11. Oktober 2018, ECSM, Universität Duisburg-Essen

Return-Oriented Programming
Angriffe auf Browser

Prof. Dr.-Ing. Lucas Davi
Juniorprofessur für Informatik
Sichere Software Systeme
Universität Duisburg-Essen

Team

Prof. L. Davi

Dipl.-Ing. M. Rodler

MSc. S. Surminski

O. Draissi

N. Wittig

NEC

CROSSING

Forschungsbereiche

Software Sicherheit

- Zero-Days
- Programmfluss-integrität
- Speicher-randomisierung

Trusted Computing

- Remote attestation
- Trusted Platform Module (TPM)

Hardwarebasierte Sicherheit

- Intel Software Guard Extensions (SGX)
- ARM TrustZone
- Rowhammer


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Das Problem mit Sicherheitslücken in Software

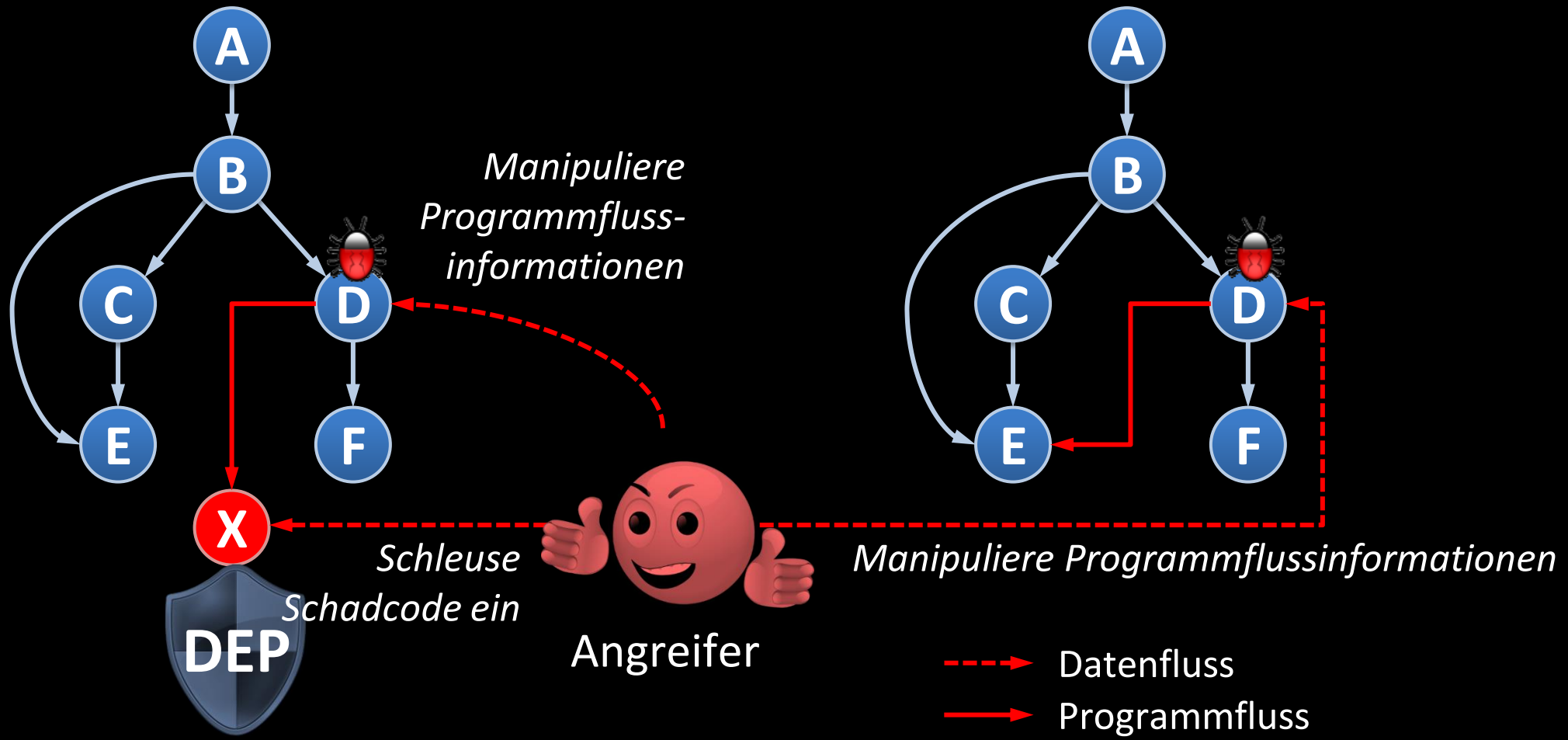
- Software wird immer anspruchsvoller und komplexer
- Die meisten Softwareentwickler sind keine Sicherheitsexperten

Wahrscheinlichkeit von Software Fehlern (Zero-Days) ist extrem hoch – man bedenke wie oft Software aus Sicherheitsgründen aktualisiert werden muss

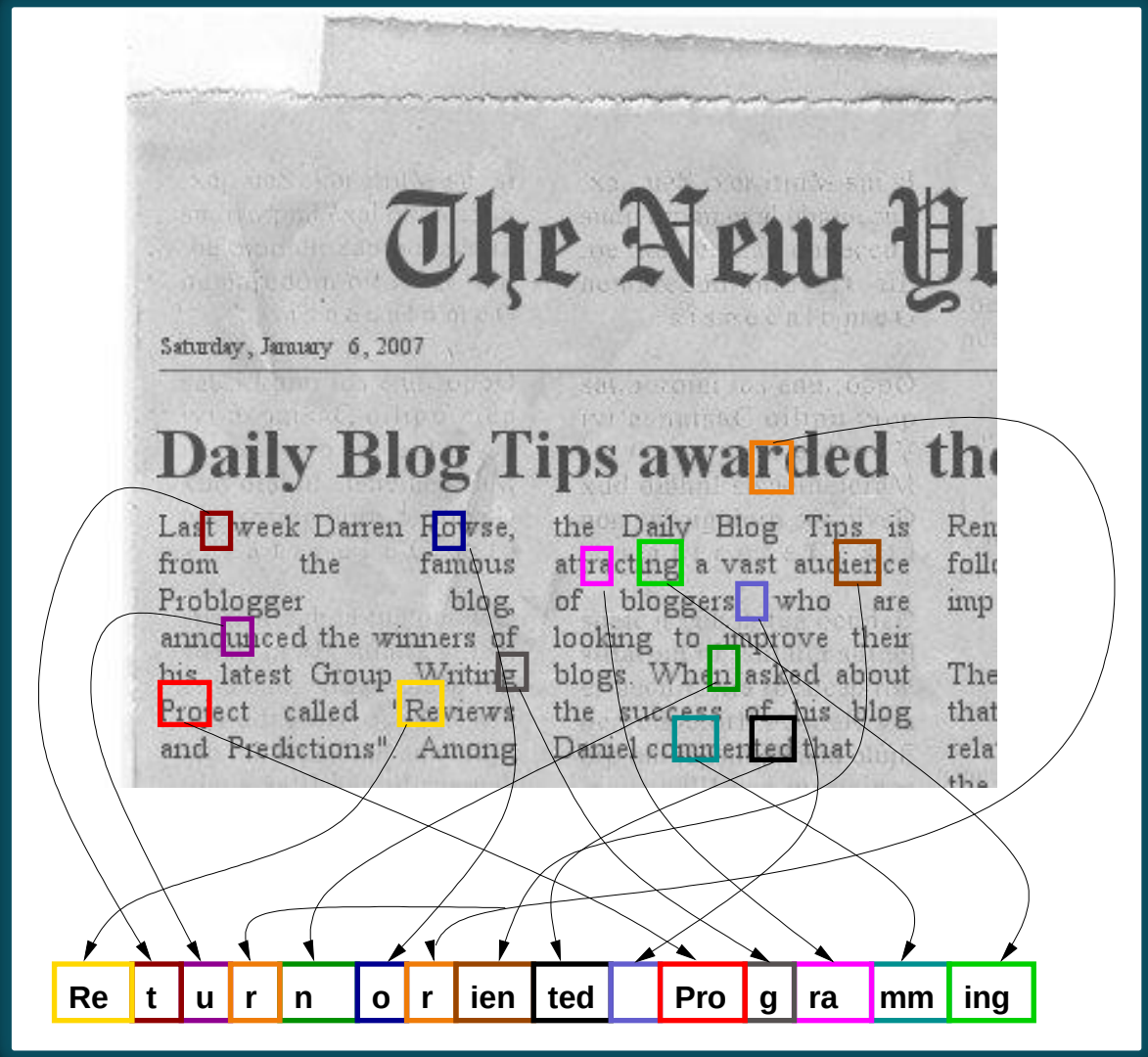
Wie können Software Fehler ausgenutzt warden?

Code-Injection Angriff

Return-Oriented Programming Angriff



Return-Oriented Programming (ROP)



Ausgewählte ROP Angriffe aus der Praxis

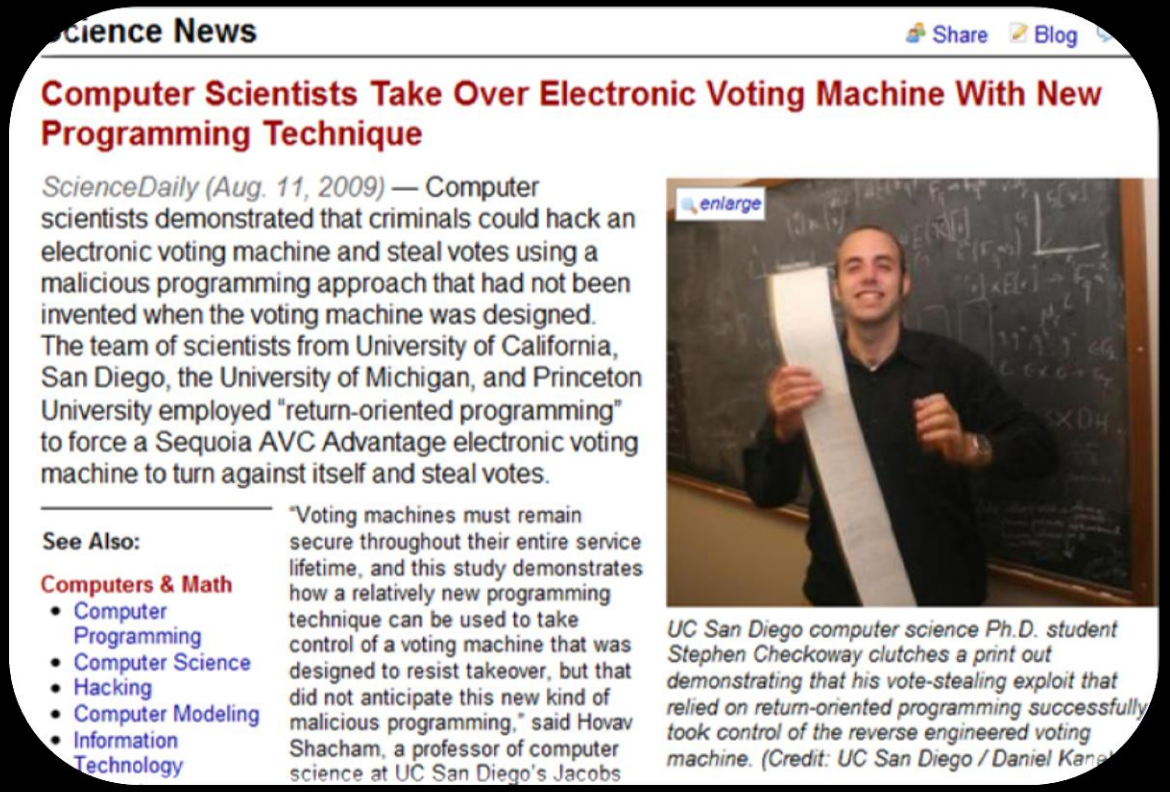
ROP Angriff auf iOS Safari Browser

Nutzer klickt auf einen bösen Link

Webseite mit bösartigen Programmcode wird geladen

SMS Datenbank wird an den Angreifer geschickt

Wahlmaschinen Hack


cience News

Share Blog

Computer Scientists Take Over Electronic Voting Machine With New Programming Technique

ScienceDaily (Aug. 11, 2009) — Computer scientists demonstrated that criminals could hack an electronic voting machine and steal votes using a malicious programming approach that had not been invented when the voting machine was designed. The team of scientists from University of California, San Diego, the University of Michigan, and Princeton University employed "return-oriented programming" to force a Sequoia AVC Advantage electronic voting machine to turn against itself and steal votes.

"Voting machines must remain secure throughout their entire service lifetime, and this study demonstrates how a relatively new programming technique can be used to take control of a voting machine that was designed to resist takeover, but that did not anticipate this new kind of malicious programming," said Hovav Shacham, a professor of computer science at UC San Diego's Jacobs

enlarge

UC San Diego computer science Ph.D. student Stephen Checkoway clutches a print out demonstrating that his vote-stealing exploit that relied on return-oriented programming successfully took control of the reverse engineered voting machine. (Credit: UC San Diego / Daniel Kan

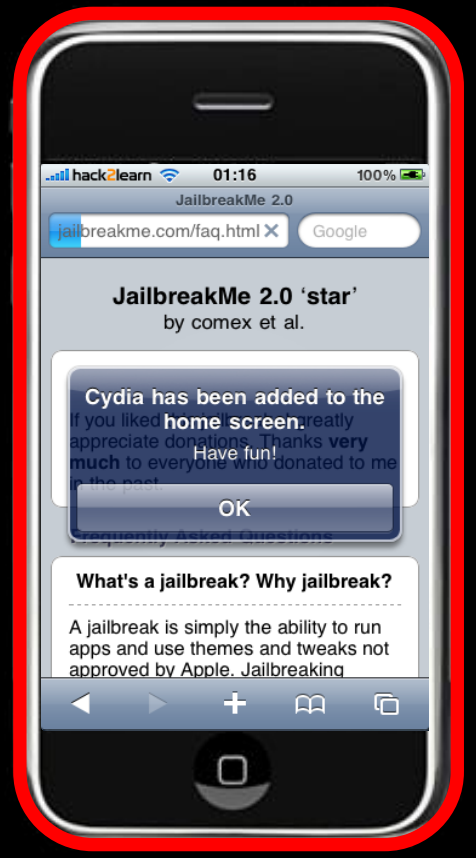
See Also:

Computers & Math
- Computer Programming
- Computer Science
- Hacking
- Computer Modeling
- Information Technology

Stagefright

ROP Angriffe auf Browser haben aber auch etwas Gutes an sich

Jaibreak über PDF Viewer des Safari Browsers

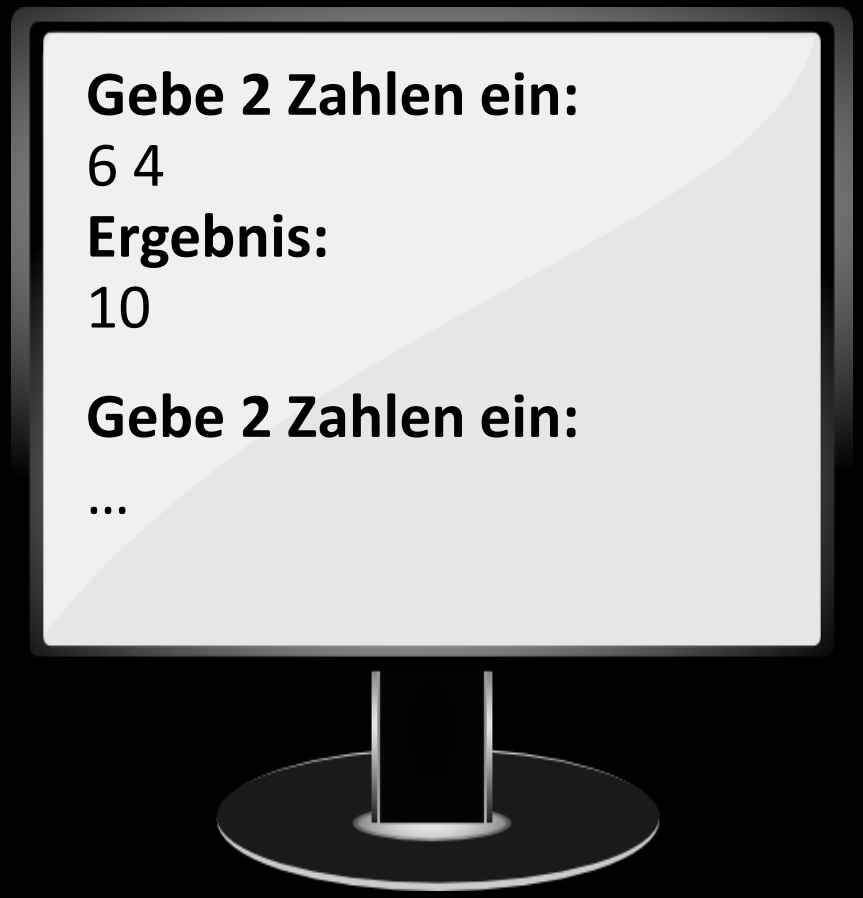


Download einer PDF Datei
http://www.jailbreakme.com/_/iPhone3,1_4.0.pdf

1) Nutze eine PDF Lücke um Safari zu kompromittieren
2) Starte den Jailbreak Prozess
3) Download von neuen Systemdateien
4) Jailbreak Prozess beendet

Wie funktioniert das Ausnutzen einer Software Sicherheitslücke?

Unser Beispielprogramm



Ausgabe auf dem Display

Ausgabe: “**Gebe 2 Zahlen ein:**”
Warte auf Eingabe von Zahl1 und Zahl2
Berechne: Zahl3 = Zahl1+Zahl2
Ausgabe: “**Ergebnis:**”
Ausgabe: Zahl3
Gehe zum Anfang

Mein Additionsprogramm

Kompilieren des Additionsprogramms

Ausgabe: “Gebe 2 Zahlen ein:”
Warte auf Eingabe von Zahl1 und Zahl2
Berechne: Zahl3 = Zahl1+Zahl2
Ausgabe: “Ergebnis:”
Ausgabe: Zahl3
Gehe zum Anfang

Mein Additionsprogramm als Textdatei

Kompilieren

CODE

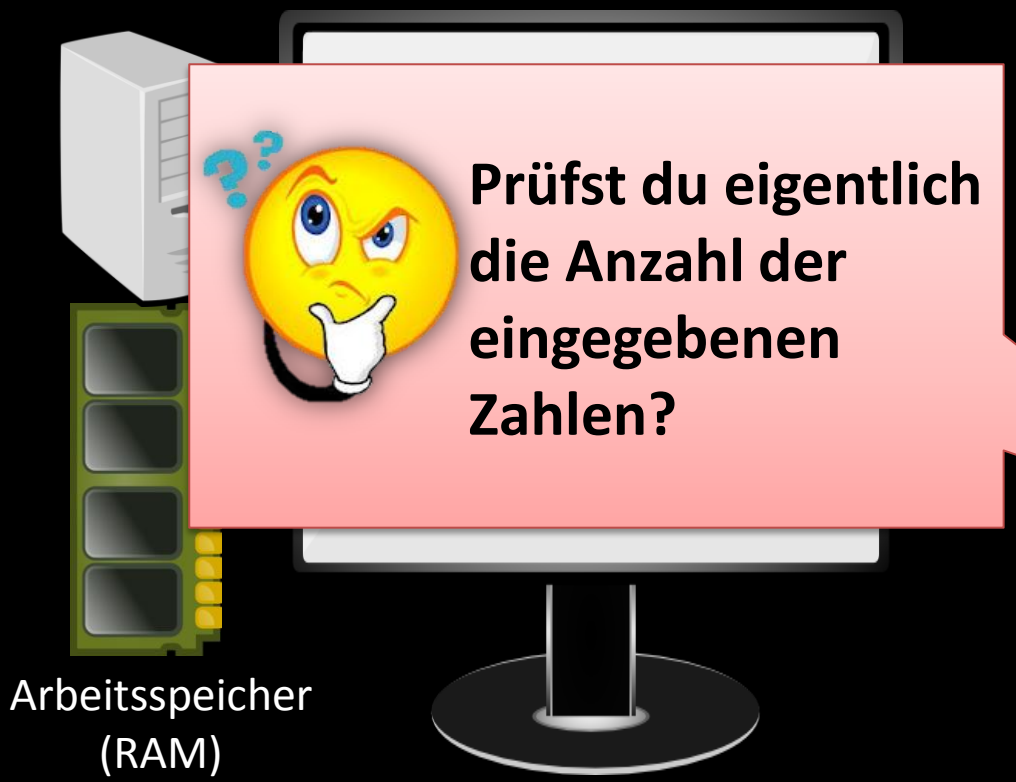
SCHREIB “Gebe 2 Zahlen ein:”
WARTE_AUF_EINGABE
LADE S1
LADE S2
ADD
SPEICHER S3
SCHREIB “Ergebnis:”
SCHREIB S3
SPRING S4

DATEN

S1: Zahl1
S2: Zahl2
S3: Zahl3
S4: Programmanfang

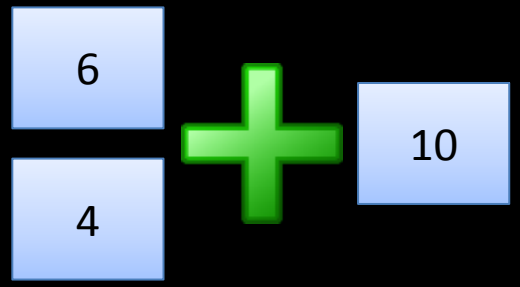
Das Additionsprogramm In Mikrobefehlen

Ausführen des Additionsprogramms



Arbeitsspeicher (RAM)

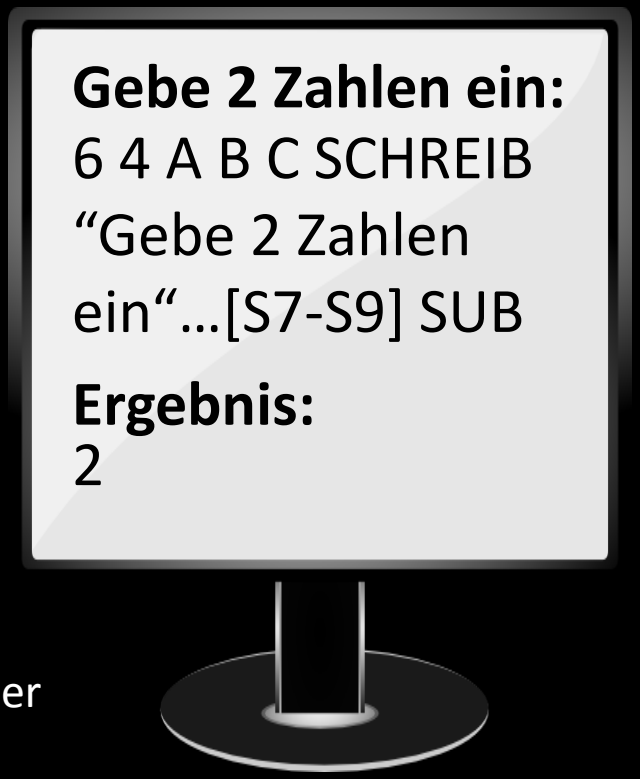
Prozessor



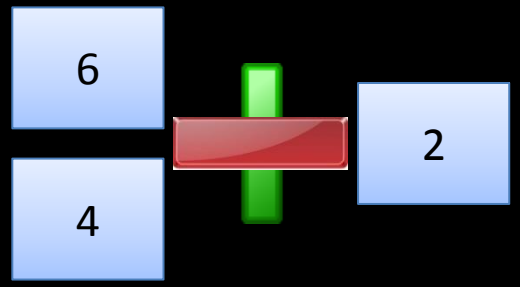
S1:	6
S2:	4
S3:	10
S4:	S6 (Programmstart)
S5:	
	SCHREIB “Gebe 2 Zahlen ein:”
S7:	WARTE_AUF_EINGABE
S8:	LADE [S1]
S9:	LADE [S2]
S10:	ADD
S11:	SPEICHER [S3]
S12:	SCHREIB “Ergebnis:”
S13:	SCHREIB [S3]
S14:	SPRING [S4]

Erster Angriff: Code Manipulation

Arbeitsspeicher (RAM)



Prozessor



	S1:	6
	S2:	4
	S3:	A
	S4:	B
	S5:	C
	S6:	SCHREIB “Gebe 2 Zahlen ein:”
IP →	S7:	WARTE_AUF_EINGABE
	S8:	LADE [S1]
	S9:	LADE [S2]
IP →	S10:	SUB
	S11:	SPEICHER [S3]
	S12:	SCHREIB “Ergebnis:”
IP →	S13:	SCHREIB [S3]
	S14:	SPRING [S4]

Abwehrmethode gegen Code Manipulation?

Verbiete die Veränderung von Code zur Laufzeit eines Programms!

Zweiter Angriff: Schadcode Einschleusen

IP →

S1:	6
S2:	4
S3:	10
S4:	S5 *(vorher S6)*
S5:	Install(Ransomware)
S6:	SCHREIB “Gebe 2 Zahlen ein:”
S7:	WARTE_AUF_EINGABE
S8:	LADE [S1]
S9:	LADE [S2]
S10:	ADD
S11:	SPEICHER [S3]
S12:	SCHREIB “Ergebnis:”
S13:	SCHREIB [S3]
S14:	SPRING [S4]

Abwehrmethode gegen Code Einschleusen?

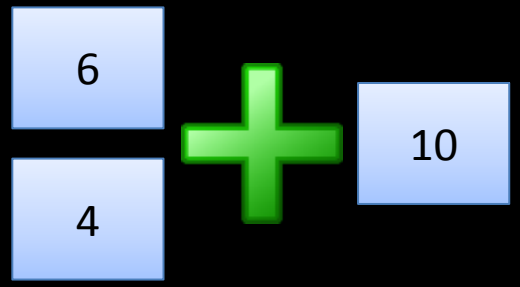
Verbiete die Ausführung von Code im Datenspeicher! (DEP)

Sind wir jetzt sicher gegen Software Angriffe?

Dritter Angriff: Code Wiederverwendung (ROP)

Arbeitsspeicher (RAM)

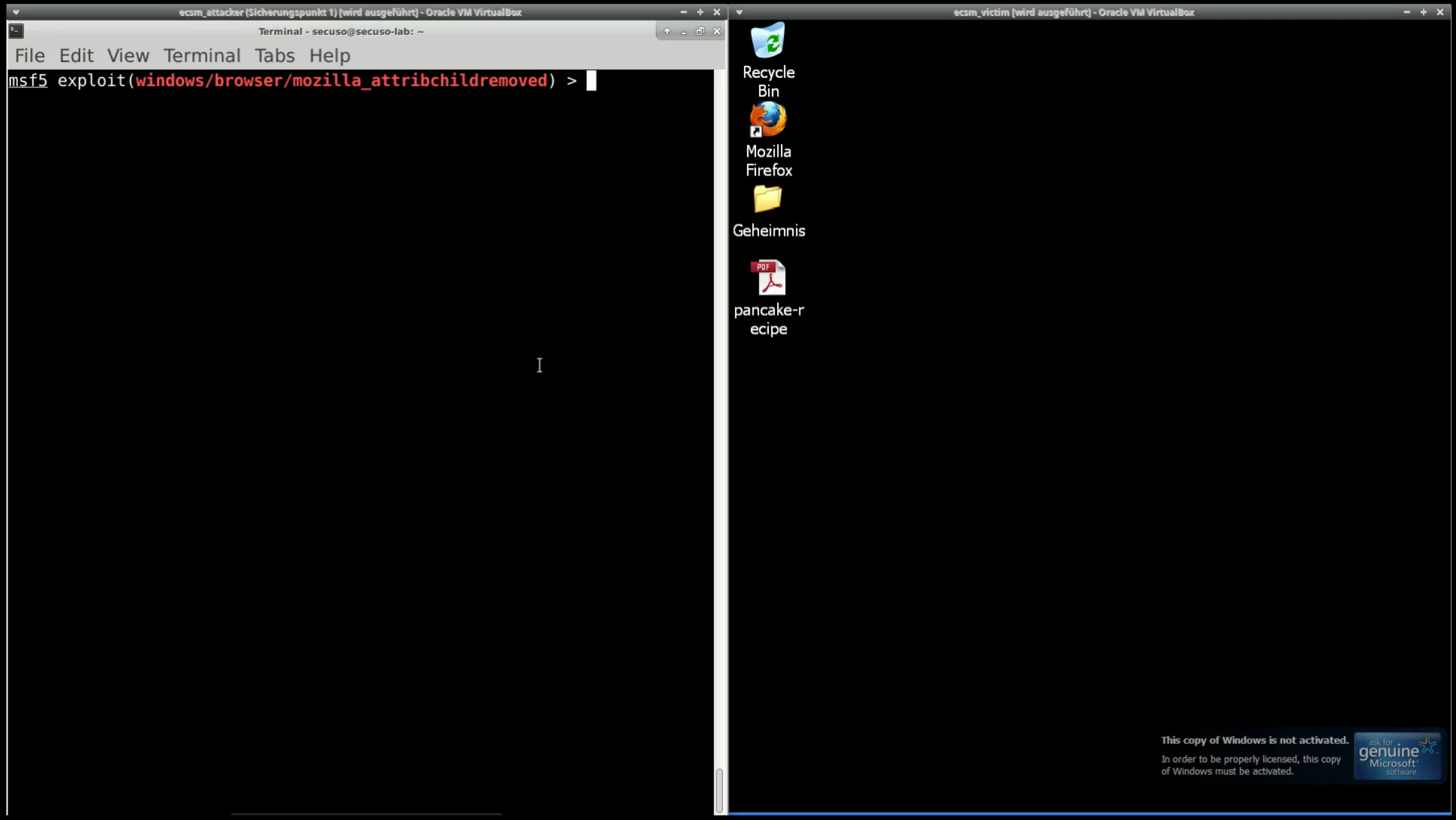
Prozessor



IP →

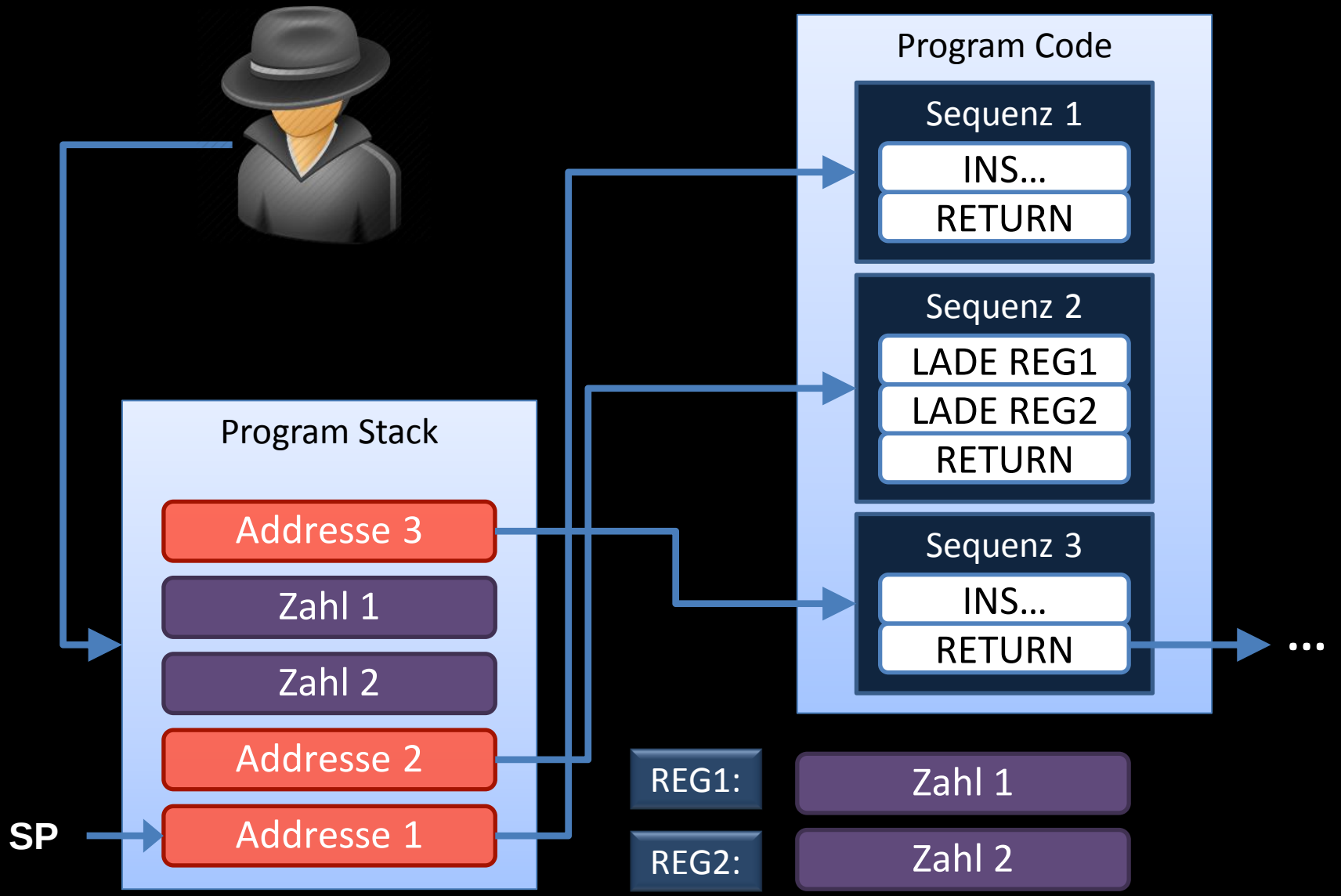
S1:	6
S2:	4
S3:	10
S4:	S8 *(vorher S6)*
S5:	
S6:	SCHREIB “Gebe 2 Zahlen ein:”
S7:	WARTE_AUF_EINGABE
S8:	LADE [S1]
S9:	LADE [S2]
S10:	ADD
S11:	SPEICHER [S3]
S12:	SCHREIB “Ergebnis:”
S13:	SCHREIB [S3]
S14:	SPRING [S4]

Wie mächtig sind ROP Angriffe im Kontext von Web Browsern?

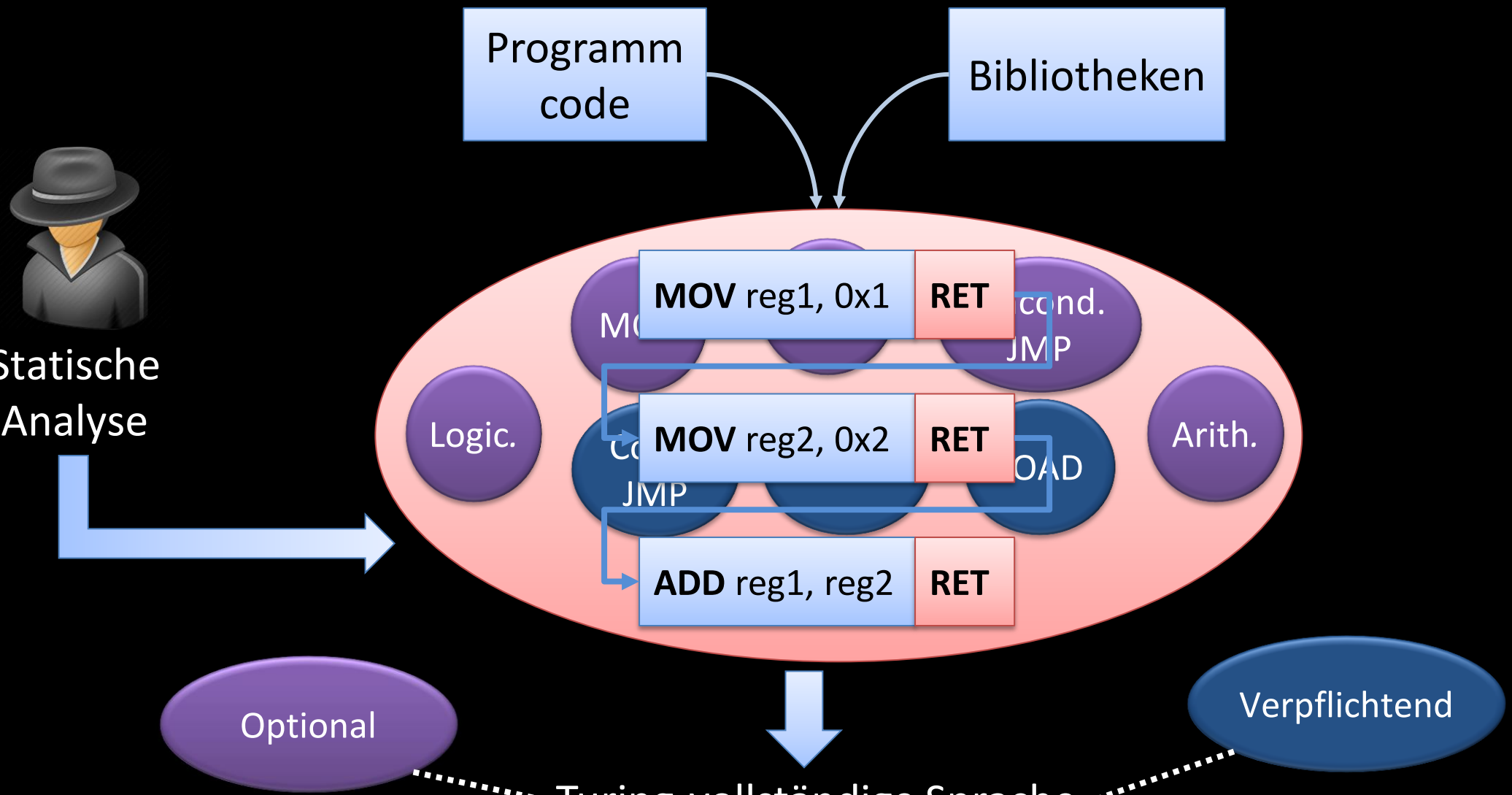

ecsm_attacker (Sicherungspunkt 1) [wird ausgeführt] - Oracle VM VirtualBox
Terminal - secuso@secuso-lab: ~
File Edit View Terminal Tabs Help
msf5 exploit(windows/browser/mozilla_attribchildremoved) >
ecsm_victim [wird ausgeführt] - Oracle VM VirtualBox
Recycle Bin
Mozilla Firefox
Geheimnis
pancake-recipe
This copy of Windows is not activated.
In order to be properly licensed, this copy of Windows must be activated.
ask for genuine Microsoft software

ROP Angriffsdetails

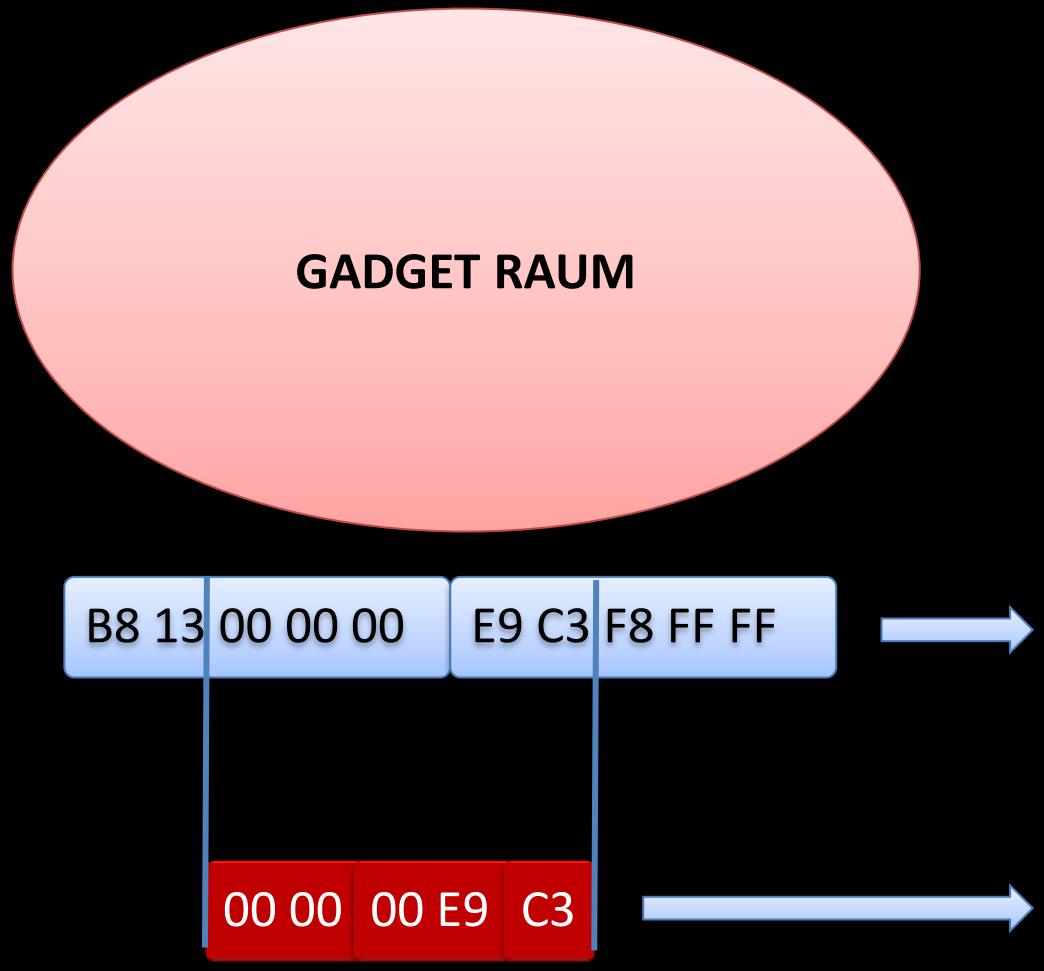
ROP Angriffstechnik



Entscheidend ist die Code Basis



PCs und Laptops sind besonders betroffen



Beabsichtigter Code

```
mov $0x13,%eax
jmp 3aae9
```

Unbeabsichtigter Code

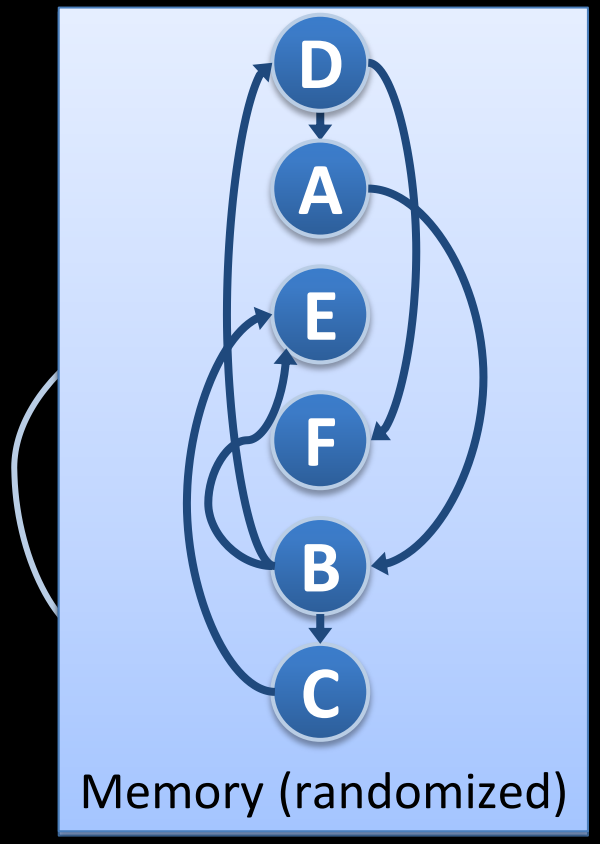
```
add %al,(%eax)
add %ch,%cl
ret
```

Wie können wir uns gegen diese Angriffe schützen?

Abwehrmethoden

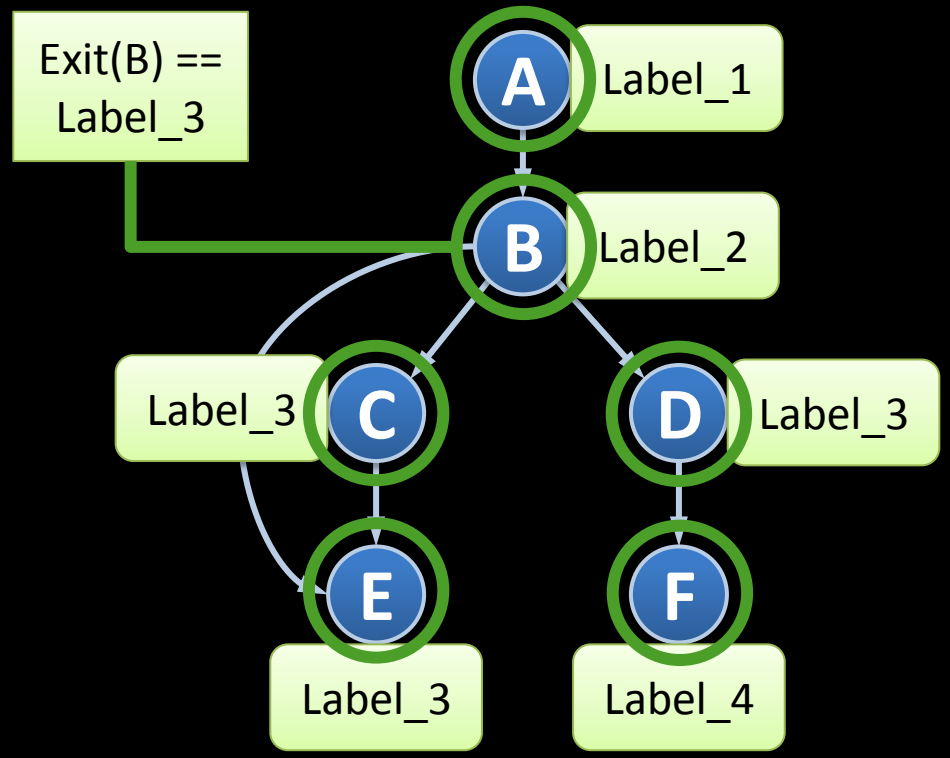
Randomisierung

[Cohen 1993 & Larsen et al., SoK IEEE S&P 2014]



Programmflussintegrität

[Abadi et al., CCS 2005 & TISSEC 2009]



Neue Sicherheitstechnologien

Intel CET

- Neue Intel Prozessoren sollen Control-Flow Enforcement Technology (CET) unterstützen
- Hardware-basierter Shadow Stack um Rücksprungadressen zu schützen

Microsoft CFG

- Applikationen für Windows 10 können mittels Microsoft Control-Flow Guard (CFG) geschützt werden
- Sicherheitscheck für Funktionsaufrufe

Google Clang-CFI

- Neues Compiler Feature um Control-Flow Integrity (CFI) für Funktionsaufrufe zu implementieren
- Anwendungsbeispiel ist der Chrome Web Browser

Was kann der Nutzer tun?

- Begrenzte Möglichkeiten
- Up-to-date Software und bald auch Hardware
- Skript-Ausführung eingrenzen
- Verdächtige Links nur in einer virtuellen Maschine öffnen

Zusammenfassung

- Return-Oriented Programming (ROP) Angriffe werden genutzt, um Sicherheitslücken in Software auszunutzen
- Diese Angriffstechnik wird insbesondere für Browser Angriffe genutzt
- Schlechte Nachricht
  - Der Nutzer kann sich nur begrenzt vor ROP Angriffen schützen, da diese Angriffe Zero-Day Lücken ausnutzen
- Gute Nachricht
  - Akademische und industrielle Forschungslösungen zur Verteidigung von ROP Angriffen werden immer effektiver und effizienter