Cyber and Hardware Security in the Age of Large-Scale Adversaries

Belfer Center for Science and International Affairs
Harvard Kennedy School, June 7, 2019

Christof Paar
Ruhr-Universität Bochum & University of Massachusetts Amherst
Agenda

- Introduction to Hardware Trojans
- Historical Perspective
- Designing a Stealthy Trojan
Hardware Trojans

Malicious change or addition to an IC that adds or remove functionality, or reduces reliability

Many rather unpleasant “applications”
Hardware Trojans & the Scientific Community

Defense Science Board
Task Force
On
HIGH PERFORMANCE MICROCHIP SUPPLY

February 2005

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140
Trojan Injection & Adversaries Scenarios

Hostile hardware blocks ("IP-cores")

IC manufacturing during shipment

NSA’s interdiction

Built-in by manufacturer
Agenda

- Introduction to Hardware Trojans
- Historical Perspective
- Designing a Stealthy Trojan
Historical Perspective: Cold War

US WWII
M-209 encryption machine

Cold War
C-52 encryption machine

AB Cryptoteknik
by Boris Hagelin

Crypto AG
by Boris Hagelin
Historical Perspective: Cold War

alleged cooperation between 
*Crypto AG* and intelligence services

Strong indication that C-52 
was artificially weakened
Historical Perspective: Cold War

1986 Berlin bombing
La Belle discothèque

retaliatory air strikes against Libya
Historical Perspective: 1990s Crypto Wars

• after 1945: Cryptography **export-controlled** on „United States Munitions List“

• Exports: **crypto keys limited to 40 bits** breakable within hours

• 1996: major **relaxation of crypto export**
Historical Perspective: recent years

• 2017: Law enforcement „Going dark“ through strong cryptography

• ... crypto backdoors can be „solution“

• Subversion of crypto standards
• Dual ECC random number generator
Historical Perspective: 2019

• How trustworthy is foreign-made equipment?

Backdoors in routers? ... or mobile networks?
Agenda

- Introduction to Hardware Trojans
- Historical Perspective
- Designing a Stealthy Trojan
Where are we with **real** HW Trojans?

- No true hardware Trojan observed in the wild
- All examples from academia
Our Thoughts

1. Designing Trojan could be fun too
2. Especially those that go *undetected*
Simple Example: Inverter Trojan

Let’s modify an inverter so that it always outputs “1” (VDD) without visible changes.

<table>
<thead>
<tr>
<th>A</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

![Diagram showing the modification of an inverter to always output 1 (VDD)]
PMOS Transistor Trojan

Unmodified PMOS transistor

Trojan trans. w/ constant VDD output
“Always One” Trojan Inverter

Q: How to build a useful Trojan from here?
Can we detect dopant Trojans?

Which one has the Trojan?

Original Inverter

Trojanized Inverter
A Real-World True Random Number Generator

Disclaimer: Attacks works against most modern TRNGs

dopant Trojan

... random numbers generate cryptographic keys for

- secure web browsing
- email encryption
- document certification
- ...

Secure Sign In

Online ID:

Save this Online ID

I forgot my Online ID

Check Your SiteKey
2 Modules form Random Number Generator

entropy source

011001011110 ...

digital post processing

allows Trojan with very precise features

Crypto Key
Attacking crypto keys

• without Trojan $2^{256}$ keys → lifetime of the the universe
• with Trojan $2^{32}$ keys → 2 seconds

attacker can break all “secure” connections

... without detection!
Research agenda

1. Fully understand “design space” of stealthy Trojan
   - Trojans with trigger conditions
   - Provably non-detectable
   - Automated injection process

2. Development of Countermeasures
   - Design obfuscation
   - Trojan-resistant protocols
   - Specialized test methods
   - ....
Learning Cryptography

Introduction to Cryptography by Christof Paar

24 video lectures

very accessible book!
Thank you very much for your attention!

Christof Paar