Hardware Trojan Detection

Maximilian Heim

University Albstadt-Sigmaringen

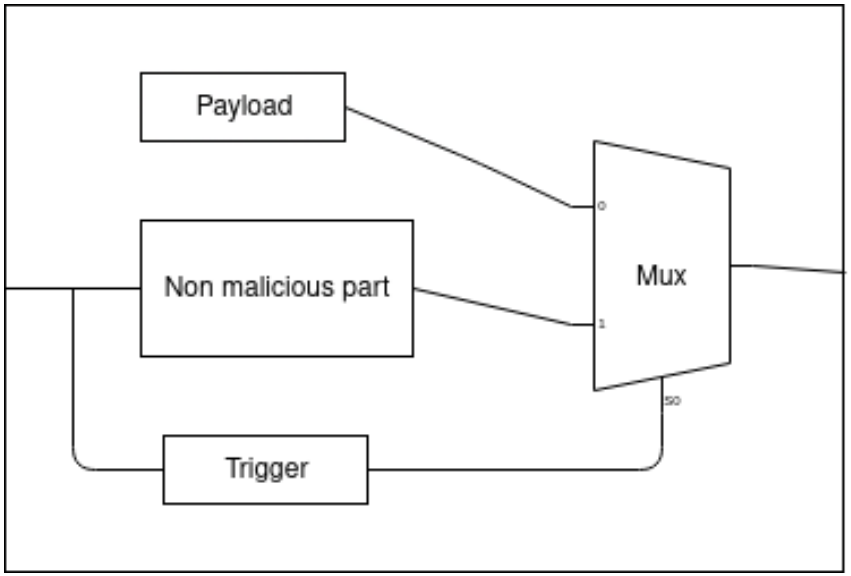
June 19, 2022

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Was sind Hardware Trojaner?

1. Bösartige Modifikation eines Integrierten Schaltkreises
2. Trigger (Time bombs, cominational...)
3. Payload (Denial of service, extraction of information, keys)

Figure: Theoretischer Aufbau eines HW Trojaners



Destruktives Reverse Engineering

- Entfernen der Oberfläche
- Visuelle Inspektion
- Vergleich mit Golden Sample
- Vorteile:
  1. 100 % Erkennungsrate
- Nachteile:
  1. Testet nur einen Chip
  2. Destruktiv
  3. Zeitaufwändig
  4. Unclonable functions

Funktionstests

- Beobachten der Ausgabe bei bestimmten Eingängen
- Vergleich mit Golden Sample
- Problem: Großer Trojan Space
- 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

Funktionstests: Statistischer Ansatz

- R.S. Chakraborty et al, "MERO: A Statistical Approach for Hardware Trojan Detection"
- `https://link.springer.com/content/pdf/10.1007/978-3-642-04138-9_28.pdf`
- Netzliste $\rightarrow$ Testvektoren
- Vektoren werden N mal getestet
- Reduktion der Testzeit um 85 %

Seitenkanaltest

- Beobachten der Leistungsaufnahme/Pfadverzögerung
- Vergleich mit Golden Sample
- 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

Seitenkanaltest: Fingerprinting

- D. Agrawal et al, "Trojan Detection using IC Fingerprinting"
- `https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4223234`
  1. Select random ICs
  2. Run IO tests, record traces
  3. Build fingerprint
  4. Destructively test for HW Trojan
  5. Match Sidechannel fingerprint of ICs to test with those of the reference

Fazit

- Destruktive Detektion ungeeignet für Testen von ICs die verwendet werden sollen
- Gegenüberstellung von Funktionstests und Seitenkanaltests:

	Funktionstests	Seitenkanaltests
Pros	1. Effektiv für kleine Trojaner 2.Produktionstoleranz unabhängig	1.Effektiv für große Trojaner 2. einfache Testerzeugung
Cons	1. Testerzeugung komplex	1. Anfällig für Produktionstoleranzen 2. Detektion von kleinen Trojanern schwierig

- Wie man sieht: Die Verfahren ergänzen sich $\rightarrow$ Kombination beider Verfahren

Quellen

- https:/d/dl.acm.org/doi/pdf/10.1145/2906147
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5340158
- https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HWT-Bericht/HWT-Bericht_Cover.pdf