Control Flow Based Security

Paul Muntean
paul@sec.in.tum.de

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

29.01.2018
Outline

1. Organization and Requirements
2. Grading
3. Time Table
4. Seminar Topics
5. Literature Research
6. Next Steps
7. Q&A
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 about ≥ 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
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%)
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.04.</td>
<td>Kick-off</td>
</tr>
<tr>
<td>18.04. - 27.06.</td>
<td>Regular meetings (presence mandatory)</td>
</tr>
<tr>
<td>02.05.</td>
<td>Delivery of the literature research, Outline of the report</td>
</tr>
<tr>
<td>09.05. - 27.06.</td>
<td>Presentations</td>
</tr>
<tr>
<td>Bis 30.06.</td>
<td>Delivery of the 1. version of the report</td>
</tr>
<tr>
<td></td>
<td>End of the presentation phase</td>
</tr>
<tr>
<td>04.07.</td>
<td>Distribution of the review topics</td>
</tr>
<tr>
<td>Bis 07.07.</td>
<td>Delivery of the reviews</td>
</tr>
<tr>
<td>08.07.</td>
<td>Return of the reviews</td>
</tr>
<tr>
<td>Bis 11.07.</td>
<td>Delivery of the final version of the report</td>
</tr>
<tr>
<td>16.07.</td>
<td>End of lectures</td>
</tr>
<tr>
<td>Time Table</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td></td>
</tr>
<tr>
<td><strong>April</strong></td>
<td></td>
</tr>
<tr>
<td>1 2 3</td>
<td></td>
</tr>
<tr>
<td>4 5 6 7 8 9 10</td>
<td></td>
</tr>
<tr>
<td>11 12 13 14 15 16 17</td>
<td></td>
</tr>
<tr>
<td>18 19 20 21 22 23 24</td>
<td></td>
</tr>
<tr>
<td>25 26 27 28 29 30</td>
<td></td>
</tr>
<tr>
<td><strong>Mai</strong></td>
<td></td>
</tr>
<tr>
<td>2 3 4 5 6 7 8</td>
<td></td>
</tr>
<tr>
<td>9 10 11 12 13 14 15</td>
<td></td>
</tr>
<tr>
<td>16 17 18 19 20 21 22</td>
<td></td>
</tr>
<tr>
<td>23 24 25 26 27 28 29</td>
<td></td>
</tr>
<tr>
<td>30 31</td>
<td></td>
</tr>
<tr>
<td><strong>Juni</strong></td>
<td></td>
</tr>
<tr>
<td>1 2 3 4 5</td>
<td></td>
</tr>
<tr>
<td>6 7 8 9 10 11 12</td>
<td></td>
</tr>
<tr>
<td>13 14 15 16 17 18 19</td>
<td></td>
</tr>
<tr>
<td>20 21 22 23 24 25 26</td>
<td></td>
</tr>
<tr>
<td>27 28 29 30</td>
<td></td>
</tr>
<tr>
<td><strong>Juli</strong></td>
<td></td>
</tr>
<tr>
<td>1 2 3</td>
<td></td>
</tr>
<tr>
<td>4 5 6 7 8 9 10</td>
<td></td>
</tr>
<tr>
<td>11 12 13 14 15 16 17</td>
<td></td>
</tr>
<tr>
<td>18 19 20 21 22 23 24</td>
<td></td>
</tr>
<tr>
<td>25 26 27 28 29 30 31</td>
<td></td>
</tr>
</tbody>
</table>
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 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
Seminar Topics (1)

Only virtual calls based attack on C++ applications


ROP based attack demonstrating that coarse grained CFI is not sufficient


Binary based protection (defense) of vTables using CFI

Seminar Topics (2)

**Binary based CFI protection (defense) against vTables hijaking**


**Clang compiler based CFI protection (defense) against vTables hijaking**


**GCC and LLVM compiler based CFI protection (defense) for complete systems against ROP attacks**

C. Tice et. al., Enforcing Forward-Edge Control-Flow Integrity in GCC & LLVM, *In the Proceedings of the 24th USENIX Security Symposium, (SEC), 2014*
Seminar Topics (3)

**Attack paper addressing the ineffectiveness of CFI based protection**


**Attack paper demonstrating the ineffectiveness of Control Pointer Integrity (CPI)**


**CFI based protection (defense) for JavaScript based application against JIT-ROP**

CFI based protection (defense) for iOS applications against ROP attacks


CFI based protection (defense) for binaries based on shadow stacks


dynamic function calls protection (defense) based on virtual function type enforcement and VTable pointer sanitization

Who wants which topic?
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/

**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

\textbf{\LaTeX-Introduction}
- Is there the need?
- Schedule a date?

\textbf{ToDos in the Familiarization phase}
1. Literature research
2. Create report structure
Q&A?