Hardware Trojan Detection

Maximilian Heim

University Albstadt-Sigmaringen

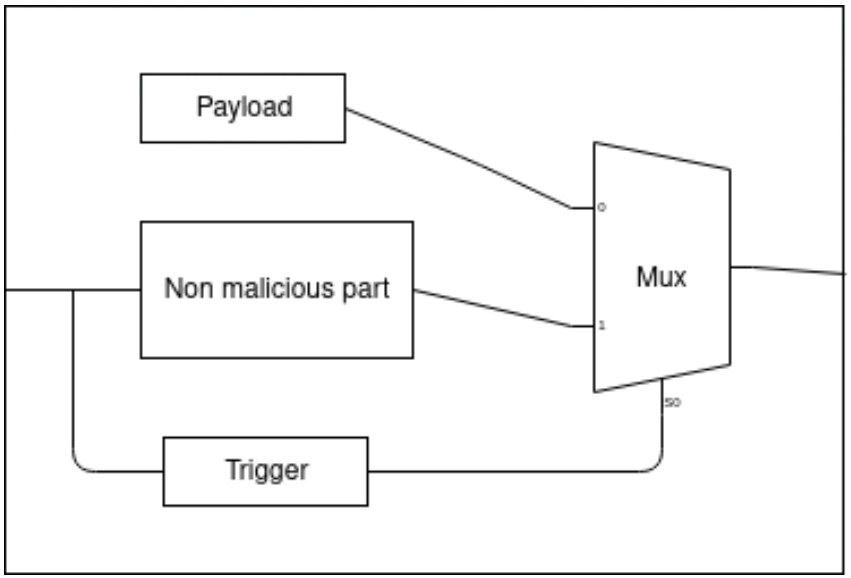
June 18, 2022

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Was sind Hardware Trojaner?

1. Bösartige Modifikation eines Integrierten Schaltkreises
2. Besteht aus einem Trigger (Time bombs, cominational...) und einer Payload (Denial of service, extraction of information, keys)

Figure: Theoretischer Aufbau eines HW Trojaners



Warum ist es wichtig diese zu erkennen?

- Militär
- Finanzen
- Energie
- Geheimdienste
- Überwachungsstaaten
- Transport
- U.v.m ...

Reverse Engineering

- Entfernen der Oberfläche Schicht für Schicht, vergleich mit Golden Sample
- Vorteile:
  1. 100 % Erkennungsrate mit passendem Equipment
- Nachteile:
  1. Testet nur einen Chip
  2. Chip ist danach kaputt
  3. Sehr zeitaufwändig

Funktionstests

- Beobachten der Ausgabe bei bestimmten Eingängen und Vergleich dieser mit Golden Sample
- Problem: Trigger sehr spezifisch, daher wird hier zum Teil auch mit Fuzzing gearbeitet
- Vorteile:
  1. Sehr einfacher Testaufbau
  2. Hohe Erkennungsrate
  3. Hunderte IC's können parallel getestet werden
- Nachteile:
  1. Je nach Komplexität des IC's sehr zeitaufwändig/unmöglich

Seitenkanaltest

- Beobachten der Leistungsaufnahme/Pfadverzögerung des IC's und Vergleich dieser mit dessen eines Golden Samples
- Vorteile:
  1. Erkennung ohne Aktivierung
  2. Sehr einfacher Testaufbau
  3. Hohe Erkennungsrate
  4. Hunderte IC's können parallel getestet werden
- Nachteile:
  1. Produktionsvariationen
  2. Bei sehr kleinen Trojanern kann die Leakage sehr klein werden
- D. Agrawal und andere stellen in "Trojan detection using IC fingerprinting" das Konzept von IC Fingerprinting vor. Hier wird basierend auf einem oder mehreren Seitenkanälen ein Fingerabdruck erzeugt der Trojaner mit einem Flächeanteil von 0.01 % erkennt.

Fazit

Quellen

- https:/d/dl.acm.org/doi/pdf/10.1145/2906147
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5340158