Betriebssystemtechnik

Adressräume: Trennung, Zugriff, Schutz

I. Einleitung

Wolfgang Schröder-Preikschat

26. April 2017

Gliederung

Schutz von Prozessen

~ **in räumlicher Hinsicht** ⇝ BST

- Angriffssicherheit (*security*)
  - Schutz einer Entität vor seiner Umgebung
  - Immunität
  - verhindern, in einen Adressraum einbrechen zu können
- Betriebssicherheit (*safety*)
  - Schutz der Umgebung vor einer Entität
  - Isolation
  - verhindern, aus einem Adressraum ausbrechen zu können

~ **in zeitlicher Hinsicht** ⇝ EZS[3]

- Einhaltung von Terminen, Vermeidung von Interferenzen

~ **in energetischer Hinsicht** ⇝ *ffs.*

- Abfederung von Energiespitzen, Einhaltung von Energiebudgets

Adressraum

(vgl. auch [4])

- realer ~
  - reflektiert die phys(ikal)ischen Eigenschaften des Rechensystems
  - nicht zu jeder Adresse gibt es einen Adressaten (Speicher, Geräte)
  - die Bindung zwischen beiden ist fest, zur Laufzeit unveränderlich
    - Vorsicht: Speicherbankumschaltung
  - ungültige Adressen implizieren undefiniertes/fehlerhaftes Verhalten
- logischer ~
  - reflektiert die strukturellen Eigenschaften eines Programms
  - zu jeder Adresse gibt es immer einen (speicher-) residenten Adressaten
  - die Bindung zwischen beiden ist jedoch lose, zur Laufzeit veränderlich
  - ungültige Adressen – innerhalb des Adressraums – gibt es nicht
    - Vorsicht: Unterschied zwischen Segmentierung und Seitennummerierung
- virtueller ~
  - reflektiert die gegenwärtige/zukünftige Auslastung des Rechensystems
  - zu einer Adresse kann es zeitweilig einen nichtresidenten Adressaten geben
  - ansonsten „erben“ die Adressen alle Eigenschaften logischer Adressräume

Adressraumtrennung

Segmentierung oder Eingrenzung von Programmen:

- Maschinenprogrammebene (Ebene 3)
  - die Zentraleinheit[1] ermöglicht Immunität/Isolation in Hardware
    - MMU (Abk. *memory management unit*) . . . . . logischer Adressraum
    - MPU (Abk. *memory protection unit*) . . . . . phys(ikal)ischer Adressraum
  - das Betriebssystem[1] programmiert diese Hardware problemspezifisch
- Programmiersprachenebene (Ebene 5)
  - der Kompilierer[1] ermöglicht Immunität/Isolation in Software
  - Programme liegen in einer typsicheren Programmiersprache vor

Prozesse können die durch ihren logischen Adressraum jew. definierte Schutzdomäne nicht oder nur kontrolliert verlassen

- Abwesenheit von Prozessor- und Speicherfehlern vorausgesetzt
  - je nach Abstraktionsebene aber mit unterschiedlichem Wirkungsfeld

[1] Prozessor

Adressraumzugriff

Folge der Trennung: Adressraumgrenzen überschreitende Operationen

- durch Wechsel der Schutzdomäne
  - prozedurbasierte Technik
    - Systemaufruf, leichtgewichtiger Fernaufruf
    - Kontrollflussfortsetzung im anderen Adressraum
  - koroutinenbasierte Technik
    - Nachrichtenversenden, Fernaufruf
    - Kontrollflusswechsel hin zum anderen Adressraum
- durch Mitbenutzung (*sharing*) von Adressraumbereichen
  - Datenverbund (*data sharing*)
    - mit gleichförmigen oder ungleichförmigen Lese-/Schreibrechten
  - Gemeinschaftsbibliothek (*shared library*)
- durch Kombinierung beider Ansätze
  - Einrichtung eines Datenverbunds beim Wechsel der Schutzdomäne
    - aus dem „eingewechselten Adressraum“ heraus veranlasst
    - zum Lesen/Schreiben von Entitäten des „ausgewechselten Adressraums“

Adressraumschutz

Isolation schafft Immunität

- hardwarebasiert, segment- oder seitenoriertiert
  - MMU/MPU vergleicht Zugriffsart und Zugriffsrecht
    - Lesen, Schreiben, Ausführen – auch in Kombination
  - CPU begeht Ausnahme von normaler Programmausführung
    - lässt den aktuellen Maschinenbefehl in die Falle (*trap*) laufen
    - bewirkt damit eine synchrone Programmunterbrechung
  - Betriebssystem führt Ausnahmebehandlung [2] durch
    - Wiederaufnahmemodell: Fortsetzung des unterbrochenen Prozesses
    - Beendigungsmodell: Abbruch des unterbrochenen Prozesses
- softwarebasiert, datentyporientiert ⇒ sprachbasiert
  - Laufzeitsystem – d. h., der Prozess selbst – führt o. g. Funktionen durch
  - bestimmte Überprüfungen nimmt jedoch bereits der Kompilierer vor
    - alle statisch, also *vor* Laufzeit, entscheidbaren Zugriffsoperationen
- in Synergie beider Ansätze: Befähigung (*capability*, [1])
  - befähigungsbasierte Systeme sind kompliziert – obwohl ideal zum Schutz

Lernziele

Vorlesung

- *Wissen* zu Adressraumkonzepten von Betriebssystemen vertiefen
- *Verstehen* über (logische) Adressräume festigen
  - inhaltliches Begreifen verschiedener Facetten von Adressräumen
  - intellektuelle Erfassung des Zusammenhangs, in dem Adressräume stehen

Übung ⇝ mikrokern-ähnliches Betriebssystem

- *Anwenden* ausgewählter Vorlesungsinhalte für OOStuBS
- *Analyse* der Anforderungen an und Gegebenheiten von OOStuBS
- *Synthese* von Adressraumabstraktionen und OOStuBS
- *Evaluation* des erweiterten OOStuBS: Vorher-nachher-Vergleich

Überblick

- Systemaufruf; Befehlsformate der Machinenprogrammebene ÜV
  - ↪ Betriebssystemarchitektur: {Nano,Mikro,Makro,Exo}kern V
  - ↪ Schichtenstruktur von Betriebssystemen V
- Segmentierung, Seitennummerierung; Seitenkacheltabelle ÜV
  - ↪ Adressraummodelle, Benutzer- und Kernadressraum V
  - ↪ sprachbasierte Systeme, Systemprogrammiersprachen V
- Interprozesskommunikation, Semantiken ÜV
  - ↪ Kommunikationsabstraktionen V
  - ↪ Mitbenutzung (*sharing*) V
- Gemeinschaftsbibliotheken, dynamisches Binden V
- Nachlese, Ausblick V

Gliederung

Anforderungen

Vorkenntnisse

- Voraussetzung

Softwaresysteme	Programmiersysteme	Hardwaresysteme
▪ SP, SPiC	▪ C, C++, `make`	▪ x86, IA64
▪ BS ⇔ OOStuBS	▪ ASM	▪ Mehrkerner

- Erfahrung
  - in der hardwarenahen Programmierung
    - Gerätetreiber, Unterbrechungsbehandlung, Prozesswechsel
  - in der Fehlersuche/-beseitigung (*debugging*) in Betriebssystemen
    - nichtsequentielle Programme, mehrkernige Prozessoren
  - in der projektorientierten Entwicklung nativer Systemprogramme
- Erwartung
  - intrinsische Motivation, kritisches Denken, positive Fehlerkultur

Unterrichtstermine und -sprache

- Vorlesungs-, Übungs- und Rechnerzeiten:
  - auf `www4.cs.fau.de` dem Reiter „Lehre“ folgen
- Unterrichtssprache:

  - Vorlesung und Übung
  - Fachbegriffe
  - informatische Fachsprache
    - `www.inf.fu-berlin.de/inst/ag-ss/montagswort`
- Sachwortverzeichnis (in Arbeit und Überarbeitung)
  - `www4.cs.fau.de/~wosch/glossar.pdf`

Übungsbetrieb

- Tafelübung ⇝ „*learning by exploring*“
  - Anmeldung über WAFFEL[2] (URL siehe Leitseite von BST)
    - Freischaltung erfolgt nach der Vorlesung, heute im Tagesverlauf
  - Übungsaufgaben sind bevorzugt in Gruppen zu bearbeiten
- Rechnerarbeit ⇝ „*learning by doing*“, kein Tafelersatz
  - Anmeldung ist nicht vorgesehen, reservierte Arbeitsplätze s.o.
  - bei Fragen zu den Übungsaufgaben, Übungsleiter konsultieren
    - Email senden bzw. einfach vorbeischauen...

Der, die, das.
Wer, wie, was?
Wieso, weshalb, warum?
Wer nicht fragt, bleibt dumm!

[2] Abk. für Webanmeldefrickelformular Enterprise Logic

Prüfungsrelevante Studienleistung

5 ECTS
- BST
- 4 SWS (2 V + 2 Ü)
- Prüfungsgespräch
  - 20 Minuten
  - Stoff zu V + Ü

7,5 ECTS
- BST++
- 6 SWS (2 V + 2 Ü + 2 EÜ)
  - erweiterte Übung
  - ggf. auch Extraaufgabe
- Prüfungsgespräch
  - 30 Minuten
  - Stoff zu V + Ü + EÜ

- Bearbeitung aller Übungsaufgaben wird dringendst empfohlen
- Anmeldung zum Prüfungsgespräch per *E-Mail* an:
  `wosch@cs.fau.de`
  - angeben ob BST oder BST++
  - Termin oder Terminfenster mitsenden
    - Prüfungszeitraum (Ausnahmen bestätigen die Regel)

Gliederung

Kontakt

- Wolfgang Schröder-Preikschat, Prof. Dr.-Ing. habil.
  - Vorlesung
  - `http://www4.cs.fau.de/~wosch`

- Gabor Drescher, M. Sc.
  - Übungen
  - `http://www4.cs.fau.de/~gabor`

- Stefan Reif, M. Sc.
  - Übungen
  - `http://www4.cs.fau.de/~reif`

- Andreas Ziegler, M. Sc.
  - Übungen
  - `http://www4.cs.fau.de/~ziegler`

Literaturverzeichnis

[1] Dennis, J. B. ; Horn, E. C. V.:
Programming Semantics for Multiprogrammed Computations.
In: *Communications of the ACM* 9 (1966), März, Nr. 3, S. 143–155

[2] Goodenough, J. B.:
Exception Handling: Issues and a Proposed Notation.
In: *Communications of the ACM* 18 (1975), Nr. 12, S. 683–696

[3] Schröder-Preikschat, W. :
Echtzeitsysteme.
http://www4.informatik.uni-erlangen.de/Lehre/WS05/V_EZS, 2005 *ff.*

[4] Schröder-Preikschat, W. ; Kleinöder, J. :
Systemprogrammierung.
http://www4.informatik.uni-erlangen.de/Lehre/WS08/V_SP, 2008 *ff.*