Übung 7

Betriebs- und Kommunikationssysteme

Tutorium bei Alexander Rademann

Von Thore Brehmer und Jonny Lam

Aufgabe 1)

Directory Traversal: Ausnutzen einer Sicherheitslücke auf einem Webserver, indem man durch eingeben einer URL auf Daten zugreifen kann, die nicht dafür vorgesehen waren.

Buffer Overflow: Durch einen Pufferüberlauf, also wenn in einem reserviertem Speicherbereich durch einen Fehler zu große Daten (größer als der Speicherbereich) geschrieben werden, kann man z.B. die Rücksprungadresse mit anderen Daten überschreiben.

Backdoor: Umgehung von einer Zugriffssicherung durch eine vom Entwickler eingebauten Code oder auch Software, oder auch durch eine vom Trojaner installierte Software die das ermöglich.

Logic bomb: Programm, das nach bestimmten logischen Bedingungen für den Computer schädliche Aktionen auslöst. Diese Auslöser können z.B. das erreichen eines bestimmten Datum oder auch das erreichen einer fehlende Datei sein.

Trojan horse: Programm das als eine Anwendung getarnt ist, aber im Hintergrund eine andere Funktion erfüllt. Z.B. löschen von Daten oder senden von Daten (z.B. Passwörter).

Virus: Ein Programm, das sich selbst verbreitet, indem er sich in andere Dateien oder in den Bootbereich (enthält Informationen zum starten eines Betriebssystems) einfügt. Durch den PC-User gelangt das Virus in andere Systeme, indem er ein Medium woanders anschließt oder eine infizierte Datei öffnet. -> Wird mithilfe des PC-Users verbreitet

Worm: Ein Wurm verbreitet sich selbst, wie das Virus. Die Art wie es sich verbreitet ist jedoch anders, ein Wurm nutzt z.B. die bestehenden Anwendungen vom Computer z.B. die Email und verschickt sich an andere Emails und kopiert sich somit selber ohne dass der PC-User was machen muss. -> wird ohne die Hilfe des PC-Users verbreitet.

Bot: Programm, das automatisch verschiedene sich wiederholende Aufgaben ausführt, ohne die Hilfe eines Anwenders.

Rootkit: Rootkits sind mehrere Softwares, die ein Betriebssystem infiltrieren um Schadsoftware oder auch Dateien vorm Virenscanner verstecken.

b)

BIOS (basic input/output system):

-Firmware von x64/x86 PCs

- wird nach dem einschalten des PCs ausgeführt und liegt auf der Hauptplatine

-sorgt dafür, dass ein PC überhaupt funktionieren kann und startet ein Betriebssystem

UEFI(Unified Extensible Firmware Interface):

- Schnittstelle zwischen Firmware der Komponenten eines PCs und des Betriebssystems
- Nachfolger des BIOS
- Kann nur auf 64-Bit-Systeme booten
- Kann Drivers selber auswählen

Der Unterschied zwischen BIOS und UEFI ist, dass z.B. Updates bei UEFI direkt aus dem Internet geladen werden können und beim BIOS nicht. Z.B. brauchte man beim BIOS erstmal das Update und dazu noch eine extra Software um das Update zu installieren. Außerdem werden die Festplatten auch anders partitioniert, beim BIOS wurde mit MBR (Master Boot Record) partitioniert. Beim UEFI wird mit GPT (GUID Partition Table) partitioniert.

→ GPT unterstützt im Gegensatz zu MBR über 2 TB Speichervolumen. GPT unterstützt bis 128 Partitionen und MBR nur 4 primäre. Bei einer MBR-Festplatte werden die Partitionen und die Boot Informationen zusammen gespeichert, im Gegensatz zu GPT , wo die Partitionen am Ende des Datenträgers gespeichert werden. Bei der GPT Variante kann man mit den Sicherungen beschädigte Dateien wiederherstellen.

Ein Nachteil für UEFI ist, dass es nur auf 64-Bit-Systeme booten kann.

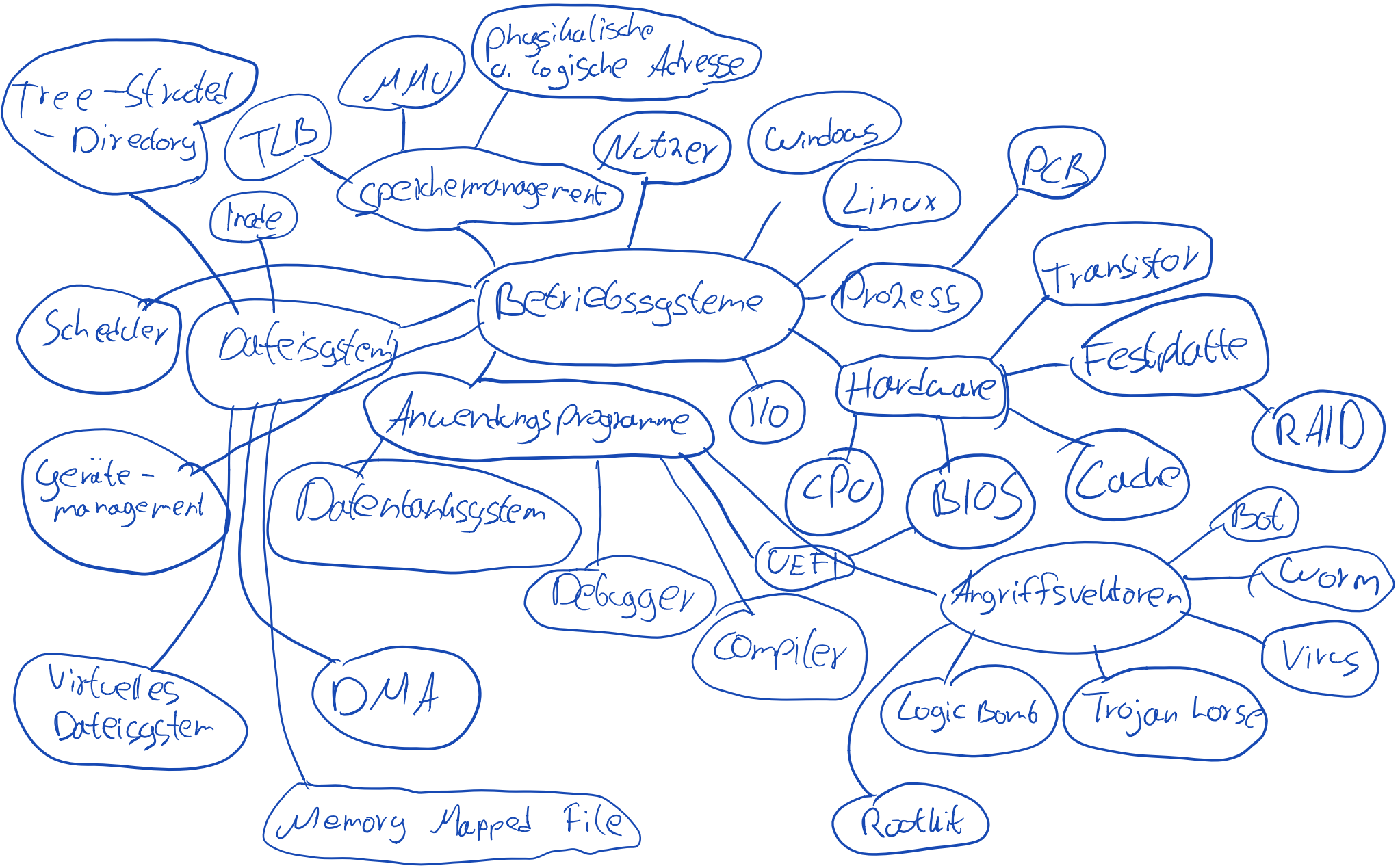
c)

Begriffe gut verstanden:

1) I/O
2) RAID
3) Tree-Structured Directory
4) BIOS
5) CACHE
6) Attack Vector
7) Scheduling
8) Inode
9) Virtual File System
10) DMA

Begriffe nicht gut verstanden:

1) Indexed Allocation
2) NTFS
3) Ext4
4) UEFI
5) Protocol
6) Internet
7) Stream Socket
8) Datagram Socket
9) World Wide Web
10) IPv6


Tree-Structed - Directory
TLB
MMU
physikalische u. logische Adresse
Inode
Speichermanagement
Netzer
Windows
Linux
PCB
Scheduler
Dateisystem
Betriebssysteme
Prozess
Transistor
Festplatte
RAID
Hardware
Anwendungsprogramme
I/O
Geräte-management
Datenbanksystem
CPU
BIOS
Cache
Debugger
UEFI
Bot
Worm
Angriffsvektoren
Compiler
Virus
Virtuelles Dateisystem
DMA
Logic Bomb
Trojan Horse
Memory Mapped File
Rootkit

Aufgabe 2)

a)

(named) Pipe: Datenstrom zwischen zwei Prozessen mithilfe eines Puffers nach dem Prinzip FIFO(First In – First Out).

Nachteil: Eine Pipe kann nur kleine Datenmengen enthalten.

Memory Mapped File(Speicherabbilddatei): Die Speicherabbilddatei enthält den Inhalt einer Datei im virtuellen Speicher. So kann die Datei mit mehreren Prozessen gelesen und bearbeitet werden.

Vorteil: gegenüber Sockets höhere Performance

POSIX Shared Memory Segments: Indem man die Speicherbereiche zweier Prozesse zusammenfügt, ermöglicht man so den Austausch gleicher Daten. → Speicher wird geteilt

Nachteil: Synchronisation der Prozesse → sicherstellen, dass nur ein Prozess auf die Informationen zugreift.

Unix Domain Socket: Sockets für den lokalen Rechner, statt IP-Adressen werden für die Kommunikation Dateien verwendet. Arbeiten verbindungsorientiert → müssen erst eine Verbindung zwischen zwei Prozessen aufbauen, die miteinander kommunizieren → Datenübertragung kann nicht mitgelesen werden. Da eine private Verbindung besteht müssen sie bei einem Server mit mehreren Prozessen gleichzeitig für jeden Kommunikationskanal einen eigenen Filedeskriptor einrichten.

Vorteil: sichere Verbindung.

Gibt es weitere Kommunikationsmöglichkeiten?

Ja, es gibt z.B. Message Queue oder ganz einfach Dateien austauschen.