

Exploiting and Defense

Dobin Rutishauser
December 2016

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

A vertical strip on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

Intro

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Dobin Rutishauser

Working as Security Analyst @ Compass Security

- ✦ Penetration Tests
- ✦ Webapp Checks
- ✦ Architecture Reviews
- ✦ & lots more

Interested in ~~Hacking~~ Security since I was little (1999+)

Compass Security Ethical Hacking & Incident Response

Compass Security ist ein auf Security Assessments und forensische Untersuchungen spezialisiertes Unternehmen. Wir führen sowohl Penetration Tests als auch Security Reviews durch und unterstützen bei der Koordination und Analyse von Vorfällen.

Penetration Tests



Als Angreifer untersuchen wir Geräte, Netze, Dienste und Anwendungen auf Schwachstellen. Mittels Social Engineering und Red Teaming testen wir das Verhalten der gesamten Organisation. » **weiterlesen**

Security Reviews



Erfahrene IT Analysten unterstützen Sie mit Zweitmeinungen zu Security-Konzepten und prüfen nach Wunsch den Aufbau, die Konfiguration und den Quellcode Ihrer Lösung. » **weiterlesen**

Digital Forensics



Unsere Forensik-Experten helfen bei der Koordination von Vorfällen und Sofortmassnahmen sowie bei der gerichtsfesten Bearbeitung von Daten. Zudem bieten wir eine unkomplizierte und schnelle Ursachenforschung. » **weiterlesen**

Security Trainings



Profitieren auch Sie vom Wissen unserer Analysten zu Penetration Testing, Netzwerkanalyse, sichere Apps und Anwendungen, Digitale Forensik und trainieren Sie in einem eigens dafür erstellten Labor. » **weiterlesen**

FileBox



FileBox ist eine Secure File Transfer und Secure Storage Lösung. Damit haben Sie die Möglichkeit, Dokumente sicher auszutauschen. » **weiterlesen**

Hacking-Lab



Hacking-Lab ist eine Online-Plattform für Ethical Hacking, Netzwerke und IT Sicherheit, die sich der Suche und Ausbildung von Cyber Security Talenten widmet. » **weiterlesen**

Compass is hiring (always)



Wir haben verschiedene Stellen als **Penetration Tester** aber auch als **Software Entwickler** offen und würden uns sehr über Deine **Bewerbung** freuen.



Bist Du grundsätzlich vom Typ "Grübler" und "Tüftler"? Hast Du Freude daran, Dich in neue Themen und Techniken einzuarbeiten? Dann bist Du bei Compass genau richtig!

Bitte schicke Deine Fragen an ivan.buetler@compass-security.com und Deine offizielle Bewerbung an hr@compass-security.com

Gruss Ivan Bütler, E1

I got a bit overboard when I was little



A vertical decorative image on the left side of the slide. It shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys. The image is partially obscured by a solid blue vertical bar on the far left.

Vorlesung

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Websites:

<https://exploit.courses>

- ✦ Online exploit development website
- ✦ Uses Hacking-Lab accounts

<https://www.hacking-lab.com>

- ✦ Half-online challenges website



**Siiiiii abr ähhhhh
EBP isch doch 32 bit?**

shutterstock

IMAGE ID: 120482521
www.shutterstock.com

A vertical strip on the left side of the slide shows a close-up of a computer keyboard. A yellow padlock is attached to the keyboard, specifically over the 'Enter' key. The image is slightly blurred and has a blue tint.

Motivation

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Looking behind
the curtain



For the computer enthusiast:

- ✦ How do functions work?
- ✦ How does the memory allocator work?
- ✦ Whats the difference between userspace and kernelspace?
- ✦ How does computer work?

For the hacker:

- ✦ Develop exploits
- ✦ Debugging of C/C++ code
- ✦ Being 31337

For the future CISO:

- ✦ Assess CVSS score for vulnerabilities
- ✦ Assess security mitigations
- ✦ Better risk analysis

ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
 MTB: Mitigation Bypass
 RCE: Remote Code Execution
 RJB: Remote Jailbreak
 SBX: Sandbox Escape
 VME: Virtual Machine Escape

Up to \$500,000	Up to \$1,500,000										1.001 Apple iOS RJB
Up to \$100,000	Up to \$200,000										1.002 Android RJB
Up to \$80,000	Up to \$100,000									2.001 Flash Player with SBX RCE+SBX	1.003 Windows Phone RJB
Up to \$50,000	Up to \$80,000							3.001 Adobe PDF Reader RCE+SBX	2.002 Chrome with SBX RCE+SBX	2.003 IE + Edge with SBX RCE+SBX	2.004 Safari with SBX RCE+SBX
Up to \$40,000	Up to \$50,000	4.001 VM Escape VME						3.003 Windows Reader App RCE	2.005 Flash Player w/o SBX RCE	6.001 OpenSSL RCE	6.002 PHP RCE
Up to \$30,000	Up to \$40,000	5.001 ASLR Bypass MTB	5.002 Antivirus RCE/LPE				3.002 Office Word/Excel RCE	7.001 Sendmail RCE	7.002 Postfix RCE	7.003 Exchange Server RCE	7.004 Dovecot RCE
Up to \$20,000	Up to \$30,000	4.002 Windows LPE/SBX	4.003 Mac OS X LPE/SBX	4.004 Linux LPE			2.006 Chrome w/o SBX RCE	2.007 IE + Edge w/o SBX RCE	2.008 Tor Browser RCE	2.009 Firefox RCE	2.010 Safari w/o SBX RCE
Up to \$10,000	Up to \$10,000	8.001 IP.Suite RCE	8.002 IP.Board RCE	8.003 phpBB RCE	8.004 vBulletin RCE	8.005 MyBB RCE	8.006 WordPress RCE	8.007 Joomla RCE	8.008 Drupal RCE	8.009 Roundcube RCE	8.010 Horde RCE

* All payout at

* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

2016/09 © zerodium.com

Content of the next 7 Friday afternoons

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

You want to learn:

- ✦ What memory corruptions are
- ✦ What buffer overflows are
- ✦ What exploits are
- ✦ How exploits are being created
- ✦ To exploit a local application
- ✦ To exploit a remote application
- ✦ Learn about anti-exploiting technologies
- ✦ To circumvent all common anti-exploiting technologies for Linux
- ✦ And some for Windows
- ✦ Use After Free
- ✦ Hack browsers
- ✦ Hack facebook "for a friend"

You will actually learn:

- ✦ Intel x86
 - ✦ Architecture
 - ✦ CPU
 - ✦ Registers
- ✦ Linux
 - ✦ Userspace memory layout, stacks, heap
 - ✦ Syscalls
 - ✦ Sockets
 - ✦ Networking
- ✦ Programming Languages
 - ✦ Assembler
 - ✦ C
 - ✦ Python
 - ✦ Bash
 - ✦ (Ruby)

24.02.2017

Theory:

- ✦ 0x01 Intro (this)
- ✦ 0x02 Intro Technical
- ✦ 0x10 Intel Architecture
- ✦ 0x11 Memory Layout

Challenges:

- ✦ 0 Introduction to memory layout – basic
- ✦ 1 Introduction to memory layout - advanced

03.03.2017

Theory:

- ✦ 0x12 C Array and Pointers
- ✦ 0x30 ASM Intro
- ✦ 0x31 Shellcode
- ✦ 0x32 Function Call Convention
- ✦ 0x33 Debugging

Challenges:

- ✦ Challenge 8
- ✦ Challenge 9
- ✦ Challenge 3
- ✦ Challenge 7
- ✦ Challenge 50

10.04.2017

Theory:

- ✦ 0x41 Buffer Overflow
- ✦ 0x42 Exploit
- ✦ 0x44 Remote Exploit

Challenges:

- ✦ Challenge11
- ✦ Challenge12

17.04.2017

Theory:

- ✦ 0x51 Exploit Mitigation
- ✦ 0x52 Defeat Exploit Mitigation
- ✦ 0x53 Exploit Mitigation – PIE
- ✦ 0x54 Defeat Exploit Mitigation ROP

Challenges:

- ✦ Challenge14
- ✦ Challenge15

24.04.2017

Theory:

- ✦ 0x72 Linux Hardening
- ✦ Defeat Exploit Mitigation – Heap Intro
- ✦ Defeat Exploit Mitigation – Heap Attacks

Challenges:

- ✦ Challenge31

31.04.2017

Theory:

- ✦ Windows Exploiting
- ✦ Secure Coding
- ✦ Fuzzing

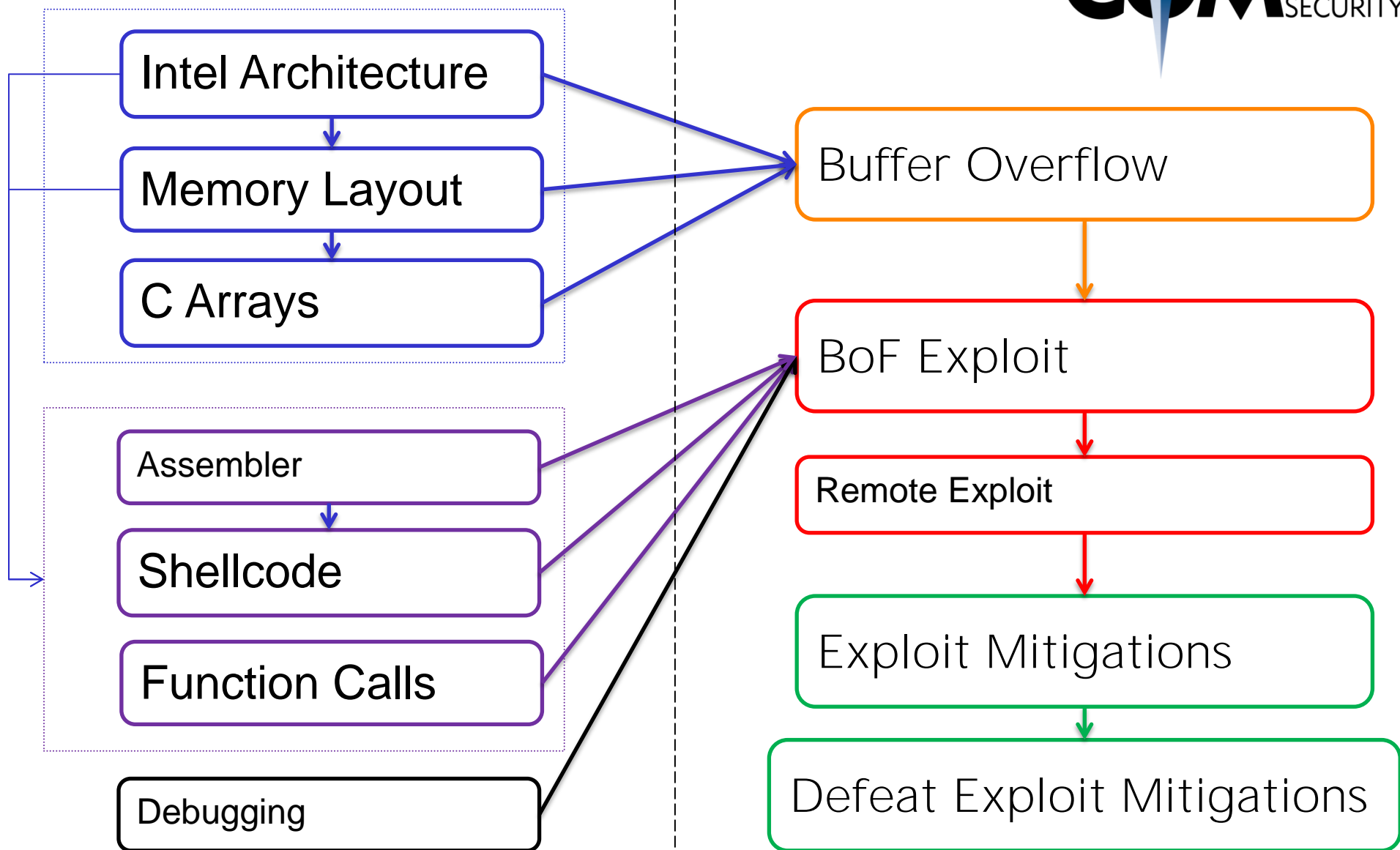
Challenges:

07.05.2017

Theory:

- ✦ Puffer
- ✦ Case Studies
- ✦ Questions

Challenges:



Exploit Mitigations

ASCII Armor

**Stack
Canary**

ASLR

PIE

DEP

Arbitrary Write

Overflow Local Vars

Heap Overflows

Brute Force

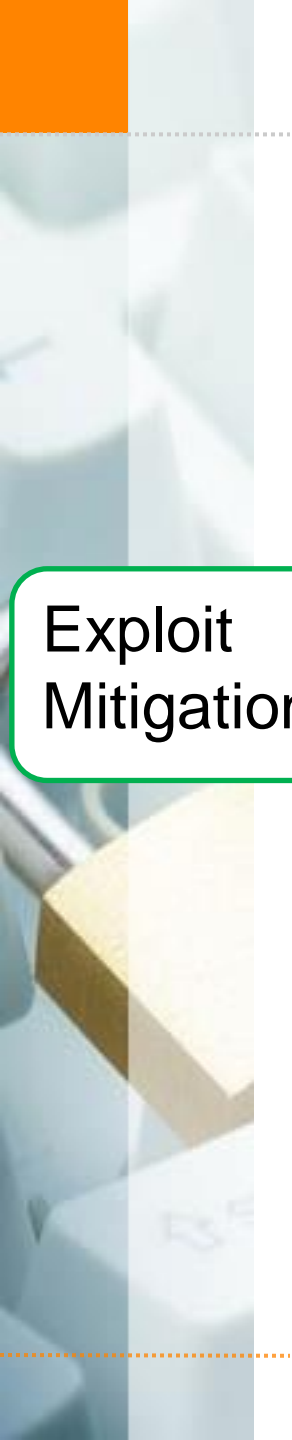
Partial RIP Overwrite

NOP Slide

Info Disclosure

Ret 2 PLT

ROP



And:



Windows Exploiting

Secure Coding

Fuzzing

Linux Hardening

Browser Security

Case Studies

What is (mainly) relevant for the oral exam?

- ✦ How does memory corruption work?
- ✦ How does an exploit work?
- ✦ What exploit mitigations exist?
- ✦ How can these exploit mitigations be circumvented?

