Device Library Attack: Silently Compromising the FPGA Design Flow

Christian Krieg, Michael Rathmair and Florian Schupfer
Institute of Computer Technology, Vienna University of Technology

Abstract

In this paper, we present work in progress which aims at detecting hardware Trojans inserted during the field programmable gate array (FPGA) design phase. Therefore, we analyze the FPGA design flow for vulnerabilities and show how to attack a design undetectable for any participant in the design flow. We are doing this by manipulating the device library, which is consulted during the synthesis process. We formally model our attack using logic cones and propose logic-cone-based equivalence checking (EC) throughout the design process for problem mitigation. With the help of a simple yet effective example kill switch we show that the problem poses a realistic threat to digital systems.

Problem Description

FPGA and CPLD Design

- FPGA and CPLD design is **less expensive**
- Tools for FPGA and CPLD design often available **free of charge**
- EC tools not available free of charge, **high license fees**

Attack Vector: Device Library

- Device libraries are used to **map logic equations** to gate representations
- Mapping is done using a lookahead LR (LALR) parser using **compiled parser tables** (we call them *device libraries*)
- Tables can be **modified** in order to change the parser's grammar
- Modification to insert **hidden functionality**

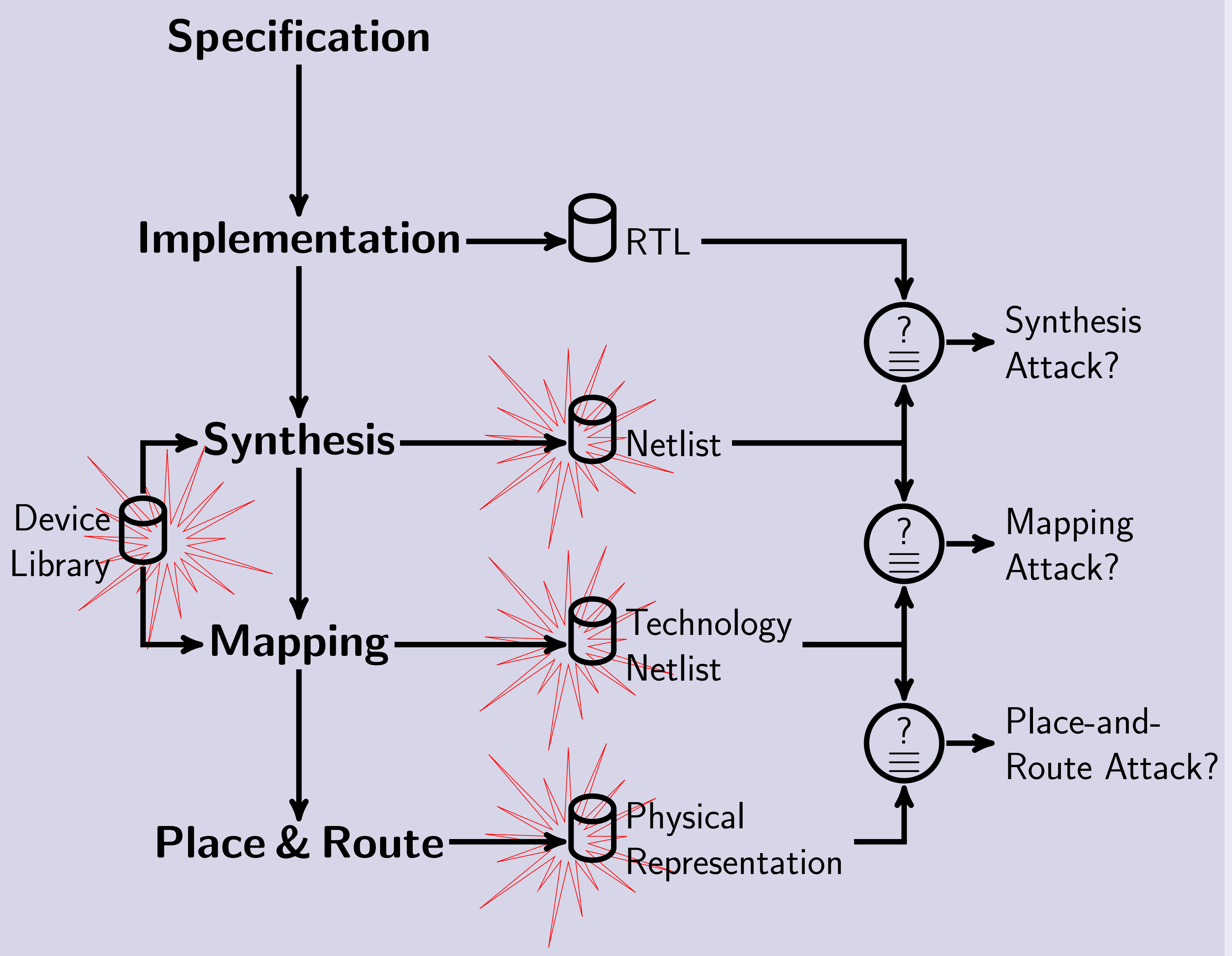
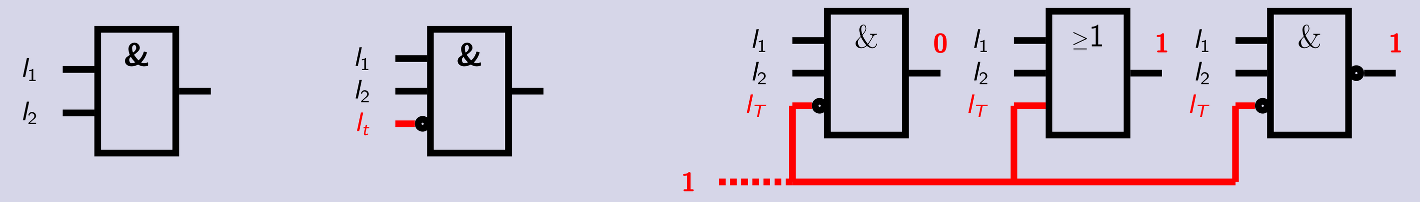


Figure 1: **FPGA Design Flow.** Compromised documents are marked with a starburst.

Attack Scenario

- **Trustworthy designer**
- Attacker from **outside**
- Device library is **replaced** by compromised version
- Example: **Additional (dominant) inputs** for logic primitives (fig. 2c)
- If 100% of logic primitives compromised: **Kill switch** [1]

Example Attack: Kill Switch



(a) Original (b) Compromised (c) Malicious gate chain

Figure 2: **Attack Scenario.** The dominating input values of different logic primitives when I_T is TRUE are shown in fig. 2c, along with resulting output values.

References

[1] S. Adee. The hunt for the kill switch. *Spectrum, IEEE*, 45(5):34–39, May 2008. ISSN 0018-9235. doi: 10.1109/MSPEC.2008.4505310.

[2] K. Hering, R. Haupt, and T. Villmann. *Cone-basierte, hierarchische Modellpartitionierung zur parallelen compilergesteuerten Logiksimulation beim VLSI-Design*. Institut für Informatik Leipzig: Report. Inst. für Informatik, 1995. URL http://books.google.at/books?id=s9GnGwAACAAJ.

Contact

Christian Krieg
☎ +43-1-58801-38464
https://www.ict.tuwien.ac.at/en/users/krieg
✉ christian.krieg@alumni.tuwien.ac.at

Acknowledgment

This work has been supported by the Austrian research funding association (FFG) FIT-IT program under contract no. 835922.

Attack Model

- The **fan-out cones** $co_{O,T}(x), x \in M_{E,T}$ of malicious gates influence the operation of the system
- A **primary output** $o \in M_O$ that is compromised contains at least one malicious gate $g \in M_{E,T}$ in its fan-in cone $co_I(o)$, therefore if $g \in co_I(o) \to o \in M_{O,T}$ where $M_{O,T} \subseteq M_O$
- A **latch** $l \in M_L$ that is compromised contains at least one malicious gate $g \in M_{E,T}$ in its fan-in cone $co_I(l)$, therefore if $l \in co_I(l) \to l \in M_{L,T}$ where $M_{L,T} \subseteq M_L$

Trojan Cones

$$Co_T(M) = \{c_T | \exists x (x \in M_O \cup M_L \wedge c_T = co(x)) \wedge \exists y (y \in M_{E,T} \wedge y \in co(x))\}. \tag{1}$$

Number of Trojan Cones

$$|Co_T(M)| = |M_{L,T}| + |M_{O,T}| = m_T. \tag{2}$$

Degree of Infection

$$d_T = \frac{m_T}{m_c} = \frac{|M_{L,T}| + |M_{O,T}|}{|M_L| + |M_O|}. \tag{3}$$

Countermeasures

- **Equivalence checking (EC)** throughout the FPGA and complex programmable logic device (CPLD) design flow
- Securing the design house's **IT infrastructure** to avoid illegitimate access

Outlook

- Recreate format of **parse tables** and extend the parser's grammar
- Investigate attack vectors at lower levels of abstraction to find more **stealthy attacks**
- Investigate **physical kill switches** to be injected during place and route