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 $\geq$ 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

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

18.04.	Kick-off
18.04. - 27.06.	Regular meetings (presence mandatory)
02.05.	Delivery of the literature research, Outline of the report
09.05. - 27.06.	Presentations
Bis 30.06.	Delivery of the 1. version of the report End of the presentation phase
04.07.	Distribution of the review topics
Bis 07.07.	Delivery of the reviews
08.07.	Return of the reviews
Bis 11.07.	Delivery of the final version of the report
16.07.	End of lectures

Time Table

April

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Mai

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Juni

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Juli

				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

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

Seminar Topics (1)

Only virtual calls based attack on C++ applications

F. Schuster et. al., Counterfeit Object-oriented Programming On the Difficulty of Preventing Code Reuse Attacks in C++ Applications, *In Proceedings of IEEE Symposium on Security and Privacy, (S&P)*, 2015

ROP based attack demonstrating that coarse grained CFI is not sufficient

E. Göktas et. al., Out Of Control: Overcoming Control-Flow Integrity, *In Proceedings of IEEE Symposium on Security and Privacy, (S&P)*, 2014

Binary based protection (defense) of vTables using CFI

R. Gawlik et. al., Towards Automated Integrity Protection of C++ Virtual Function Tables in Binary Programs, *In Proc. of the Annual Computer Security Applications Conference, (ACSAC)* , 2014

Seminar Topics (2)

Binary based CFI protection (defense) against vTables hijaking

C. Zhang et. al., VTint: Protecting Virtual Function Tables Integrity *In Proceedings of the Annual Network & Distributed System Security Symposium, (NDSS)*, 2015

Clang compiler based CFI protection (defense) against vTables hijaking

D. Jang et. al., SAFE DISPATCH: Securing C++ Virtual Calls from Memory Corruption Attacks , *In Proceedings of the Annual Network & Distributed System Security Symposium, (NDSS)*, 2014

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 of CFI based protection

N. Carlini et. al., Control-Flow Bending: On the Effectiveness of Control-Flow Integrity, *In the Proceedings of the 24th USENIX Security Symposium (SEC)*, 2015

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

I. Evans et. al., Missing the Point(er):On the Effectiveness of Code Pointer Integrity, *In Proceedings of IEEE Symposium on Security and Privacy, (S&P)*, 2015

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

B. Niu et. al., RockJIT: Securing Just-In-Time Compilation Using Modular Control-Flow Integrity, *In the Proc. of the ACM Conference on Computer and Communications Security, (CCS)*, 2014

Seminar Topics (4)

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

J. Pewny et. al., Control-Flow Restrictor: Compiler-based CFI for iOS *In Proc. of the Annual Computer Security Applications Conference, (ACSAC)*, 2013

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

U. Erlingsson et. al., XFI: Software Guards for System Address Spaces, *In the Proc. of the ACM Conference on Computer and Communications Security, (OSDI)*, 2006

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

C. Zhang et. al., VTrust: Regaining Trust on Virtual Calls, *In Proceedings of the Annual Network & Distributed System Security Symposium, (NDSS)*, 2016

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/`

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?