Graph Algorithms for Hardware Reverse Engineering

Bochum, Germany, July 20, 2017

Marc Fyrbiak
Chair for Embedded Security
Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum
Global IC Supply Chain

Problem . . . and Solutions

- **Problem I:** Hardware Trojans
  - **Solution I:** Hardware reverse engineering
Problem . . . and Solutions

● Problem I: Hardware Trojans
  ○ Solution I: Hardware reverse engineering

● Problem II: Hardware reverse engineering tools
  ○ Solution II: We developed one . . . with the help of a very successful AI study project.
Problem I: Hardware Trojans
  ◦ Solution I: Hardware reverse engineering

Problem II: Hardware reverse engineering tools
  ◦ Solution II: We developed one . . . with the help of a very successful AI study project.

Problem III: Optimal layout of hardware (= graph) to support human analyst
Your Task

- Get used to the hardware reverse engineering context
- Understand different concepts of graph layout algorithms
- Implement and evaluate graph layout algorithms
  - [Optional] GPU implementation
Requirements and What You Learn

Requirements:
- 2 - 3 students (Bachelor or Master)
- Background in C, C++, Qt, Python
- Interest in graph layout algorithms, graphical user interfaces
Requirements and What You Learn

Requirements:
- 2 - 3 students (Bachelor or Master)
- Background in C, C++, Qt, Python
- Interest in graph layout algorithms, graphical user interfaces

What You Learn:
- Problems in hardware reverse engineering
- Understanding of graph layout algorithms
Contact

M. Sc. Marc Fyrbiak
Chair for Embedded Security
Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum
Room: ID 2/645
E-mail: marc.fyrbiak@rub.de
Tools for Embedded Software Reverse Engineering

Bochum, Germany, July 20, 2017

Marc Fyrbiak
Chair for Embedded Security

Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum
Open Challenges in Embedded Systems

Hacked Cameras, DVRs Powered
Today’s Massive Internet Outage
krebsonsecurity.com - Oct 2016

Millions of IoT devices enlisted into DDoS bots
with Bashlite malware
scmagazine.com - Aug 2016
Open Challenges in Embedded Systems

Hacked Cameras, DVRs Powered
Today's Massive Internet Outage
krebsonsecurity.com - Oct 2016

Millions of IoT devices enlisted into DDoS bots
with Bashlite malware
scmagazine.com - Aug 2016

Industrie 4.0 macht auch neue
Security-Konzepte erforderlich
zdnet.de - Feb 2016

BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches
Stahlwerk
helse.de - Dec 2014
Open Challenges in Embedded Systems

Hacked Cameras, DVRs Powered Today’s Massive Internet Outage
krebsonsecurity.com - Oct 2016
Millions of IoT devices enlisted into DDoS bots with Bashlite malware
scmagazine.com - Aug 2016

Industrie 4.0 macht auch neue Security-Konzepte erforderlich
zdnet.de - Feb 2016
BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk
heise.de - Dec 2014

Hackers remotely kill a Jeep on the highway—with me in it
wired.com - Jul 2015
The Jeep hack was only the beginning of smart car breaches
businessinsider.com - Jul 2015
Hacked Cameras, DVRs Powered Today’s Massive Internet Outage
krebsonsecurity.com - Oct 2016
Millions of IoT devices enlisted into DDoS bots with Bashlite malware
scmagazine.com - Aug 2016

Industrie 4.0 macht auch neue Security-Konzepte erforderlich
zdnet.de - Feb 2016
BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk
heise.de - Dec 2014

Hackers Remotely Kill a Jeep on the Highway—With Me in It
wired.com - Jul 2015
The Jeep hack was only the beginning of smart car breaches
businessinsider.com - Jul 2015

70 Prozent der Unternehmen sind von Produkt- oder Markenpiraterie betroffen. Der geschätzte Schaden für den deutschen Maschinen- und Anlagenbau beträgt 7,3 Milliarden Euro jährlich.
vdma.org - Apr 2016
Wie haben sich die Plagiaturen das notwendige Wissen beschafft?
Reverse Engineering 69%
vdma.org - Apr 2016
Solution - Obfuscation

*Code Obfuscation*

Transforms code that is difficult to understand for human reverse engineers
Solution - Obfuscation

Code Obfuscation
Transforms code that is difficult to understand for human reverse engineers

- Hamper reverse engineering
- Safeguard intellectual property
- Watermarking
- Exploit Mitigation
Your Task

- Development of a tool to arm embedded firmware with obfuscation
- Modular design to integrate variety of obfuscation techniques
- Improvements of reverse engineering tools
Your Task

- Development of a tool to arm embedded firmware with obfuscation
- Modular design to integrate variety of obfuscation techniques
- Improvements of reverse engineering tools
- Technical details for obfuscation and reverse engineering at start of the project 😊
Requirements and What You Learn

Requirements:
- 2 - 3 students (Bachelor or Master)
- Background in Python
- Basic understanding of embedded systems and assembler
- Interest in reverse engineering and obfuscation

What You Learn:
- Embedded systems
- Reverse engineering and obfuscation techniques
- Compiler internals
M. Sc. Marc Fyrbiak
Chair for Embedded Security
Horst Görtz Institute for IT-Security, Ruhr-Universität Bochum
Room: ID 2/645
E-mail: marc.fyrbiak@rub.de