Control Flow Based Security

Peng Xu, Paul Muntean
peng@sec.in.tum.de, paul@sec.in.tum.de

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

29.06.2016
Outline

1. Organization and Requirements
2. Grading
3. Time Table
4. Seminar Topics
5. Literature Research
6. Next Steps
7. Q&A
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 $\geq 10$ 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>29.06</td>
<td>Kick-off</td>
</tr>
<tr>
<td>17.10 - 19.12</td>
<td>Regular meetings (presence mandatory)</td>
</tr>
<tr>
<td>17.10</td>
<td>Delivery of the literature research, Outline of the report</td>
</tr>
<tr>
<td>07.11 - 19.12</td>
<td>Presentations</td>
</tr>
<tr>
<td>Bis 30.12</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>09.01.17</td>
<td>Distribution of the review topics</td>
</tr>
<tr>
<td>Bis 16.01</td>
<td>Delivery of the reviews</td>
</tr>
<tr>
<td>23.01</td>
<td>Return of the reviews</td>
</tr>
<tr>
<td>Bis 30.01</td>
<td>Delivery of the final version of the report</td>
</tr>
<tr>
<td>07.02</td>
<td>End of lectures</td>
</tr>
<tr>
<td>October</td>
<td>November</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>1 2</td>
<td>1 2 3 4 5 6</td>
</tr>
<tr>
<td>3 4 5 6 7 8 9</td>
<td>7 8 9 10 11 12 13</td>
</tr>
<tr>
<td>10 11 12 13 14 15 16</td>
<td>14 15 16 17 18 19 20</td>
</tr>
<tr>
<td>17 18 19 20 21 22 23</td>
<td>21 22 23 24 25 26 27</td>
</tr>
<tr>
<td>31</td>
<td></td>
</tr>
</tbody>
</table>
Before we go to the topics...

Questions, comments, need for discussion?
Seminar Topics

Overview

1. What is the control flow integrity (CFI)?
2. How CFI protects the software security?
3. Only CFI based defense is enough?
4. Several advanced attacks, such as ROP, JIT-ROP as well as COOP
5. CFI is introduced to defend the ROP and its variants
6. One advanced attack which based on the vTable hijacking
7. Source code recompiling based defense for the vTable hijacking
8. Binary rewriting based defense for the vTable hijacking
Seminar Topics (1) - basic

Control flow integrity - new version
Nathan Burow et. al., Control-Flow Integrity: Precision, Security, and Performance, ACM CSUR, 2016

Coarse-grained CFI can be diverted
### Seminar Topics (2) - Attacks

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ROP attack</strong></td>
<td>Hovav Shacham et. al., The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86), <em>In the Proc. of the ACM Conference on Computer and Communications Security, (CCS)</em>, 2007</td>
</tr>
<tr>
<td><strong>Blind-ROP attack</strong></td>
<td>Andrea Bittau et. al., Hacking Blind, <em>S&amp;P</em>, 2014</td>
</tr>
<tr>
<td><strong>COOP attack</strong></td>
<td>Felix Schuster et. al., Counterfeit Object-oriented Programming, <em>S&amp;P</em>, 2015</td>
</tr>
</tbody>
</table>
### Seminar Topics (3) - CFI-based defense

**CFI for ROP**

Nicholas Carlini et. al., ROP is Still Dangerous: Breaking Modern Defenses, *USENIX*, 2014

**CFI for JIT-ROP**

Ben Niu et. al., Modular Control-Flow Integrity, *In the Conference on Programming Language Design and Implementation*, PLDI14

**hash-based CFI**

B. Niu et. al., Cryptographically Enforced Control Flow Integrity, *CCS*, 2015

**hardware-based CFI**

Source-code recompiling based defense
Dongseok Jang et. al., SAFEDISPATCH: Securing C++ Virtual Calls from Memory Corruption Attacks, *NDSS*, 2014

Source-code recompiling based defense
Caroline Tice et. al., Enforcing Forward-Edge Control-Flow Integrity in GCC LLVM, *USENIX*, 2014

Binary rewriting based defense
Robert Gawlik et. al., Towards Automated Integrity Protection of C++ Virtual Function Tables in Binary Programs, *ACSAC*, 2014

Binary rewriting based defense
Topic assignment

- 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://portal.acm.org/)
- [http://www.springerlink.com/](http://www.springerlink.com/)
- [http://www.computer.org/](http://www.computer.org/)
- [http://citeseer.ist.psu.edu/](http://citeseer.ist.psu.edu/)
- [http://scholar.google.com/](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

**\LaTeX-Introduction**
- Is there the need?
- Schedule a date?

**Todos in the Familiarization phase**
1. Literature research
2. Create report structure
Q&A?