Kick-off: Control Flow Integrity Based Security

Paul Muntean
paul@sec.in.tum.de

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

04.07.2017

Outline

Organization

The seminar will be organized as a scientific conference:

1. Familiarization phase (approx. 2 Week)
2. Manufacturing phase (approx. 6 Week)
3. Review phase (approx. 2 Week)
4. Improvement phase (approx. 2 Week)
5. Talk preparation (approx. 1 Week)
6. Talk and Discussion

Requirements

Report Elaboration

- Delivery of a scientific paper with minimum 10 pages in length
- Usage of LaTeX is mandatory for all
- Formatting with the LaTeX-Style of Springer (LNCS)

Reviews

- Each one of you creates two anonymous reviews about other two reports
- Size of the one review: approximately one page in LaTeX
- Additionally each of you will get an review from us

Presentation

- Preparing of the presentation (Tool free choice)
- 30 minutes presentation
- Afterwards 15 minutes discussion

Grading

The Grading is comprised of all personal contributions of this seminar and is composed of:

- Report (50%)
- Presentation (25%)
- Delivered review (15%)
- Participation and discussion (10%)

Time Table

04.07.	Kick-off
18.10. - 27.01.	Regular meetings (presence mandatory)
31.10.	Delivery of the literature research, Outline of the report
09.11. - 12.12.	Presentations
Bis 19.12.	End of the presentation phase and delivery of the 1. version of the report
09.01.	Distribution of the review topics; one email; 2 reports/student
16.01.	Delivery of the reviews to me over email, two pdf files
23.01.	Return of the reviews to the students
30.01.	Final report delivery in email format and in one pdf file

Organization

Before we go to the topics...

Questions, comments, need for discussion?

Seminar Topics

Overview

1. Only virtual calls based attack on C++ applications
2. ROP based attack demonstrating that coarse grained CFI is not sufficient
3. binary based protection of vTables using CFI
4. binary based CFI protection against vTables hijaking
5. Clang compiler based CFI protection against vTables hijaking
6. GCC and LLVM compiler based CFI protection for complete systems
7. attack paper addressing the ineffectiveness of of CFI based protection
8. attack paper demonstrating the ineffectiveness of Control Pointer Integrity (CPI)
9. CFI based protection for JavaScript based applications
10. CFI based protection for iOS applications
11. CFI based protection for binaries based on shadow stacks
12. dynamic function calls protection based on virtual function type enforcement and vTable pointer sanitization

Topic assignment

- Who wants which topic?

Literature Research

Goal:

- To find relevant literature
- Main arguments, Techniques or Approaches...
  1. find,
  2. understand,
  3. explain,
  4. prove them
- Structure Topics
  - Report structure

Literature Research & Sources

Good

- Books, Library
- `http://portal.acm.org/`
- `http://www.springerlink.com/`
- `http://www.computer.org/`
- `http://citeseer.ist.psu.edu/`
- `http://scholar.google.com/`
- `http://dblp.uni-trier.de/`

Wrong

- Heise-Newsticker
- Wikipedia
- e.g., *Website XYZ*

Access to Literature

Through the Authors Website

- Authors publish the papers mostly on their websites
- Other resources can be found through Google Scholar

Through Springer, ACM, IEEE

- Download of papers costs
- TUM has full rights to download papers
- Usage on an Proxy-Server required:
  `www.lrz.de`
- Access through the proxy in the TUM web is restricted

Next Steps

LaTeX-Introduction

- Is there the need?
- Schedule a date?

ToDos in the Familiarization phase

1. Literature research
2. Create report structure

Q&A?