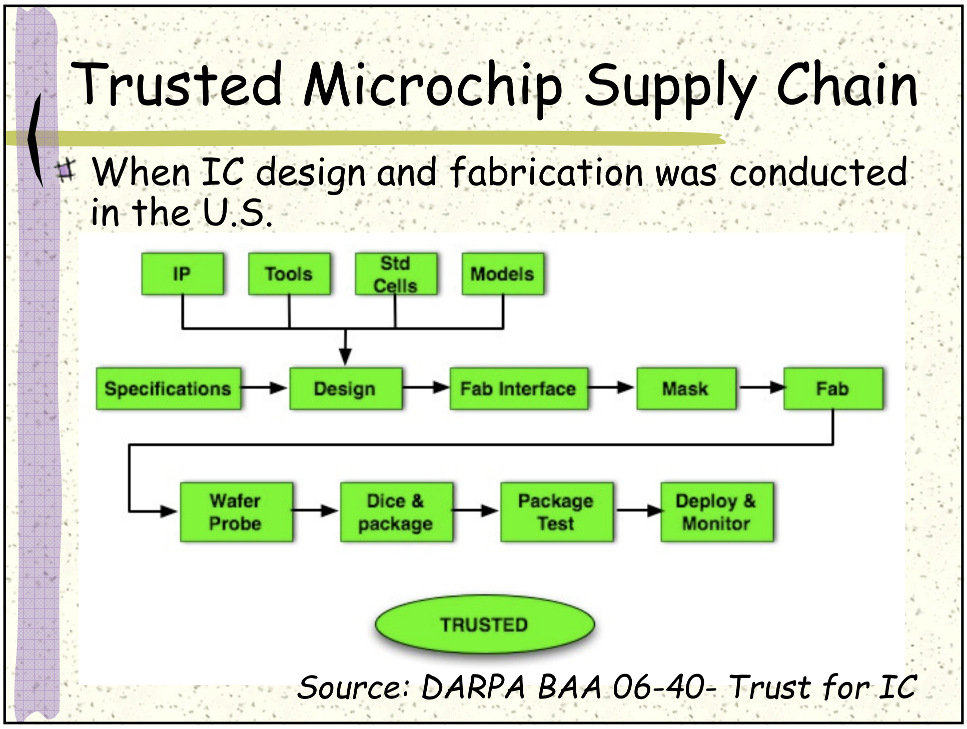
Hardware Security -- Vulnerabilities

Cybersecurity Specialization



You can't and should not trust the hardware you are given

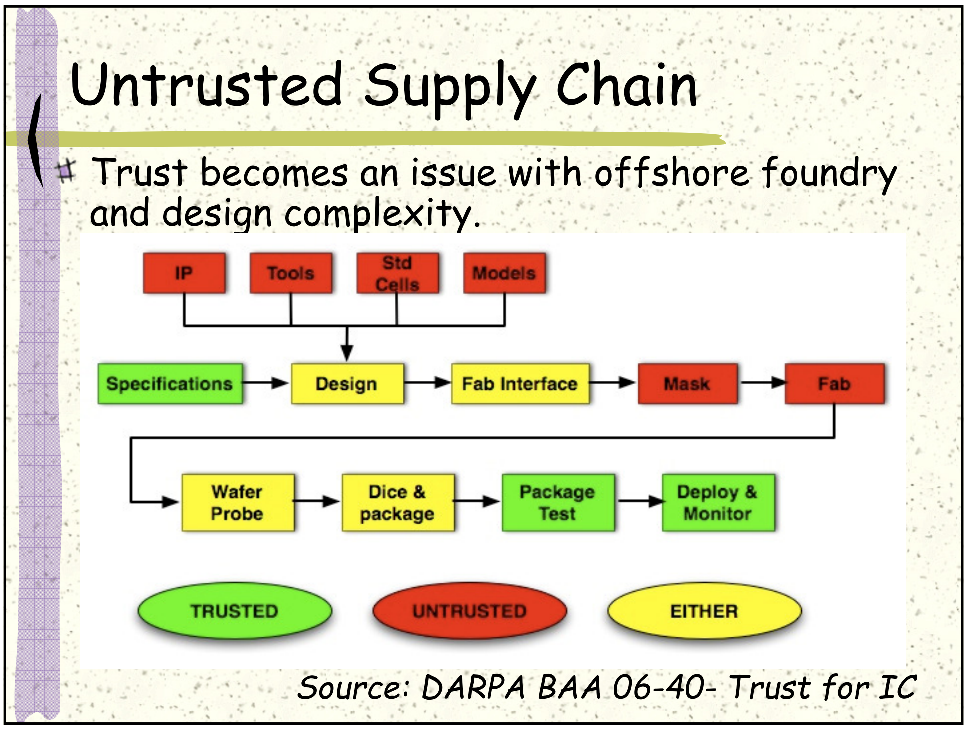
- Trust in microchip supply chain
  - Backdoors
  - Untrusted third party IPs and design tools
  - Improper design and implementation
  - Hardware Trojans
- Side-channel attacks
- Physical attacks



Trusted Microchip Supply Chain

- When IC design and fabrication was conducted in the U.S.

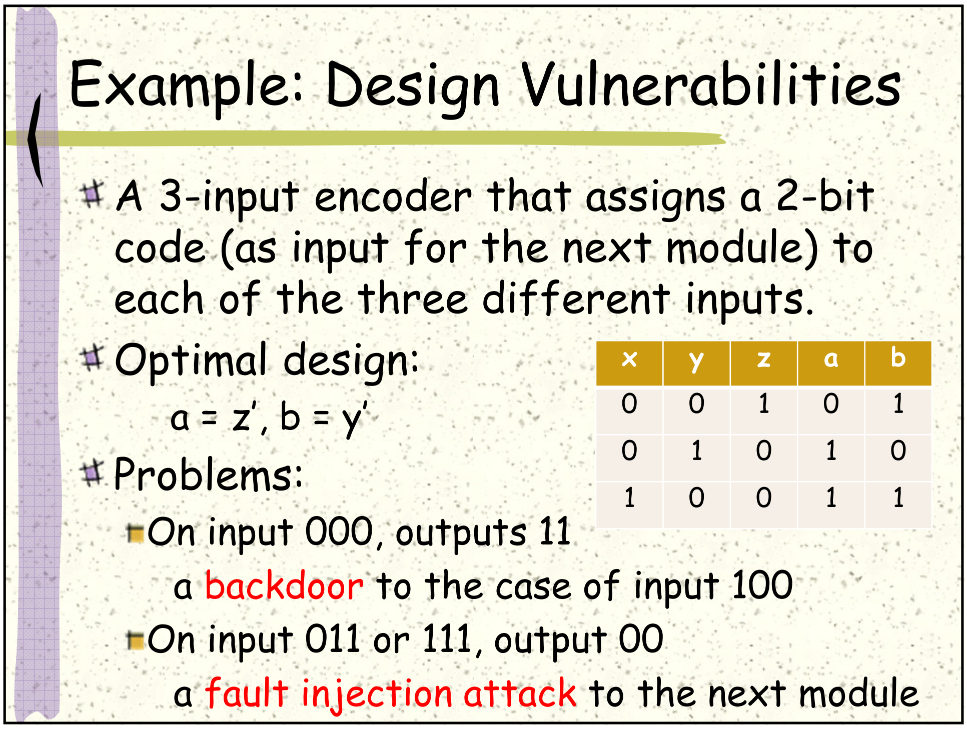
Source: DARPA BAA 06-40- Trust for IC



Untrusted Supply Chain

- Trust becomes an issue with offshore foundry and design complexity.

Source: DARPA BAA 06-40- Trust for IC



Example: Design Vulnerabilities

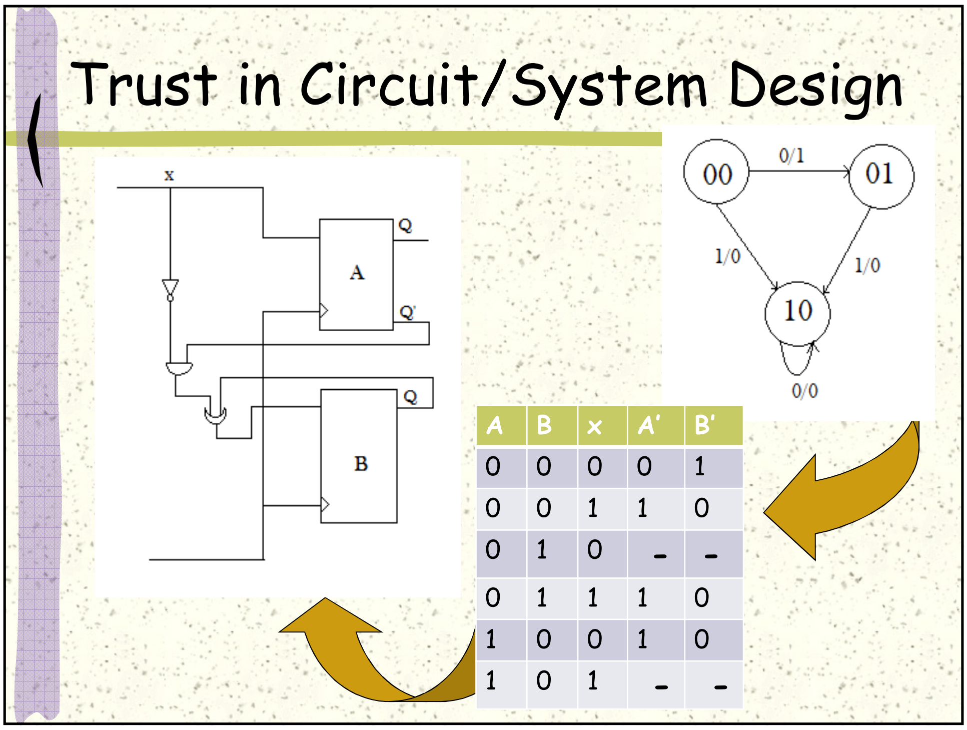
- A 3-input encoder that assigns a 2-bit code (as input for the next module) to each of the three different inputs.
- Optimal design:

  a = z', b = y'
- Problems:
  - On input 000, outputs 11

    a backdoor to the case of input 100
  - On input 011 or 111, output 00

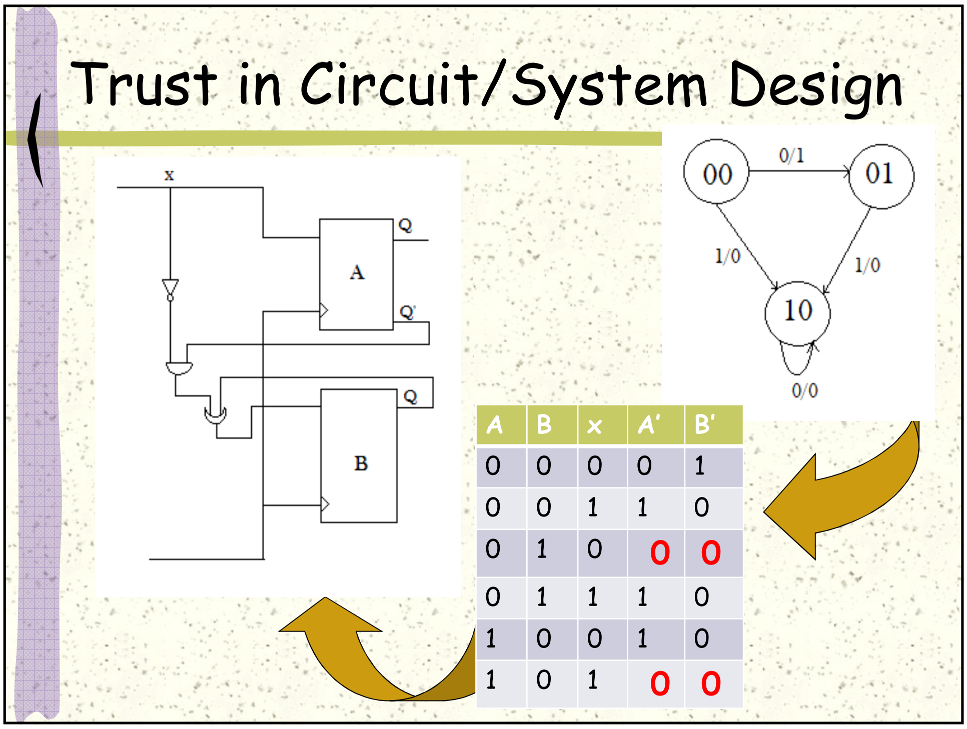
    a fault injection attack to the next module

x	y	z	a	b
0	0	1	0	1
0	1	0	1	0
1	0	0	1	1



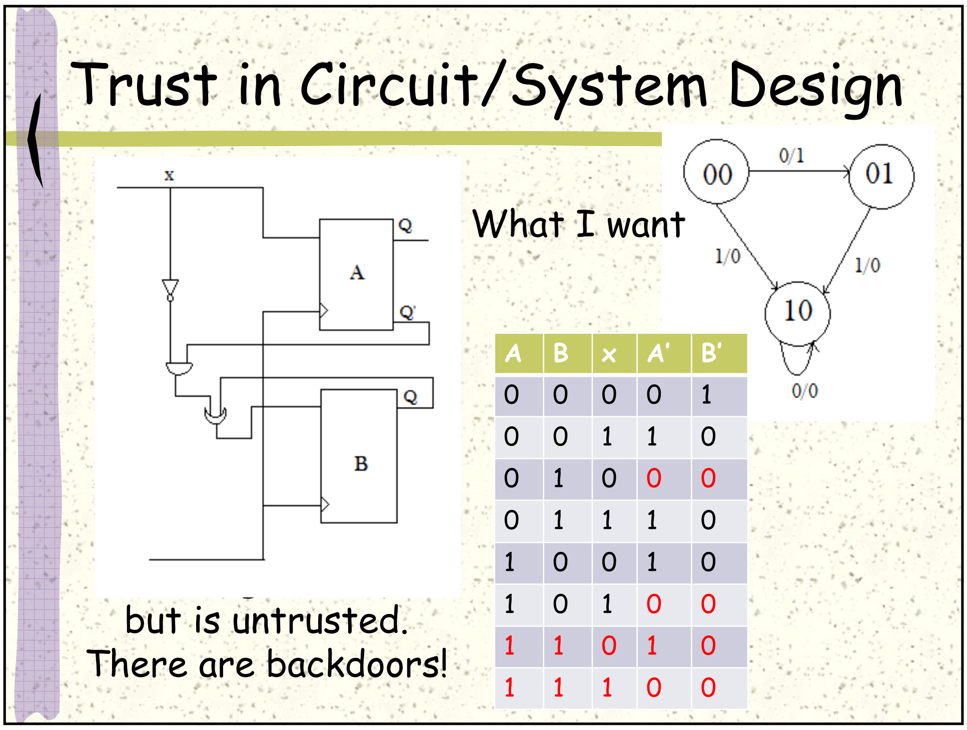
Trust in Circuit/System Design

A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	-	-
0	1	1	1	0
1	0	0	1	0
1	0	1	-	-



Trust in Circuit/System Design

A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	0	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	0

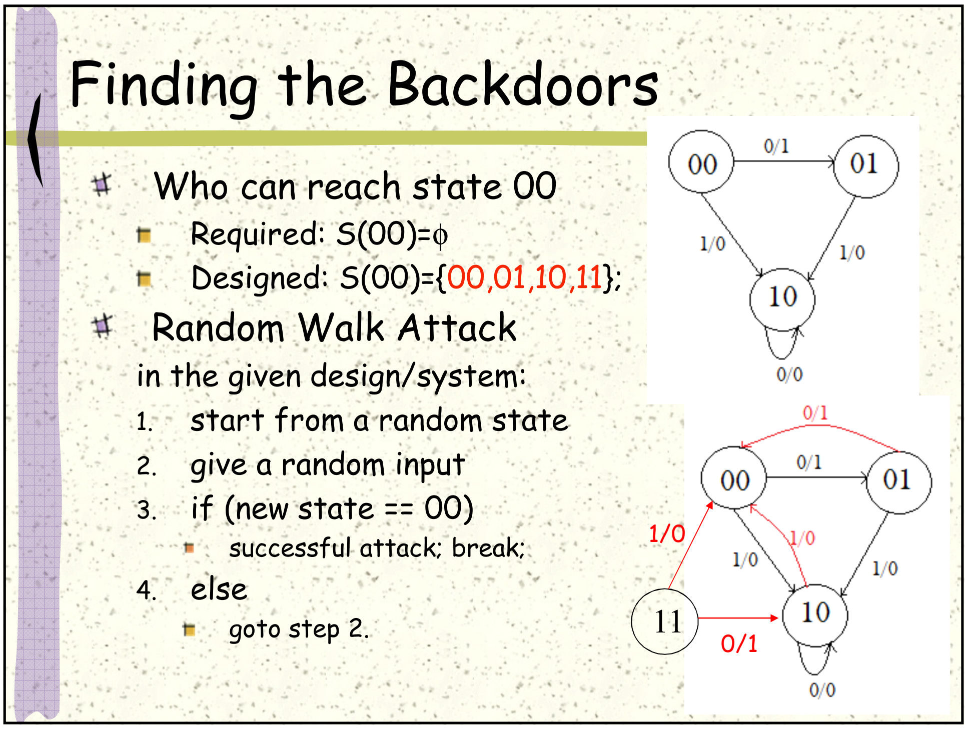


Trust in Circuit/System Design

What I want

A	B	x	A'	B'
0	0	0	0	1
0	0	1	1	0
0	1	0	0	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	0
1	1	0	1	0
1	1	1	0	0

but is untrusted.
There are backdoors!

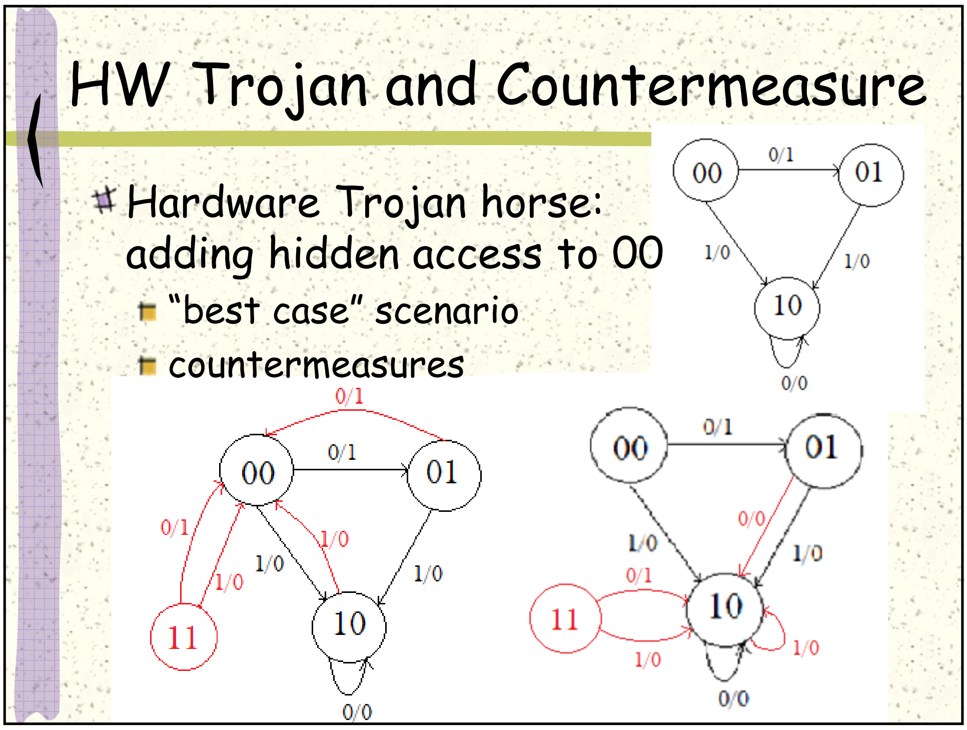


Finding the Backdoors

- Who can reach state 00
  - Required: S(00)=ϕ
  - Designed: S(00)={00,01,10,11};
- Random Walk Attack

in the given design/system:

1. start from a random state
2. give a random input
3. if (new state == 00)
   - successful attack; break;
4. else
   - goto step 2.



HW Trojan and Countermeasure

- Hardware Trojan horse: adding hidden access to 00
  - "best case" scenario
  - countermeasures