

Eingebettete Systeme

Prof. Dr. rer. nat. Peter Gerwinski

2. Februar 2021

Eingebettete Systeme

<https://gitlab.cvh-server.de/pgerwinski/es>

- 1 Einführung**
- 2 Einführung in Unix**
- 3 TCP/IP in der Praxis**
- 4 Versionsverwaltungssysteme**
- 5 Bus-Systeme**
- 6 Echtzeit**
 - 6.1** Was ist Echtzeit?
 - 6.2** Echtzeitprogrammierung
 - 6.3** Multitasking
 - 6.4** Ressourcen
 - 6.5** Prioritäten
 - 6.6** Threads
- 7 Verschlüsselung**
 - 7.1** Verschlüsselungsverfahren
 - 7.2** Zertifizierung von Schlüsseln

6 Echtzeit

6.5 Threads

Parallelisierung

- Programme parallel ausführen: Prozesse jeweils eigener Speicherbereich
- Programmteile parallel ausführen: Threads gemeinsamer Speicherbereich
- in beiden Fällen:
Synchronisation über Semaphoren, insbesondere Mutexe

Ziele

- einfachere Programmierung nebenläufiger Aktionen
→ neue Probleme durch Synchronisation
- Nutzung mehrerer Prozessoren/Kerne

6 Echtzeit

6.5 Threads

Anwendungen

- GUI-Programmierung
- Kommunikations-Software
- Numerik

- Beispiel: Mumble-Partybot
- Übungsaufgabe: Chat-Software
- Übungsaufgabe: responsive GUI

6 Echtzeit

6.5 Threads

Übungsaufgabe: Chat-Software

- Benutzer tippen Chat-Messages ein.
- Nach Eingabe von ENTER soll die Message als ganze „animiert“ ausgegeben werden, d. h. mit einer geringen Verzögerung zwischen den einzelnen Zeichen, z.B. 1/20 Sekunde.
- Ein Bot schreibt gelegentlich die aktuelle Uhrzeit in den Chat.
- Irgendwann wird der Bot mit der Textausgabe kollidieren. Das Programm soll dieses Problem einerseits demonstrieren und andererseits zeigen, wie es sich durch Verwendung von Mutexen beheben läßt.
- Vorgabe: Lösung in C.
Optional: Lösung in weiteren Programmiersprachen.
- Hinweis: <https://www.thegeekstuff.com/2012/05/c-mutex-examples/>

6 Echtzeit

6.5 Threads

Übungsaufgabe: responsive GUI

- Ein Haupt-Thread wartet auf Ereignisse.
- Wenn diese eintreten, bearbeitet es sie und initiiert einen Neuaufbau des Bildschirms.
- Der Bildschirmaufbau erfolgt in separaten Threads, damit der Haupt-Thread sofort weiterarbeiten kann.
- Wenn durch die weitere Verarbeitung der Bildschirmaufbau hinfällig geworden ist, sollte der Haupt-Thread das dem Bildschirmaufbau-Thread signalisieren, damit dieser abbrechen kann.

7 Verschlüsselung

7 Verschlüsselung

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7 Verschlüsselung

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1).x$ Motivation

Man kann auch mit sehr merkwürdigen Objekten wie mit „ganz normalen“ Zahlen rechnen.

7 Verschlüsselung

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1) \cdot x$ Motivation

Man kann auch mit sehr merkwürdigen Objekten wie mit „ganz normalen“ Zahlen rechnen.

Anwendungen:

- Funktionsweise von Computern (\longrightarrow Rechnertechnik)
- Fehlererkennung
- Fehlerkorrektur
- Verschlüsselung
- Digitale Signaturen

7 Verschlüsselung

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1) \cdot (x + 1)$ Gruppen

Definition: Sei G eine Menge, $*$ eine Verknüpfung auf G . Wenn

- $\forall a, b, c \in G: (a * b) * c = a * (b * c)$ (Assoziativgesetz),
- $\exists e \in G: \forall a \in G: a * e = e * a = a$ (neutrales Element),
- $\forall a \in G: \exists a^{-1} \in G: a * a^{-1} = a^{-1} * a = e$ (inverses Element),

dann heißt $(G, *)$ eine *Gruppe*.

7 Verschlüsselung

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1) \cdot (x + 1)$ Gruppen

Definition: Sei G eine Menge, $*$ eine Verknüpfung auf G . Wenn

- $\forall a, b, c \in G: (a * b) * c = a * (b * c)$ (Assoziativgesetz),
- $\exists e \in G: \forall a \in G: a * e = e * a = a$ (neutrales Element),
- $\forall a \in G: \exists a^{-1} \in G: a * a^{-1} = a^{-1} * a = e$ (inverses Element),

dann heißt $(G, *)$ eine *Gruppe*.

Definition: Sei $(G, *)$ eine Gruppe. Wenn zusätzlich

- $\forall a, b \in G: a * b = b * a$ (Kommutativgesetz),

dann heißt $(G, *)$ eine *kommutative Gruppe*.

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1) \cdot (x + 2)$ Ringe

Definition: Sei R eine Menge; seien $+$ und \cdot Verknüpfungen auf R . Wenn

- $(R, +)$ eine kommutative Gruppe ist,
- $\forall a, b, c \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz),
- $\forall a, b, c \in R: (a + b) \cdot c = a \cdot c + b \cdot c$ und $a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributivgesetze),

dann heißt $(R, +, \cdot)$ ein *Ring*.

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1) \cdot (x + 2)$ Ringe

Definition: Sei R eine Menge; seien $+$ und \cdot Verknüpfungen auf R . Wenn

- $(R, +)$ eine kommutative Gruppe ist,
- $\forall a, b, c \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz),
- $\forall a, b, c \in R: (a + b) \cdot c = a \cdot c + b \cdot c$ und $a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributivgesetze),

dann heit $(R, +, \cdot)$ ein *Ring*.

Definition: Sei $(R, +, \cdot)$ ein Ring. Wenn zustzlich

- $\forall a, b \in R: a \cdot b = b \cdot a$ (Kommutativgesetz),

dann heit $(R, +, \cdot)$ ein *kommutativer Ring*.

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1) \cdot (x + 2)$ Ringe

Definition: Sei R eine Menge; seien $+$ und \cdot Verknüpfungen auf R . Wenn

- $(R, +)$ eine kommutative Gruppe ist,
- $\forall a, b, c \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativgesetz),
- $\forall a, b, c \in R: (a + b) \cdot c = a \cdot c + b \cdot c$ und $a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributivgesetze),

dann heißt $(R, +, \cdot)$ ein *Ring*.

Definition: Sei $(R, +, \cdot)$ ein Ring. Wenn zusätzlich

- $\forall a, b \in R: a \cdot b = b \cdot a$ (Kommutativgesetz),

dann heißt $(R, +, \cdot)$ ein *kommutativer Ring*.

Definition: Sei $(R, +, \cdot)$ ein (kommutativer) Ring. Wenn zusätzlich

- ein $e \in R$ existiert, so daß für alle $a \in R$ gilt: $a \cdot e = e \cdot a = a$ (neutrales Element),

dann heißt $(R, +, \cdot)$ ein *(kommutativer) Ring mit 1*.

7. $(x^2 - 1)$ Der Herr der Ringe: Manchmal ist $1 + 1 = 0$.

7. $(x^2 - 1) \cdot (x + 3)$ Körper

Definition: Sei K eine Menge; seien $+$ und \cdot Verknüpfungen auf K . Wenn

- $(K, +, \cdot)$ ein Ring mit 1 ist und
- $(K \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist,

dann heißt $(K, +, \cdot)$ ein *Körper*.

7 Verschlüsselung

7.1 Verschlüsselungsverfahren

Symmetrische Verschlüsselung:

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall

7 Verschlüsselung

7.1 Verschlüsselungsverfahren

Symmetrische Verschlüsselung:

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall
- spezieller Pseudozufall:
Enigma, RC4, DES, 3DES, IDEA, Rijndael, Blowfish, Twofish, CAST5, ...

7 Verschlüsselung

7.1 Verschlüsselungsverfahren

Symmetrische Verschlüsselung:

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall
- spezieller Pseudozufall:

Enigma, RC4, DES, 3DES, IDEA, Rijndael, Blowfish, Twofish, CAST5, ...

unsicher

Rijndael = AES, RC4 = CipherSaber

7 Verschlüsselung

7.1 Verschlüsselungsverfahren

Symmetrische Verschlüsselung:

Derselbe Schlüssel zum Ver- und Entschlüsseln

- Cäsar-Chiffre: monoalphabetische Substitution
- Vigenère-Chiffre: polyalphabetische Substitution
- Kryptanalyse: Kasiski-Test, Friedman-Test
- One-Time-Pad
- Pseudozufall
- spezieller Pseudozufall:
Enigma, RC4, DES, 3DES, IDEA, Rijndael, Blowfish, Twofish, CAST5, ...
unsicher
Rijndael = AES, RC4 = CipherSaber

Problem: geheimer Kanal für Schlüsselaustausch erforderlich

Lösung: *asymmetrische Verschlüsselung*

7 Verschlüsselung

7.1 Verschlüsselungsverfahren

Asymmetrische Verschlüsselung:

Verschiedene Schlüssel zum Ver- und Entschlüsseln

- mathematische Operation „schwierig“ umkehrbar
- Messung von „schwierig“: Landau-Symbol
- Beispiele:
 - Primfaktorzerlegung schwieriger als Multiplikation von Primzahlen
 - Logarithmus schwieriger als Potenz
- Verfahren:
 - RSA, DSA, ElGamal, ECRSA, ...

7 Verschlüsselung

7.1 Verschlüsselungsverfahren

Asymmetrische Verschlüsselung:

Verschiedene Schlüssel zum Ver- und Entschlüsseln

- mathematische Operation „schwierig“ umkehrbar
- Messung von „schwierig“: Landau-Symbol
- Beispiele:
 - Primfaktorzerlegung schwieriger als Multiplikation von Primzahlen
 - Logarithmus schwieriger als Potenz
- Verfahren:
 - RSA, DSA, ElGamal, ECRSA, ...

Problem: Verfahren sind langsam

Lösung: *hybride Verschlüsselung*:

asymmetrisches Verfahren verschlüsselt symmetrischen *Sitzungsschlüssel*

7 Verschlüsselung

7.1 Verschlüsselungsverfahren

Asymmetrische Verschlüsselung:

Verschiedene Schlüssel zum Ver- und Entschlüsseln

- mathematische Operation „schwierig“ umkehrbar
- Messung von „schwierig“: Landau-Symbol
- Beispiele:
 - Primfaktorzerlegung schwieriger als Multiplikation von Primzahlen
 - Logarithmus schwieriger als Potenz
- Verfahren:
 - RSA, DSA, ElGamal, ECRSA, ...

Problem: Verfahren sind langsam

Lösung: *hybride Verschlüsselung*:

asymmetrisches Verfahren verschlüsselt symmetrischen *Sitzungsschlüssel*

Problem: nicht-manipulierbarer Kanal für Schlüsselaustausch erforderlich

Lösung: *Zertifizierung*

7 Verschlüsselung

7.2 Zertifizierung von Schlüsseln

- S/MIME: hierarchische Baumstruktur
- OpenPGP: Web of Trust

7 Verschlüsselung

7.2 Zertifizierung von Schlüsseln

- S/MIME: hierarchische Baumstruktur
- OpenPGP: Web of Trust – kann auch hierarchische Baumstruktur sein

OpenPGP: E-Mail, spezielle Anwendungen, . . .

- Vertrauen in den Schlüssel: mathematisch berechenbar
- Vertrauen in die Person: persönliche Entscheidung

7 Verschlüsselung

7.2 Zertifizierung von Schlüsseln

- S/MIME: hierarchische Baumstruktur
- OpenPGP: Web of Trust – kann auch hierarchische Baumstruktur sein

OpenPGP: E-Mail, spezielle Anwendungen, . . .

- Vertrauen in den Schlüssel: mathematisch berechenbar
- Vertrauen in die Person: persönliche Entscheidung

S/MIME: Webseiten, E-Mail, spezielle Anwendungen, . . .

- Vertrauen in den Schlüssel: mathematisch berechenbar
- Vertrauen in die Person: wird vom Anbieter vorgegeben