Großer Beleg

Konzepte zur Vermeidung von Denial-of-Service-Angriffen in L4/DROPS

WS 2005/2006

Stefan Lebelt
lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

”Als DoS-Angriff
(Denial of Service attack, etwa: Dienstverweigerungs-Angriff)
bezeichnet man einen Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen.
In der Regel geschieht das durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von einem DDoS (Distributed Denial of Service)“

(wikipedia - [dos])

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

- DoS-Angriffe sind Angriffe auf die Verfügbarkeit von Diensten und Ressourcen.
- Verfügbarkeit bedeutet, dass Informationen dort und dann zugänglich sind, wo und wann sie von Berechtigten gebraucht werden.

[Pfi]

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Zwei grundlegende Arten von DoS:

- Ausnutzen von Programmier-/Implementationsfehlern
  - Bsp.: Ping of Death
  - Schwer allgemein zu bekämpfen
- Auslastung beschränkter Ressourcen
  - Bsp.: Mailbombing

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Warum DoS in L4/DROPS?

- Mikrokern-basierte Systeme
- Dienste als Userland-Server (Treiber, Speicherverwaltung, ...)
- Client-Server-Muster (Thread – Pager, Thread – DOpE, ...)
- Beschränkte Ressourcen (CPU, Speicher, Threadanzahl, ...)

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Mögliche Angriffe in L4/DROPS

- IPC
- Speicher
- Task-/Threadverwaltung
- Scheduling

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Mögliche Angriffe in L4/DROPS: IPC

- DDoS-Attacke auf die IPC-Warteschlange
- Stehlen von Prioritäten

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Mögliche Angriffe in L4/DROPS: Speicher

- Mapping-Attacke – Angriff auf den Kernspeicher
- Pager-Angriff („Speicherhunger“)
- Angriff auf dynamisch allokierende Server

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Mögliche Angriffe in L4/DROPS: Task-/Threadverwaltung

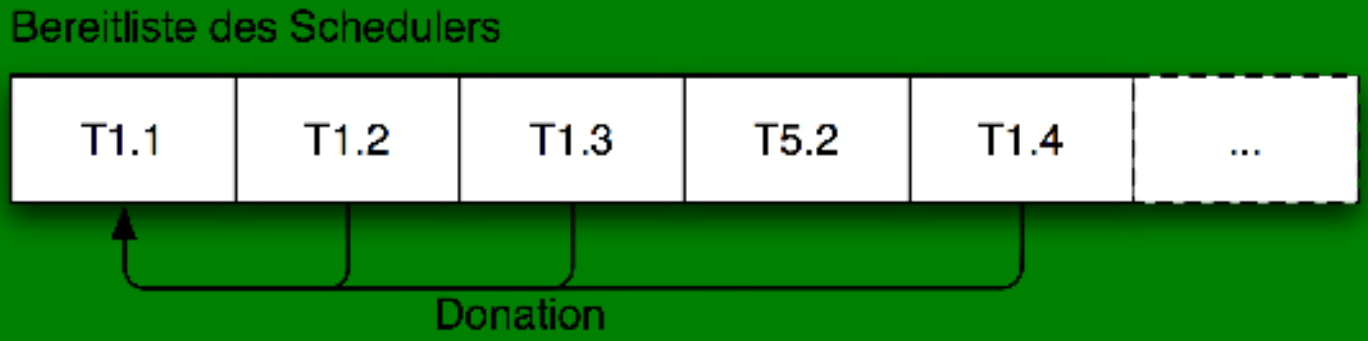
- Aktivitätsbomben
- allgemein DDoS (Infrastruktur)

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Mögliche Angriffe in L4/DROPS: Scheduling

- Missbrauch von Time-Slice-Donation



lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Zwei grundlegende Ansätze:

- Replikation (Beseitigung der Beschränkung)
  - *„If an object gets to many requests, replicate it“*
    (Andrew Tannenbaum)
- Kontrollierte Bereitstellung
  - Vergabe/Entzug
  - Kontrollierende Instanz ([Clans & Chiefs], Ressourcen-Manager, Endpunkte)
  - Policies (Quotas, Ökonomische Modelle)

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Forderungen

- Flexible Reaktionsmöglichkeiten auf „Speicherhunger“
- Vertrauenswürdige Memory-Donation an den Server
  - Mit L4-Bordmitteln **nicht** möglich!

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

„Dealman“: Idee

- Ressourcen-Provider als kontrollierende Instanz (Bsp.: Pager)
- Systemweiter Bankmanager („Dealman“) verwaltet Konten
- Ressourcen-Provider verlangen „Gums“ (γ) bei Allokation
- Möglichkeit der Übertragung von γ an andere Tasks/Threads

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

„Dealman“: Daten

- „Kontonummer“
- Kontingente mit id, Budget, Lendingparameter
- Capability (Zugriffsschutz)

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

„Dealman“: Dienste

- Abfragen von Kontingenten
- Dekrementieren/Inkrementieren von Kontingenten durch Ressourcen-Provider
- Überweisungen zwischen Konten und Kontingenten (Donation & Lending)

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

„Dealman“: Arbeitsweise des Pagers (Ressourcen-Providers)

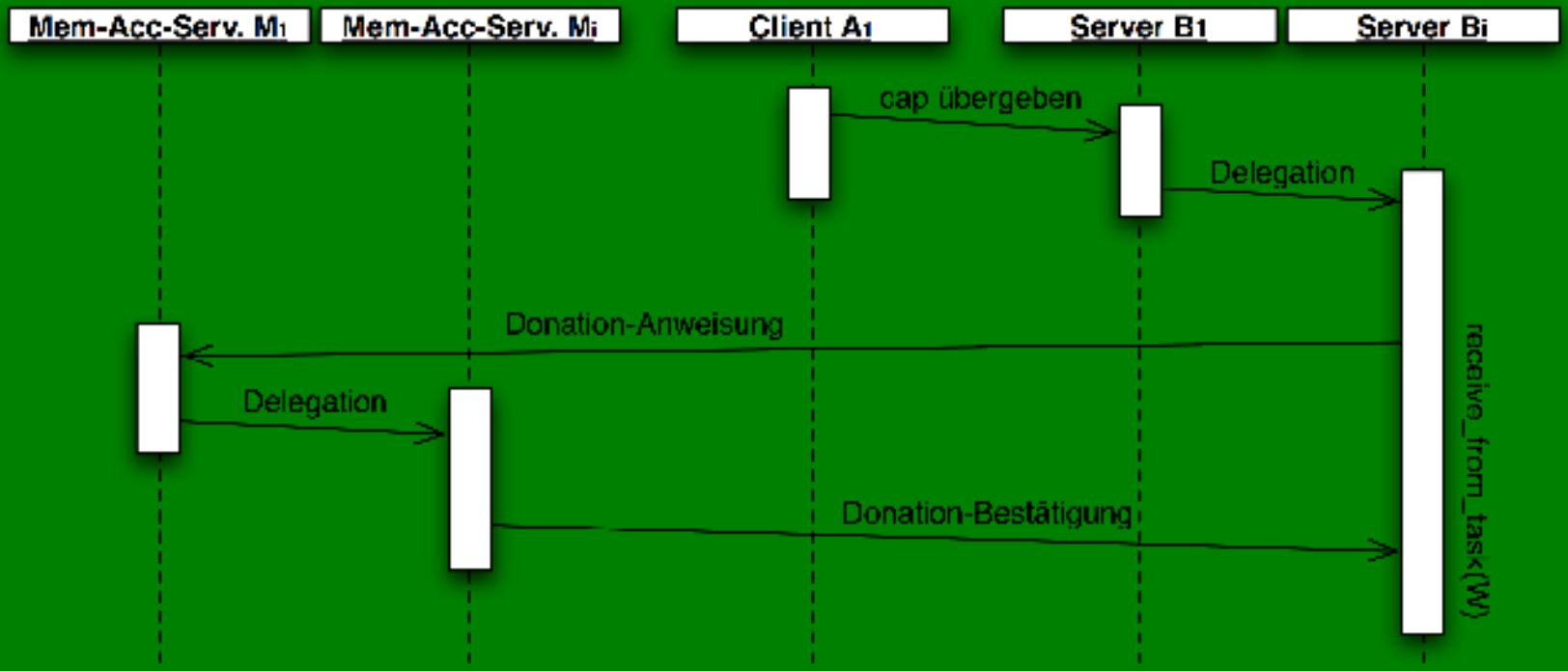
- Angabe eines Kontingents bei Speicherallokation
- Pager belastet das Kontingent und reserviert entsprechende Kacheln

- Rücknahme von Mappings bei negativ werdendem Kontingent
  - Pager wird vom „Dealman“ informiert
  - oder prüft zu bestimmten Zeiten die Kontingente seiner Clients

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

„Dealman“: Trusted-Donation-Protokoll

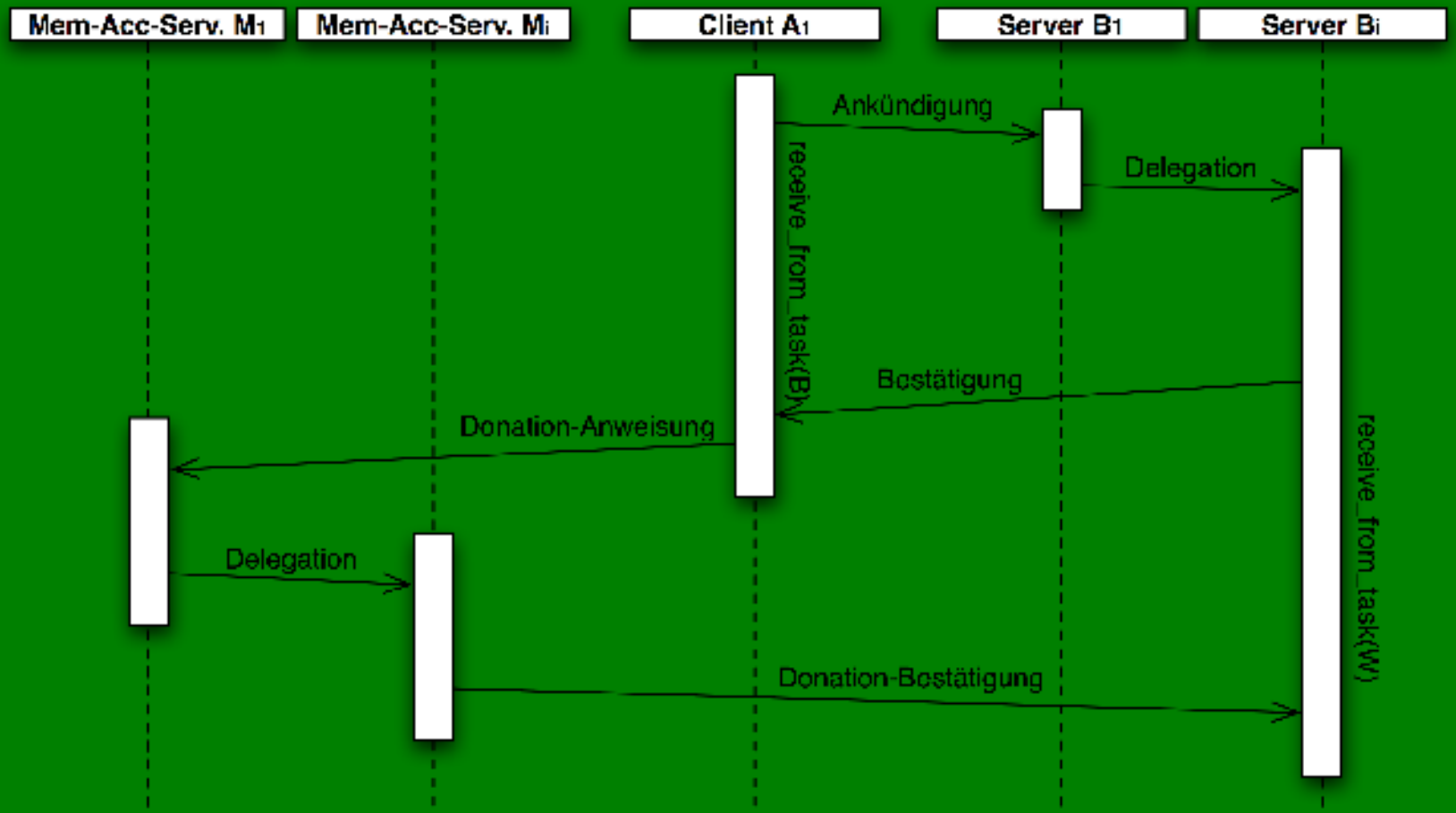


... ermöglicht auch Lending!

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

„Dealman“: Untrusted-Donation-Protokoll



lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Zusammenfassung

- Schutz der Ressourcen-Provider vor „Speicherhunger“
- Donation/Lending
- Nicht auf Speicher begrenzt

- Kontrollierte Bereitstellung von Ressourcen mit Hilfe von Ideen der ökonomischen Modelle
- Handel mit Ressourcen (teilweise auch unterschiedlicher Art)
- Lösung der meisten DoS-Probleme (insbesondere DDoS)

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Probleme

- Berufung auf experimentelle Ansätze (L4.sec)
- Ausgangspunkt: Ein-Prozessor-System
- Abwägung zwischen Kosten und Nutzen notwendig

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Ausblick – Es ist noch sehr viel zu tun!

- Implementation
- Anpassung der Basisdienste (Pager, DopE, simple_ts, ...)
- Untersuchung der Folgen von ökonomischen Systemen
  - Wie lassen sich volks- und betriebswirtschaftliche Gesetze und Strukturen nutzen und welche Auswirkungen hat das auf die Softwareentwicklung?
  - Wie effizient sind derartige Markt- und Wirtschafts-strukturen.
  - Sind derartige Markt- und Wirtschaftsstrukturen außerhalb von Schutzkonzepten überhaupt wünschenswert?

lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Vielen Dank für die Aufmerksamkeit!

22.12.2005 - 22:24:03
lebelt@os.inf.tu-dresden.de

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Dealman: Daten

Kontodaten

tid: B	cap: 8di

Ressourcen-Provider

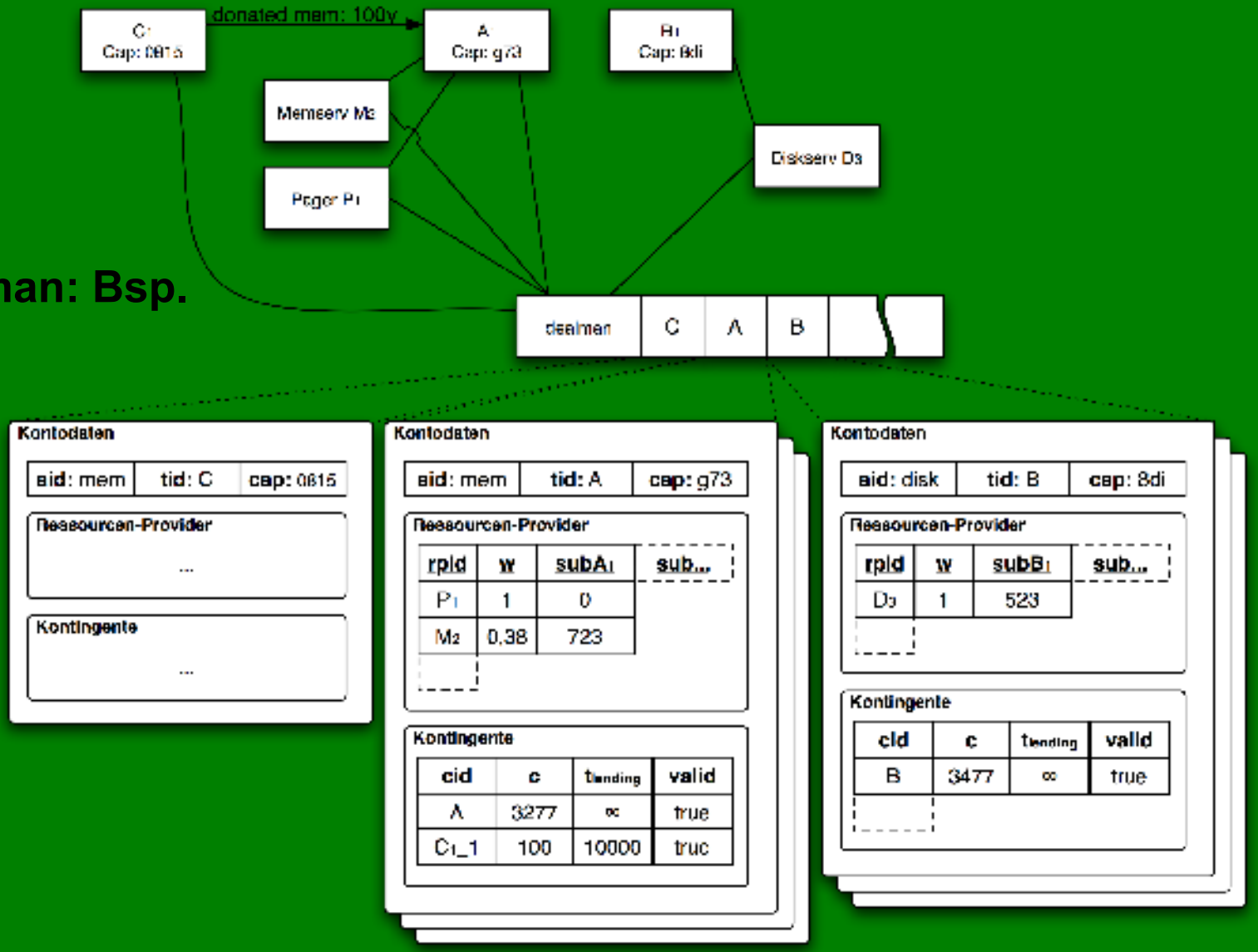
rpid	w	subB1	sub...
P3	1	523	

Kontingente

cid	c	tlending	valid
B	3477	∞	true

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Dealman: Bsp.



Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Systemstart

- Taskmanager τ_0 erzeugt alle TaskIDs
- τ_0 verwaltet Taskbaum (steht selbst in dessen Wurzel)
- τ_0 startet den „Dealman“
- τ_0 legt für sich selbst Konten für jede Ressource beim „Dealman „ an
- τ_0 ermittelt Angebot jeder Ressource und schreibt sich entsprechende Menge an Gums auf den jeweiligen Konten gut
- τ_0 erzeugt alle notwendigen Tasks, erzeugt deren Konten und „überweist“ jeweils bestimmte Beträge

Konzepte zur Vermeidung von DoS-Angriffen
in L4/DROPS

Taskerzeugung

Der Thread T1 möchte eine neue Task S erzeugen.

- T1 stellt eine entsprechende Anfrage beim Taskmanager τ_0.
- τ_0 prüft durch Abfrage des Task-Kontostandes von T beim ”Dealman“ , ob noch Tasks erzeugt werden dürfen. Falls ja passiert folgendes:
  - τ_0 legt beim Dealman“ neue Konten für die neue Task S an.
  - τ_0 überträgt eine bestimmte Menge an Gums der Konten von T auf die entsprechenden Konten von S .
  - τ_0 reduziert das Task-Konto von T um den Preis für eine neue Task.
  - τ_0 trägt S unterhalb von T in den Taskbaum ein.
  - τ_0 erzeugt S .

Bitte klicken Sie um die Präsentation zu beenden ...