

# SISTEMI OPERATIVI

Note:

Renzo Davoli

voglio scrivere TUTTO quello che ha detto il prof.  
(TUTTO a parte cose che "non reputo inserenti" alla lezione...)  
scrivo usando i COLORI:

■ ROSSO: per le date nel formato ANNO-MESE-GIORNO  
per parole con definizioni in blu

■ BLU per i nomi delle slide (esempio 00-intro.pdf)  
per definizioni e frasi che "se alzo gli occhi"  
dal removable note che il prof sta leggendo  
o parlando di cose scritte sulle slide

■ GRIGIO informazioni: "aggiunte da me":

- per indicazioni riguardanti le slide  
ad esempio "a che pagina siamo?"
- parti del discorso riguardanti di cosa sta  
parlando ad esempio "questo" (...)
- oggetti mancanti se lo reputo utile
- ricerche per quanto riguarda sigle (aggiunte da me)  
o link o cose cercate dal prof
- RiASSUNTI fatti dal prof
- messaggi e commenti del prof importanti

■ NERO: Tutto quello che dice (o non so se dovrei scrivere in blu  
poiché non alzo gli occhi alle slide ...).

Sistemi operativi anno 2021-2022 registrazione: 2° semestre

2022-02-25

p+1

slide 00-intro.pdf

Ieri abbiamo visto queste belle cose abbiamo visto cosa abbiamo fatto. Il Sistema Operativo è un livello di astrazione e l'importante è che fornisce un API in maniera tale che il processo utente venga confinato controllato in maniera tale che il processo corrente possa, anche qui c'è la metafora con il mondo reale, convivere civilmente con processi che condividono l'ambiente di lavoro. Il Sistema Operativo è un gestore di risorse, rende tutto più facile. Macchina Estesa, dipende dall'hardware, rende i programmi portabili. Abbiamo lavorato nello storia, volendo tornare qui (allo storia) un attimo perché "ciò che avviene in passato non è detto che non sia utile anche nel futuro". Questa (00-intro.pdf pag 22 Generazione Z (1955-1965)) che sembra un'architettura antica, desueta in realtà è usata ma non in sistemi general-purpose per esempio chi di voi ha giocato con un arduino sa che non si può dire che abbia un sistema operativo, ma proprio un monitor, oppure chiamato loader per l'arduino. Cioè l'arduino altro non è che un microcontrollore, adesso se ne usano di vario genere, compreso adesso c'è anche l'arduino con il nuovo chip della raspberry pie, comunque quello classico è un atmega

di qualche genere diciamo per molti arduini è il 328 e che sarebbe un debole sistema però per inserire, per caricare il programma avrebbe bisogno di un device esterno. L'arduino è di fatto un microcontrollore con in più un loader, un loader che viene precaricato, che viene mantenuto in una eeprom (più che in una eeprom in una non volatile... una eeprom). Arduino atmega non è una macchina di Von Neumann è una macchina di Harvard, quindi ha due memorie separate, una per i programmi e una per i dati. Nella memoria per i programmi che è

non volatile, per essere un arduino viene precaricato un piccolo programma, che può essere simile a questo monitor, che all'accensione o al reset per pochi secondi si ferma e guarda se sta arrivando dati dalla seriale emulata su USB e se in questi pochi secondi arrivano dati li interpreta come un programma da caricare, sempre nella parte programma oltre il loader. Quindi assomiglia molto a questo (gen. 2) vedete il compilatore Fortran se voi avete l'arduino e il primo programma tipico dell'arduino blink, viene caricato blink e fa quello che deve fare poi resettate/riaccendete/caricate un altro programma e fate altre cose. Quindi come vedete queste architetture ritornano in altri ambienti, non si può dire che sia un sistema operativo

è molto embrionale come sistema.

(va a pag 37 dicendo che abbiamo visto le cose in mezzo...)

Ecco abbiamo visto tante funzionalità che possono avere i sistemi operativi. I sistemi operativi si riconoscono dall'interfaccia delle system call dalla loro API. E abbiamo visto che ci sono delle funzionalità che ci possono essere o non essere e che se ci sono o non ci sono si evince dal fatto se l'interfaccia delle systemcall di questi sistemi prevede o meno funzionalità chiamate specifiche per queste funzioni. Se manca tutta la classe di systemcall per definire chi è l'utente del processo corrente e cambiare l'utente del processo corrente il sistema non sarà multi-user, ma sarà pensato per fare programmi senza protezione tra utenti e così via. Oltre alle cose classiche ci sono altre funzionalità del sistema operativo che possono esserci o non esserci e queste caratterizzano sistemi operativi per usi specifici, per esempio i sistemi operativi possono supportare o no il PARALLELISMO (pag 37). Cosa è il parallelismo? Lo dice la parola, la capacità di fare più operazioni contemporaneamente. Un processore standard normale, un singolo CORE, fa una cosa sola in un'unità di tempo. Quindi abbiamo visto che i sistemi operativi capaci di funzionare su singolo processore o eseguono codice del KERNEL o eseguono codice applicativo e possono dall'uno all'altro o da Kernel a user

caricando uno stato o da user a Kernel perché avviene una richiesta del processo a un altro evento asincrono. Come possono essere i sistemi paralleli? I sistemi paralleli possono essere Single Instruction Multiple Data (SIMD) detti anche sistemi vettoriali. Quindi questi sistemi fanno più cose contemporaneamente, ma in realtà eseguono la stessa istruzione su dati diversi, su vettori, su sequenze di dati in modo che l'operazione venga fatta nello stesso momento su tanti dati. O se no ci sono le Multiple Instruction Multiple Data (MIMD) che sono quelle che eseguono programmi differenti su dati differenti. Quindi per esempio se avete un sistema multicore, un sistema multicore è una macchina parallela di tipo MIMD. E voi conoscete dei sistemi SIMD? Li avete mai visti? Pensate che sono dei processori che per come sono fatti velocizzano le operazioni che devono essere fatte contemporaneamente su grandi quantità di dati. Non vi viene in mente un esempio? Bepo!

Studente: forse nella lavorazione delle immagini sui tanti pixel

Sì, e chi fa l'elaborazione delle immagini gestendo tanti pixel? Le SCHEDE VIDEO, e infatti queste schede video poi talvolta vengono utilizzate chiamandole con il nome di GPU (Graphics Processing Unit) per fare elaborazioni dove la stessa operazione deve essere fatta su grandi quantità di dati. Per esempio l'implementazione

dell'evoluzione di una rete neuronale. Per cui abbiamo un vettore che ci dà tutti gli stati di eccitazione dei vari neuroni, abbiamo la matrice con i pesi che ci indica quanto lo stato di un neurone debba propagarsi allo stato di un altro e per far evolvere la rete bisogna che questi calcoli vengano svolti su tutti i neuroni che compongono la rete neuronale. E quindi: una macchina SIMD è molto comoda per questo. Un altro modo di classificare macchine parallele è quello di guardare quanti CORE/processori ci sono. Ci possono essere sistemi a basso parallelismo, pochi processori in genere molto potenti, o sistemi massicciamente paralleli, un gran numero di processori che possono anche avere potenza non elevata

(pag 38) Un altro tipo di classificazione dei sistemi paralleli sono sistemi TIGHTLY COUPLED, quindi sono sistemi dove i core collaborano all'interno di un architettura che prevede il bus di comunicazione a memoria condivisa, è questo il modello dei sistemi Personal Computer Multicore, dove avete ... che ne so... 2, 4, 8 core, però questi CORE condividono il bus, la memoria. ok? E invece sistemi LOOSELY COUPLED sono sistemi dove ogni unità di elaborazione è un processore con la sua memoria (memoria privata), e i suoi canali di comunicazione ed è collegato con altri processori, secondo una determinata TOPOLOGIA. ok? Normalmente i sistemi tightly

coupled usano pochi processori, i sistemi loosely coupled usano tanti processori. Perché secondo voi non si fanno sistemi tightly coupled con 256 processori / core ? Prepol

studente: Perché più aumentano i processori più sarà il numero di processori che nello stesso momento chiederanno l'accesso alla memoria e quindi...

Esattamente! Perché essendo un bus a memoria condivisa diventa collo di bottiglia. Quindi non si ottengono prestazioni perché diventa elemento critico il bus perché è vero che si può spendere di più e tentare di ottenere dei bus più performanti più veloci però c'è un limite fisico alla cosa. Mentre invece ci sono state sperimentazioni, per esempio la CONNECTION MACHINE era una macchina che aveva 65.536 processori collegati fra loro con una topologia ad IPERCUBO. Che cos'è un CUBO?

"Non si capisce un cubo" :D no... (lasagna) ...

dimensioni	1	2	3	...	N
cubo	• - •	! - !	! - !	! - !	e poi potete continuare!

 Questo é un cubo. Ma questo é un particolare cubo.  
E il cubo di dimensione 3. Esistono cubi di TUTTE le dimensioni. Il cubo di dimensione uno  $\bullet$ . Cubo di dimensione 2  $\square$ . Cubo di dimensione 3  $\boxtimes$ . E poi potete continuare. Come potete creare il cubo di dimensione  $N+1$ ? Per fare il cubo di dimensione  $N+1$  prendete 2 cubi di dimensione  $N$  e collegate tra loro i nodi corrispondenti. Quindi qui abbiamo un cubo di dimensione 1  $\bullet$ , qui ne ho preso 2  $\bullet$  e li ho collegati assieme  $\boxtimes$ . Qui ho preso 2 cubi di dimensione 2  $\square$  e li ho collegati assieme  $\boxtimes$ . Se volessi passare alla dimensione 4 già ancora si può vedere nello spazio fate due cubi concentrici, uno dentro l'altro e collegate i nodi. OK? Questo é correlato ai numeri binari. Qui  $\bullet$  avete un bit 0 o 0 o 1. Qui  $\boxtimes$  avete fatto due copie e quindi il primo bit vi rappresenta a quale copia volete accedere e il secondo bit, il bit meno significativo é il bit all'interno del cubo precedente. Per fare un cubo in più il primo bit vi indica a quale cubo del livello precedente scegliete e poi avete l'indirizzo nel cubo più basso. Quindi collegando i processori secondo un IPERCUBO con 65.536 punti, vuol dire che é un cubo di dimensioni 16 (infatti  $2^{16} = 65.536$ ). La cosa bella é che ogni processore

può parlare con ogni altro processore facendo non più di 16 passi, nonostante ci siano 65.536 processori.

La connection machine è fallito, perché secondo voi?

L'idea della connection machine era quella di prendere dei processori a bassa potenza e ne mettere insieme dei numeri enormi. (un esempio di loosely è la connection machine).

Anche se un processore non è una valvola, anche i processori hanno la loro possibilità di guastarsi, e mettendone insieme 65.536 uno ha la probabilità di guastare un processore 65.536 volte quella di un processore singolo. Questo è uno dei fattori e l'altro è mentre con un sistema / i sistemi che abbiamo / i nostri portatili che hanno  $N$  core questi sistemi vengono utilizzati spesso anche con programmi che non sono adatti all'elaborazione parallela, ma perché avete bisogno di fare più cose quindi mettete un processo che non è parallelo che funziona su un processore mentre un altro funziona in quell'altro per utilizzare proficuamente delle architetture di questo genere tutti gli algoritmi che andate a scrivere devono essere pensati per funzionare lì sopra.

Perché non ha senso mandare lì sopra l'esecuzione di un processo sequenziale imperativo standard.

Perché userà un processore e ne avete ... e andrà piano come un singolo processore. ok? Quindi comunque esistono sistemi loosely coupled

anche magari con meno processori e... o forse oggi rinascono ma rinascono nella forma di SISTEMI DISTRIBUITI (nag 40 poi torniamo a 39). Cioè invece di pensare a una macchina singola con tanti processori si dice "prendiamo tanti sistemi come sistemi singoli (con processore, memoria... come tanti personal computer) e poi facciamo in modo di considerare tutto questo enorme insieme di macchine convenzionali come un sistema unico". ok? Ed è l'architettura che stanno usando per fare i nuovi supercomputer. avete sentito Leonardo?... Se poi andate anche molto più vicino all'INFN in area morassutti (ci si arriva a piedi) avete in mente dove è il dipartimento di fisica? Se andate a vedere i siti online ci sono sistemi di elaborazione che i fisici usano tantissimo per fare elaborazioni delle tracce degli acceleratori, elaborano dati che vengono dal CERN. Vedete che lì avete distese e distese di "rack" con nei "rack" dei server, ma quei server non sono dei server singoli: quei server vengono visti come un unico sistema di elaborazione che coinvolge tutte queste macchine. E quindi se volete la differenza tra sistema massivamente parallelo (loosely coupled) e sistema distribuito è una differenza labile, il concetto è simile, solo che mentre

si pensava di fare una topologia, una struttura, una macchina specifica nei sistemi distribuiti vengono viste tante macchine convenzionali come un sistema unico. Qual'è il problema? qui (connection machine) veniva studiata una rete specifica per l'elaborazione, in questo caso tutta la topologia di collegamento, la parte di connessione tra processori viene fatta con sistemi specifici di rete. Qual'è il problema nei sistemi distribuiti? Siccome sono sistemi di rete e non delle architetture di bus interne come quelle loosely coupled, hanno maggiore latenza e questo si ripercuote sugli algoritmi e sullo studio di come sfruttarli appieno. Questo è più o meno una descrizione hardware di come sono fatte le macchine.

Come impatta tutto questo sui sistemi operativi?

(pag 39) Parliamo di sistemi paralleli, sistemi multicore, sistemi tightly coupled. I sistemi operativi più diffusi usano MULTIPROCESSING SIMMETRICO (SMP). Cosa significa? che tutti i processori vengono gestiti nello stesso modo. "Non c'è un processore più quale degli altri" citando Orwell :D. Tutti i processori eseguono una copia identica del sistema operativo e eseguono processi. Quindi qual'è il problema? L'abbiamo già in parte visto, che questi vari processori vivono come il processore singolo quindi eseguono processi, succede una cosa, viene chiesta una systemcall, arriva un interrupt, vuole eseguire il Kernel, esegue il Kernel e fa .... Però il problema è che se ci sono più processori

che vogliono eseguire il Kernel, questi processori hanno strutture dati in comune. E quindi occorre fare in modo che si coordinino nell'accedere alle strutture dati. E, ripasso dal primo semestre, siccome i vari core i vari processori hanno disabilitazione degli interrupt indipendenti occorre utilizzare altre davorerie, altre soluzioni per creare sistemi di mutua esclusione, ed è per questo che sono nati gli spin-lock. Quindi per fare dei sistemi operativi SMP occorre che i processori forniscano delle istruzioni per consentire spin-lock, quali test & set, atomic swap, e la coppia di istruzioni lock-load store-conditional che è la coppia di istruzioni che consente di fare test & set su processori RISC. I processori RISC non possono fare due cose in un colpo solo quindi sono due istruzioni, ma sono fatte in maniera che la seconda fallisce se è successo qualcosa tra la prima e la seconda. L'altra alternativa è MULTIPROCESSING ASIMMETRICO quindi si può pensare di avere un processore master che gestisce il Sistema Operativo, gestisce l'assegnamento dei processi ai vari processori, e gli altri processori sono solo slave che eseguono i singoli processi come viene indicato dal processore master. (pag 41) SISTEMI DISTRIBUITI invece si comportano in modo diverso, appaiono come un'unica macchina. Un esempio di Sistema Operativo Distribuito lo potete pensare come quello del nostro laboratorio. Se accedete al laboratorio esistono tante macchine, le riconoscete perché di fianco al login di ogni macchina

c'è scritto il nome alla quale vi collegate. Sono nomi di personaggi d'opera .... Però quando accedete (anche remotamente via SSH) alla fine non vi interessa niente a quale macchina voi avete fatto accesso. Il sistema è tutto allineato. Avete la vostra home directory dovunque voi siate (non come i sistemi delle aule, in cui abbiamo una home directory staccata in ogni aula quindi le nostre preferenze...). E ciò che non vedete è che ci sono dei sistemi di installazione, aggiornamento di tutto il sistema distribuito che sono condivisi. Quindi se c'è da aggiornare il sistema non è che i tecnici del nostro dipartimento vadano di macchina in macchina ad aggiornare il sistema, ci sono dei meccanismi per tenere tutto il sistema distribuito allineato con quello che serve. Quindi in questo caso quello che ci serve dal punto di vista dei Sistemi Operativi per dare questa situazione è ovviamente condivisione efficace del file system, poi occorre database condivisi per quello che sono utenti, password, gruppi e così via, possono esserci meccanismi per distribuire il carico fra computer se volete utilizzarli per fare elaborazione massiva/massiccia. (pag 42) Andiamo in un'altra classe di sistemi in realtà poco conosciuti, i sistemi REAL TIME, penso che abbiate sentito questo termine solo che di solito non vengono definiti correttamente. REAL TIME non significa veloce, può essere tranquillamente lento, dipende dal problema che dovrete risolvere. La definizione esatta di sistemi real-time la trovate qui (pag 42, i linki sono disponibili sulla pagina del corso):

## Definizione: Sistemi real-time

Sono i sistemi per i quali la correttezza del risultato non dipende solamente dal suo valore ma anche dall'istante nel quale il risultato viene prodotto.

Vi dico che i sistemi real-time sono i sistemi per i quali il risultato è corretto non solo se è corretto nel proprio valore, ma se è corretto nel tempo in cui viene prodotto. OK? Quindi tecnicamente "se io progetto un sistema per dire ... devo trovare la risposta alla vita, l'universo in ogni cosa ma non ci deve mettere meno di 200 anni" è real time. Perché se quello mi risponde a 199 anni la risposta è sbagliata perché gli avevo creato un vincolo temporale, ora chiaramente questo è uno scherzo con citazione di Douglas Adams, ma ... perché ovviamente quello che interessa è avere un risultato entro un determinato tempo. Però non è detto che sia... l'importante è che sia deterministico, non ci interessa che sia veloce, che sia veloce abbastanza per il problema che andiamo a risolvere. (pag 43) Infatti abbiamo due tipi di sistemi real-time: HARD real-time e SOFT real-time. Quelli hard real-time sono quelli con effetti catastrofici se il vincolo temporale non viene rispettato. Purtroppo in questi giorni è tornata per vicinanza geografica alla mente il problema della centrale di Černobyl'. Una centrale nucleare ha un sistema di controllo, un sistema di controllo che come pensate è un sistema realizzato

con dei sistemi di elaborazione quindi materia nostra. Questo sistema non è poi... nelle centrali a Fissione... non è poi un sistema tanto elaborato perché ci sono dei meccanismi di rallentamento della reazione nucleare e quindi se la temperatura diventa troppo elevata occorre limitare, occorre ridurre la velocità della reazione. Nelle vecchie centrali avevano delle barre di grafite che venivano messe, inserite o estratte, dal nucleo di uranio. Ora però queste operazioni fatte nell'arco di decine di minuti, anche... non so esattamente i tempi ma non millisecondi, microsecondi. Quindi anche un errore potrebbe farcela per solo fare il calcolo necessario però deve essere garantito, perché se o non arrivo in tempo perché si blocca il sistema oppure non hanno previsto che poterà arrivare l'acqua del maremoto come Fukushima gli effetti sono catastrofici, ma non sono le centrali nucleari gli unici ambienti. Se avete visto, spero da lontano, gli apparati della terapia intensiva, sono apparati con a bordo degli elaboratori. Non è il caso che questi sfapino le tempestiche delle loro attività, che gli infusori diano troppo o troppo poco farmaco o si blocchi tutto aspetti che qualcuno dia Ctrl+Alt+Delete, perché alla macchina si può fare ma alla persona collegata NOI Non solo ma se pensate agli zeri, ai grandi zeri di linee, spero che non

pensiate che la cloche del pilota sia collegata con dei carri agli alettoni. La cloche non è altro che un sofisticato joystick attaccato a dei sensori che danno input a un sistema di elaborazione, ed è il sistema di elaborazione che poi pilota tutte le superfici di volo. Tutti questi sono esempi di sistemi hard real-time.

I Sistemi Operativi per i sistemi hard real-time sono completamente diversi da quelli visti fin ora.

Anche i processi dei sistemi hard real-time non sono neanche scritti in C, sono scritti in linguaggi fatti apposta dove per esempio ogni loop ha un numero massimo di iterazioni consentite se no si chiama la routine di emergenza, perché non ci si può scherzare e tra l'altro non sono sistemi operativi in cui dici adesso lanci un processo. L'insieme dei processi che quel sistema deve elaborare viene stabilito a priori, viene calcolato lo Scheduler statico in modo che siamo sicuri che tutti facciano quello che devono fare, e lo si fa in condizioni non critiche, quando la centrale nucleare è ferma, quando il sistema di controllo della terapia intensiva non ha nessun malato collegato, quando l'aereo è a terra. A quel punto si carica tutto, si mette in funzione, magari si mette in funzione anche con sistemi replicati per full tolerance e si lancia tutto il sistema così com'è ok? Quelli che in realtà sono molto più diffusi sono i sistemi SOFT real-time. I Sistemi Operativi per Personal Computer

sono tipicamente SOFT real-time. Quindi se avete un processo che sta facendo rendering di un frame video, o ancora peggio di frame audio, che sono più fastidiosi gli audio del video, quelli con un sistema di priorità si fa in modo che raramente possono sbagliare la loro tempistica. Però capite bene che è una gamma di problemi completamente diversi. Tipicamente i sistemi SOFT real time sono best-effort cioè se voi prendete un sistema fatto benissimo, studiato con cura e lo sovraaccaricate state tranquilli che il vostro filmato salta un po' e l'audio è singhiorzante.

Comunque mi preme dirvi che real-time non è l'esecuzione veloce.

Così abbiamo finito i lucidi che abbiamo iniziato ieri (00-intro.pdf (registrazione: 2022-02-25 pt1 minuto 45:40)) e cominciamo a ripassare l'architettura (01-arch-hw.pdf) in particolare guardiamo quelle parti di architettura che ci interessano per lo sviluppo dei sistemi operativi. Un segnale <https://nandgame.com> questo è un gioco a livelli che insegna l'architettura degli elaboratori, come dicono i miei figli...? "Io ho incominciato il gioco e sono stato sopra tutto il pomeriggio perché non riuscivo più a sciararmi". Qual è la parola giusta? ... intrappa... Sei arrivata a costruire completamente l'albero logico a un elaboratore capace di

eseguire programmi. Ritenni se vi piace quando lo avete provato (non fatevi adesso se no non stareste attenti alla lezione).

bot: nand to tetris

prof: non ho capito la battuta.

Questa (pag 2) è la nostra benemerita macchina di Von Neumann.

Forse si può dire "virale" del gioco... (registrazioni: 48:20)

C'è la CPU che ha all'interno l'unità di controllo e l'unità aritmetico logica. C'è un bus, attaccato al bus ci sono non i dispositivi ma i controller dei dispositivi e c'è la MMU (Memory Management Unit  $\Rightarrow$  unità di gestione della memoria) che collega alla memoria Principale.

Sai conosco il libro nand to tetris, se volete nand to tetris è molto più professionale e usa linguaggio di descrizione di hardware. Voi avete usato nand to tetris al corso (di architettura)? Il gioco mi consente di portare conoscenze meno formalizzate di quelle di nand to tetris anche a studenti della scuola secondaria ( $\Rightarrow$  1° grado medie, 2° grado licenza...). Ok.

(pag 3) Avete visto l'anno scorso architettura dei processori, concetti base relativi alla memoria e linguaggio assembly? Avete visto un linguaggio assembly?

Studente: quello di nand to tetris.

Consiglio, comunque bene o male, come effetto collaterale, quest'anno vedrete l'assembler di mips. Quando vedete in esecuzione il programma vedete la transcodifica

delle istruzioni mips. Tra l'altro il pezzo che fa il reverse-assembly delle istruzioni mips è proprio un pezzo della macchina Mmips che ho fatto con le mie manine... :D. ok.

(pag 4) INTERRUPT! Questo è un concetto chiave fondamentale e ancora oggi vedo che spesso anche all'esame viene sbraitato.

L'**INTERRUPT** è un meccanismo che permette l'interruzione del normale ciclo di esecuzione della CPU.

La CPU (Central Processing Unit) e qui mi appello alle conoscenze dell'anno scorso, miracolosamente se qualcosa non è chiaro fermatemi e rivediamo tutto quello che c'è da rivedere. Le CPU vivono la loro vita

caricando l'istruzione corrente, e come fanno a caricare l'istruzione corrente? Hanno un registro che si chiama

Program Counter o Instruction Register, sono sinonimi.

Lo buttano sul bus accendendo il bit del leggi. La memoria risponde mettendo sul bus dati l'istruzione.

L'istruzione viene caricata nel registro di decodifica.

A quel punto, passo successivo, il processore analizza l'istruzione caricata e (lo vedete benissimo anche su nand to tetris, o con l'architettura dei libri di Tanenbaum) e quello che fa è configura i vari componenti per fare/ eseguire l'istruzione voluta. Se pensate all'architettura di un processore, i vari bus interni al processore mi piace vederli come i binari dei modelli ferrovieri. "Dove vanno i dati?", "Dove vanno presi i dati?"

dipendono da come sono stati settati gli scambi.  
Praticamente la decodifica dell' istruzione altro non è che fare in modo che dalla stringa dell' istruzione vengano settati gli scambi dei bus della CPU perché al passo successivo possa essere eseguita l' istruzione, nel caso alla fine l' istruzione fa lo store dei risultati, e così via.  
Quindi come il motore a 4 tempi: aspirazione, compressione, scoppio e scarico questa (CPU) fa:

carica l' istruzione, decodifica l' istruzione, esegue l' istruzione e poi torna da capo. Quando arriva in fondo e vuole tornare da capo fa un passaggio in più. Dice:

"È avvenuto un INTERRUPT?", o meglio l' interrupt alla fine arriva al processore come un filo o più fili. Uno di questi bit è a 1 o sono tutti a 0? Se vede che c' è un interrupt il processore è organizzato per prendere l' indirizzo particolare, che è stato messo apposta per questa funzionalità, e metterlo nel program counter. Quindi in realtà il processore al ciclo successivo avrà fatto un salto a sua insaputa. Il programma non ha detto in quel momento di fare il salto, ma siccome è avvenuto un interrupt viene cambiato il program counter, ovviamente il valore precedente del program counter lo deve salvare da parte se no non riesce a tornare indietro.  
Se gli INTERRUPT sono MASCERATI questa operazione non viene fatta. E quindi anche se ci sono

questi fili accesi per dire "guarda che c'è un interrupt" il processore continua con l'istruzione successiva, e così via. Perché vengono introdotti gli interrupt?

L'interrupt fondamentale, l'interrupt per il quale è stato creato il concetto di interrupt è l'interrupt di Input / Output (I/O).

Ricordate che gli interrupt o sono quelli veri INTERRUPT HARDWARE sono comunicazioni che vanno dai controller dei dispositivi al processore, ok? Quindi il caso più tipico, l'abbiamo visto anche con la funzione scenica, la teatralizzazione di inizio corso, l'interrupt di I/O più importante è quello che viene mandato dai controller per dire "ho finito l'operazione" di I/O.

Facendo così il Sistema Operativo può attivare tante operazioni di I/O nei vari controller e poi mettersi a fare altre cose perché quando uno dei dispositivi avrà finito l'operazione manderà l'interrupt. Poco disinteressarsi del fatto che ci siano operazioni di I/O in corso perché verrà PRONTAMENTE AVVERTITO, prontamente è importante, nel momento della fine dell'operazione di I/O. Ma domanda tipica

è "Senza interrupt si può fare multiprogrammazione?"

Sì, ma la farà inefficiente. Perché l'unico modo che c'è per vedere se l'unità di I/O ha finito è chiederglielo.

Via bus il processore può sempre dire "Hei! Unità di I/O hai finito? Cosa stai facendo?". Ma facendo così si dovranno utilizzare solo tecniche di POLLING: "Hai finito?" "Hai finito?" "Hai finito?"... In un sistema monotask, quando mettete micro-sleep nell'

arduino per fare il bit di accendi / spegni, quello perde tempo, quello sta lì a ciclare a dire "Hai finito?" "Ho finito?" ... non ha altro da fare! Ma se io usassi dei meccanismi del genere (*polling*) su processori da Personal Computer ovviamente perderei un sacco di prestazioni. O perdo prestazioni, chiedendo troppo spesso "Hai finito?", o perdo prontezza cioè mi accorgo dopo del tempo che l'unità di I/O ha finito, alla fine perdo prestazioni lo stesso. Ecco gli INTERRUPT possono essere sia hardware che software, se volete in molti autori, anche a me piace chiamare gli interrupt hardware INTERRUPT, gli interrupt software TRAP. Gli interrupt software è il meccanismo per l'idea di usare lo stesso meccanismo degli interrupt per poter codificare degli eventi causati dal processo in esecuzione. Quindi occorreva una maniera per poter fare in modo, ve l'ha detto anche ieri, che il processo in esecuzione vive in ambiente confinato e controllato. ... far in modo che se il processo in esecuzione tentava di fare una corbelleria DAVOLERIA... :D: divisione per zero, accesso in memoria dove non può, uso di istruzione illegale... inventarsi tutto quello che può fare un processo di male... Non scoppiasse tutto, ma attirasse l'attenzione del Kernel (del S.O.). Allora l'idea è stata "noi abbiamo già un meccanismo che serve per attirare l'attenzione del

Sistema Operativo quando avviene gli interrupt del controller, gli interval hardware. Utilizziamo lo stesso strumento per gestire quando succedono degli errori, delle situazioni anomali causate dal processo in esecuzione. OK? Quindi gli interval hardware sono generati dai controller e normalmente sono attività asincrone che non sono relative al processo in esecuzione in questo momento. Gli interval software invece utilizzano lo stesso meccanismo degli interrupt per errori del processo in esecuzione.

(pag 5)

bot: quindi quando un programma interrompe la sua esecuzione per core dumped ad esempio l'esecuzione viene terminata da una trap?

Sì, se c'è segmentation fault... tra l'altro... allora... ponete di fare un bel programma che prende un indirizzo 0, assegna un puntatore a 0 e tenta di stampare ciò che c'è a quel puntatore.

Tra l'altro ho notato, non me lo ricordo, ma ho visto che pmpcs usa il valore di NULL a -1, secondo me sarebbe bene cambiarlo e lo riportiamo a 0 perché è quello standard voluto dal C. Secondo me se cambiate la costante e ricompilate tutto dovrà funzionare tutto ugualmente, senza che succeda niente. Lo cambiamo tra fase 1 e fase 2 così vediamo che tutto funzioni. Dicono segmentation Fault lo

causa il processo in esecuzione quindi "io sono il processo in esecuzione. Sono in user-mode, posso fare tutto quello che mi consente le istruzioni aritmetico logiche e l'accesso alla mia memoria. Faccio questa istruzione in cui tento di accedere alla memoria con indirizzo sbagliato. Il ciclo di CPU carica decode esegue, l'esegui crea la trap. Al passo successivo viene generata la trap e come se fosse un interrupt si passa all'esecuzione di un indirizzo del Kernel, che quindi incomincia a... Il Kernel si risveglia, praticamente, normalmente è dormiente e viene svegliato quando avviene un interrupt per una trap. Il Kernel parte, guarda quello che è successo, dice ah guarda "il processo X ha tentato di accedere ..." e lo vede guardando i registri della CPU. A quel punto dice "cosa devo fare adesso?". Ed è il Kernel che mette in piedi, parliamo di UNIX, quell meccanismo di mandare al processo il SEGNALE. Quindi il Kernel dice ah, siccome io sono UNIX e c'è scritto nelle regole che per mandare "se un processo fa un errore di indirizzamento nella memoria devo dare segmentation fault" il Kernel chiama quella funzione per mandare un SEGNALE quella chiamata dalla systemcall Kill di un altro processo. D'esecuzione non viene terminata dal trap, il passaggio è più lungo, il trap causa la generazione del segnale.

Non è detto che una segmentation Fault termini il processo.  
Voi potete mettere nel processo un gestore di segmentation Fault che comandi le cose e vi faccia continuare l'esecuzione.  
Perché può essere catturato il segmentation Fault. Il fatto che poi il segmentation Fault non venga catturato, si comporta come qualsiasi altro segnale non gestito che prevede la terminazione. Prego!

Studente: Non mi è chiaro come viene generata la trap?

Perché ... quando ... in caso di accesso in memoria la CPU esegue soltanto un'istruzione, ci vorrebbe un lato software che capisce che quell'indirizzo è sbagliato.

Sì, sì è la MMU che comunica ... È ancora un po' più complesso di così, ci abbiamo un capitolo di gestione della memoria fatto apposta per questo... provo a dire...

Quando si scrive sul bus un indirizzo e alla MMU è stato indicato quale Tabella delle pagine... quale risoluzione usare in questo momento. La MMU guarda in una cache, che si chiama Translation Lookaside Buffer (TLB), non so se l'avete visto ad architettura, c'è una piccola cache che tiene le ultime risoluzioni fatte, in realtà a livello di pagina/frame non a livello di istruzione, comunque se lì non c'è la MMU manda una trap al processore in ogni caso. Possono darsi due casi. Può semplicemente esserci che, siccome la MMU non può tenere tutta la mappa della memoria in memoria

sarebbe troppo pesante per la MMU, semplicemente può succedere che quella risoluzione non sia al momento nello mappa, allora il Sistema Operativo è lui che ricarica la parte mancante e fa riportare e tutto va bene. Se alla prima trap della MMU, perché non trova nella cache che ha a bordo la risoluzione, arriva al Sistema Operativo e dice "meh! Questo è un indirizzo che non ho neanche nella tabella quella estesa che gestisco io" a quel punto il Kernel genera il segnale. Comunque parte da una segnalazione della MMU. Divisione per 0 o istruzione illegale vengono generati direttamente dal processore.

pausa (min 1:07:45).

Sistemi operativi anno 2021-2022 registrazione: 2° semestre

2022-02-25

pt 2

slide 01-arch-hw.pdf

(fine pausa, riprendiamo)

Allora, mi raccomando un controller è un pezzo di hardware, il driver è un pezzo di software. Oggi purtroppo nei sistemi moderni è difficile vedere dove sono i controller. Se prendete una scheda madre, più o meno moderna anche se è meglio se un po' vecchietta, si vedono perfettamente i bus e i connettori.

Nota: 2022-02-25 pt 2

LA REGISTRAZIONE È  
MOLTO SALTELLANTE...

MOLTI BUCHI: → molte righe vuote

⇒ Fatevi il .mkv)

perché scrivere tutto è impossibile!  
anche tornando indietro con l'audio!

quindi alle pagine successive scrivo sulle slide o in  
gruppi schermi ... potrete scrivere nel .txt  
... aggiungere pagine... lasciate queste note!  
aggiungendo pagine al pdf DOPO aver scritto le altre  
registrazioni ↗ si lo posso fare DOPO!

di cosa parla la lezione?

cerca su google PCI BUS ved: immagini

interrupt trap

T

→ gestione interrupt

→ "Interrupt Driven" operative Systems

→ Interrupt Multipli → disabilitazione interrupt  
→ interrupt immediati

01-arch-hw.pdf  
da pag 6 a pag 17

# Sistemi operativi anno 2021-2022 registrazione: 2° semestre

2022-03-03

slide 01-arch-hw.pdf

Cravatta di oggi: "Ponti Giapponesi di Monet" qual'è il messaggio? È sempre impressionista, ma il messaggio è più nel PONTE oggi. Bisogna costruire ponti. Muri, tombe o altre cose distruggono il vivere civile, i ponti uniscono. Non a caso i Popi venivano spesso chiamati "pontefici" → che creavano ponti. OK, torniamo a Sistemi Operativi. Avete dubbi o domande? Riassunto delle puntate precedenti:

Stiamo iniziando a guardare come costruire Sistemi Operativi, mentre prima abbiamo visto come usarli, cosa sono. E stiamo guardando di capire alcuni particolari relativi all'architettura all'hardware. Nello schema che abbiamo visto un paio di lucidi prima, abbiamo visto che il sistema operativo è quello stato che crea un'astrazione sull'hardware. Quindi se volete costruire un Sistema Operativo dovete sapere come funziona l'hardware, qual'è il linguaggio parlato dall'hardware. Abbiamo visto dall'inizio di questo paio di lucidi: "cosa sono gli interrupt?", "Perché gli interrupt sono così importanti?", e che diventano veramente il motore che fa funzionare i sistemi operativi. Andiamo poi a vedere quelle che sono le risorse che il sistema operativo deve gestire.

Era stata arrivata qua (slide 23 01-arch-hw.pdf) se ricorda bene. Una risorsa molto importante, fondamentale è la RAM (Random Access Memory) per come sono costruiti i sistemi

oggi. La RAM è la memoria veloce, direttamente accessibile al processore volatile. Non sempre i sistemi erano fatti così, il primo sistema che ho usato nella mia vita aveva una memoria ai nuclei di ferrite, e quindi quella che era la memoria di lavoro era non volatile, era permanente. Mentre invece nei sistemi comuni oggi si tende a usare la RAM da RAM assieme ai registri è l'unico spazio di memorizzazione acceduto direttamente dal processore. Per accedere a memoria secondaria e terziaria ed altre risorse, non lo si fa direttamente parlando con il bus, ma bisogna tramite il bus dare dei comandi a dei controller che accedono al device. La RAM nei sistemi moderni è chiamata RAM statica, viene costruita con praticamente dei condensatori che si caricano, deve essere rinfrescato il contenuto perché tende a scemare con il tempo, ma tutta questa attività è invisibile al Kernel perché viene fatta direttamente dai moduli della RAM stessa. Quindi per quanto riguarda l'uso della RAM si accede direttamente al bus mettendo l'indirizzo a cui si vuole leggere e scrivere e si da il comando LOAD / STORE. Nei sistemi moderni, però, l'indirizzamento della RAM non viene attuato in maniera diretta ma tramite un'unità fisica, un componente fisico chiamato Memory Management Unit (MMU). Mi raccomando per le abbreviazioni e i concetti similari: Esiste una cosa chiamata Memory Mapper, che è una componente del sistema operativo e del software. Esiste una cosa chiamata Memory Management Unit che è una componente hardware ed è il componente che interfaccia la memoria.

Se volete il Memory Manager è il componente del sistema operativo che pilota, programma, configura la MMU. ok.  
Esistono ancora nei sistemi delle ROM (Read Only Memory), pensate a epram o cmos ram, alimentate, cioè memorie normalmente utilizzate in sola lettura. Tipicamente queste memorie vengono utilizzate per funzionalità molto basiliari, per esempio per fare il boot della macchina. Lo avete un po' visto anche quando avete visto un po' di architettura di pmp (microvmps). (pop 24)

Esistono alcuni dispositivi che sono MEMORY MAPPED, che si riescono ad accedere come se fossero memoria, ad esempio il video grafico dei Personal Computer. Ad alcuni indirizzi di bus corrispondono delle aree che non sono vere aree di memoria, ma dove il sistema può scrivere dei dati e questi dati vengono letti in tempo reale. È una memoria a doppio accesso: il bus scrive da un lato e dall'altro vengono letti da un componente, la scheda grafica, che prende questi valori scritti come valori normalmente come luminosità RGB (Red Green Blue, i tre colori) per accendere i vari pixel sullo schermo. Lo schermo grafico viene acceduto in questo modo, la gestione è semplice e lineare perché in questa modalità uno sa calcolare l'indirizzo di quel pixel, scrivere un valore e il valore diventa una luminosità di un pixel. Ma dall'altra parte necessita di sincronizzazioni di accesso. Essendoci due componenti che contemporaneamente accedono a questa memoria a doppio accesso, quello

che succede è che ci vogliono meccanismi di sincronizzazione  
talvolta fatti in maniera hardware, perché ad esempio  
il video non faccia FLICKERING (Visionario Oxford...  
Sostanzialmente, lo sfarfallio dell'immagine sullo schermo  
di un televisore o di un computer.). Quindi spesso c'è  
una doppia memoria, viene scritto il nuovo frame poi  
si dà l'impulso per fare in modo che il nuovo  
frame diventi quello visibile dall'utente. (pag 25)

DISCHI! Nonostante l'avvento, nonostante la presenza di  
dischi allo stato Solido (Solid State Drive  $\Rightarrow$  SSD) si usano  
tantissimo ancora i dischi rotazionali; i dischi convenzionali,  
quelli che abbiamo visto alla prima lezione di questo  
semestre direttamente aperti. I dischi sono dispositivi che memorizzano  
l'informazione in forma magnetica e quindi mantengono l'informazione  
in maniera non volatile, significa che anche se togliete l'alimentazione  
potete ritrovare i dati scritti. L'accesso è diretto (random i.e. non  
sequenziale). Per capire questa affermazione bisogna vedere che  
esistono anche dei dispositivi magnetici ad accesso sequenziale,  
che erano i nastri, i tape (erano ad accesso sequenziale).

L'indirizzamento su disco è dato in termini di 3 parametri:  
**cilindro, settore e testina**. Per cambiare cilindro, pensa lo  
abbiate visto anche ad architettura, quindi non sta a lungo in testa,  
c'è il pettine delle testine e quindi se voi non muovete il  
pettine delle testine il disco gira e quindi tutto ciò che è  
memorizzato con quella posizione delle testine è accedibile, vuoi  
aspettando che durante una rotazione transiti il settore sotto la

testina, vuoi decidendo di usare una delle testine fra quelle disponibili. Se invece uno vuole spostare il pettine delle testine, quindi cambiare cilindro si chiama cilindro perché ovviamente se tenete le testine ferme il disco gira tutti i dati saranno a una certa distanza dal punto di rotazione, quindi se lo pensate geometricamente è un cilindro. Per cambiare cilindro ci vuole un tempo meccanico di spostamento della testina. Per cambiare settore ci vuole un tempo meccanico per aspettare che quel dato che vogliamo leggere o scrivere passi sotto la testina. Per cambiare testina non ci vuole tempo meccanico basta tempo elettronico. Per intenderci per cambiare cilindro occorrono dei tempi dell'ordine di millisecondi e dipende anche da quanti cilindri dovrete saltare, per cambiare settore il tempo si può anche calcolare, perché quando comprate un disco il disco fa i parametri di lavoro a il numero di giri al secondo. Se avete un disco a basso costo oppure un disco che fa 5400 giri al minuto RPM (revolutions per minute) e se prendete un disco molto costoso ne fa 15000, non è che possiate avere un disco che fa 200000 giri al minuto, decollerelde il computer :D no, non ce la si fa fisicamente a costruirlo. Quindi se pensate 5400 giri... facciamo 600 per fare i conti pari se poi fosse 6000 giri al minuto al secondo sono 100, quindi vuol dire 10 millisecondi, quindi anche quello non è un tempo banale. ok?

Dal punto di vista del sistema operativo questo cosa significa? Perché non è indolare avere questa gestione. Significa che le operazioni di SEEK devono essere limitate e bisogna fare in modo

(pag 26)

che siano l'orari. Quindi quello che succede è che, visto che i vari processi chiederanno in concorrenza di voler leggere e scrivere dati su disco occorrerà avere anche in questo caso dei meccanismi di scheduling di ordinamento delle richieste che ottimizzino il percorso della testina su disco. OK? E' altra cosa, che incide più sull'implementazione del file-system rispetto alla gestione fisica del disco è quello di fare in modo che dati che vengono acceduti spesso, in sequenza e vicini nel tempo siano vicini anche su disco. Se voi utilizzerete dei file-system, e lo vedremo, poco efficienti, costruiti male, per esempio FAT (File Allocation Table), a forza di usarlo quel file system spargerà i "pezzi dei file" in posti casuali del disco. OK? È quindi farà in modo che il sistema man mano perda sempre di più di prestazioni. OK? Infatti sono quei file system per i quali è prevista deframmentazione. Non so se avete mai fatto defrag. ma potrete scegliere altri file system che non avevano questo tipo di problema. Mi vengono in mente 2 cose che vi faccio vedere per compiere il ritmo.

su google cerca "cybernare pezzo nel cyberspazio"  
clicca su "Trappola nel Cyberspazio - Roberto di Cosmo"  
link: <https://www.dicosmo.org/Piege/cyberespace/trappola.html>  
Roberto di Cosmo, nonostante il nome è italianoissimo, ma vive e lavora in Francia, insegnava direi a Paris Diderot, (leggi il capitolo intitolato "armadi a cassetti e la galleria dei censelli") e racconta: "Ebbene durante uno dei miei viaggi mi sono ritrovato a fianco di un gentilissimo signore, giovane e dinamico

funzionario d'impresa, che si apprestava ad eseguire sulla sua macchina il famigerato programma DeFrug. Questo programma mostra una bella matrice riempita di piccoli quadrati di tanti colori che si muovono in tutte le direzioni mentre il disco lavora intensamente e rumorosamente.

Non ho potuto resistere alla tentazione (...): dopo essermi complimentato per il mio bel portatile, gli ho chiesto, fingendo la più grande ignoranza, [di un famosissimo professore di informatica] cosa fosse quel bellissimo programma che io non avevo sul mio portatile. Con un'aria di superiorità mista a compassione (...) mi ha risposto che si trattava di uno strumento essenziale che bisogna lanciare di tanto in tanto per "fare andare la macchina più veloce". Ha proseguito ripetendomi a memoria gli argomenti che si trovano nei manuali Windows: più si utilizza il disco, più questo si "frammenta", e più il disco è frammentato più la macchina è lenta.

A questo punto ho tirato fuori il mio computer portatile, che non utilizza Windows, ma GNU/Linux (...) e gli ho detto con un'aria un po' stupita, che tutto quello che mi aveva detto mi sorprendeva enormemente: sul mio portatile il disco è molto poco frammentato e più si utilizza meno si frammenta.

[...] Questo disco è come un gigantesco armadio a cassetti: ogni cassetto ha la stessa capienza e ciascun disco contiene alcuni milioni di cassetti [meno di quelli di oggi]. Se i dati che vi interessano sono sistemati in cassetti contigui, vi si può accedere più velocemente [...] .

Immaginiamo un ministero che conserva i suoi dossier in un enorme armadio con milioni di cassetti [ ... ].

Se avete un segretario [ lo metto al maschile perché lo trovo più coerente ... ] con due candidati dalle abitudini molto diverse uno che quando trova un dossier si limita a ruotare i cassetti e quando trova uno nuovo lo separa in piccoli fascicoli e li mette a caso nel primo cassetto vuoto che trova. Un altro che conserva sulla sua scrivania una lista di cassetti vuoti contigui e aggiorna la lista tutte le volte che la pratica viene chiusa. Questo lo trovo una maniera molto simpatica di raccontare la frammentazione.

L'altra cosa che mi volevo far vedere (vediamo se lo trovo) (cerca su google "Lost We Remember: Cold Boot Attacks on Encryption Keys" link: [https://www.usenix.org/legacy/event/sec08/tech/full\\_papers/haldeman.pdf](https://www.usenix.org/legacy/event/sec08/tech/full_papers/haldeman.pdf) oppure <https://cipsite.s3.amazonaws.com/xp-content/uploads/2019/01/23195456/haldeman.pdf>)

"Voi pensate che la RAM sia volatile, in realtà qui hanno fatto vedere un attacco su chiavi crittografiche fatte sulla RAM in che modo? Prendendo la RAM in funzione e facendo queste azioni velocissime, e poi neanche troppo veloci, tempo qualche secondo:

- Spegnete brutalmente la macchina senza che il sistema possa fare shutdown.
- Togliete la RAM e consigliatela

è ancora possibile leggere quello che c'è scritto sulla RAM.

Interessante... ecco (pag 6, Figura 4 dell' articolo)

Quello è l'immagine nella RAM e vedete il contenuto dopo  
• 5 secondi • 30 secondi • 60 secondi e • 5 minuti.

Quindi congelato, entro 5 secondi avete ancora tantissime informazioni  
utili per vedere (ovviamente era un'immagine ma l'hanno fatto  
vedere su chiavi critografiche)..., in fondo chiavi critografiche quando  
voi scrivete la password, è vero che nel sistema viene salvata in  
maniera critografata e così via, ma per fare l'input della  
password quella password per un po' passa in RAM, in chiaro."  
Comunque per vostra informazione non penso vi sia utile per fare  
Sistemi Operativi a prova di congelamento della RAM.

Quando si dice che la RAM è volatile è proprio perché  
è fatta con i condensatori, quindi i condensatori si scaricano  
pian piano, non c'è più il meccanismo di refresh perché non  
c'è più corrente, ma il contenuto può essere recuperato.

OK. (pag 27)

SSD. Ho aggiunto questo lucido perché anche SSD ha degli effetti  
collaterali sui sistemi operativi. Per copiare cosa dobbiamo fare con i sistemi  
operativi dobbiamo capire quali sono le caratteristiche alle quali dobbiamo stare attenti:  
di queste apparecchiature. Il numero di cicli di scrittura è limitato,  
alto ma limitato, quindi occorre per quanto possibile spargere  
uniformemente sulla gamma di indirizzi, cioè nello spazio  
memorizzabile le operazioni. Quindi è bene riciclare lo spazio  
riutilizzato in maniera da... Non importa come nei dischi  
cercarlo vicino, ma occorre fare in modo di riciclare e  
riutilizzare ora ciò che abbiamo utilizzato in tempo più remoto,

in maniera tale da sporgere l'accesso su tutti gli indirizzi.

Si leggono a blocchi. Si scrivono a blocchi (numerosi blocchi)

Il meccanismo di scrittura dell'SSD prevede che la scrittura non venga fatta per un blocco solo ma per un gruppo di blocchi. OK? Queste cose sono normalmente abbastanza mascherate dai controller, ma meglio si sanno queste cose, per esempio è bene fare in modo che cose che vengono aggiornate contestualmente siano a indirizzi limitrofi. Per il numero di cicli di scrittura limitato vedremo che ci sono degli effetti collaterali anche non solo nella gestione fisica del dispositivo ma anche sul file system, per esempio un caso tipico d'uso è quello di evitare di fare aggiornamenti non necessari, grosse cache aiutano, ma tra l'altro nei sistemi UNIX, per esempio, è possibile, quando si monta un file system, dichiarare se si vuole avere la data di ultimo accesso al file o no.

In realtà la data di ultimo accesso ad un file, accesso non modifica, se togliete la data di modifica saltano un sacco di cose per esempio make non funziona più. Mentre invece la data di ultima lettura è rocambole utile, quindi di solito se avete dei dischi SSD si fa in modo che non venga aggiornata, c'è il parametro di mount che si chiama `noatime` `no access time`, che fa in modo che non ci sia questa informazione aggiornata. Pensate "Quanti file leggete?" "Quanti file scrivete?" "Quante volte leggete un file?", pensate `/etc/passwd` tutte le volte che c'è un autenticazione da qualche parte o si vuole vedere qual'è il nome corrispondente a un utente c'è un accesso a quel file.

Quanto più velocemente degrada un disco allo stato solido (SSD) se chiedete questo aggiornamento? Perché ovviamente i dati di controllo continuano a essere aggiornati ad ogni accesso, e quasi si tenta di fare cache degli inode usati però... (pag 28)

Quindi possiamo pensare di avere una gerarchia di memoria, abbiamo tante memorie, abbiamo registri, RAM, dischi e anche unità offline.

Andrew Tanenbaum ha detto

"Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway"

e il prof lo ha tradotto con:

"Non sottovalutate mai il bandwidth  
di un vagone ferroviario carico di nastri"

google traduttore lo ha tradotto con:

"Non sottovalutare mai la larghezza di banda di  
una station wagon piena di nastri che sfreccia  
lungo l'autostrada".

In realtà il bandwidth può essere notevolissimo, è difficile accederlo... E cosa c'entra con questo? Di solito le memorie vengono chiamate memoria primaria, secondaria, terziaria. E prima ancora della memoria primaria ci sono i registri. La memoria primaria è quella direttamente accessibile dal processore, quindi normalmente la RAM. La memoria secondaria è la memoria accessibile tramite un controller dal processore quindi i dischi rigidi e i SSD. La memoria terziaria è memoria offline che può essere collegata in necessità, la memoria terziaria normalmente ha bisogno di un intervento umano o

simili per farlo.

bot: che cosa intende per cicli di scrittura?

Per la SSD, quando dovete aggiornare il dato che avete memorizzato sulla SSD dovete dare un comando di scrittura e quindi quello è un ciclo di scrittura, il ciclo di scrittura fisico.

Come dicevo prima normalmente per farne il meno possibile si tengono dei buffer, quindi se un dato un piccolo file viene acceduto, modificato più volte in realtà non ci fa alcuna scrittura fisica, se non in fondo se il file non viene anche cancellato. OK? Quindi l'idea è quante scritture fate, lo chiamo ciclo di scrittura e non scrittura perché è diversa la scrittura che appare a voi quando scrivete un programma fate una write e la scrittura fisica che viene fatta poi veramente sulla SSD. Come le chiavette USB, che infatti sono fatte più o meno della stessa pasta, se mai provate a usarla pesantemente in lettura e scrittura e la staccate senza fare l'operazione di chiusura di umount su quella chiavetta ci può essere di tutto, perché tenderà a fare meno scritture possibili fisiche e molte cose quando l'andate a scollegare pensavate di averle fatte ma erano ancora nel buffer.

Allora abbiamo una gerarchia di memoria (pag. 29, figura)

Partendo dai registri guardiamo una riga sì e una riga no.

registri, memoria principale che è la RAM; memoria secondaria Dischi SSD; memoria terziaria. Poi c'è una linea di demarcazione tra la memoria volatile e quella non volatile, ma oltre gli elementi dispari nel mezzo ci sono gli elementi per cui sono le CACHES. L'ultima parte l'ho un po' inventata per

domandarmi che cos'è oggi l'equivalente delle memorie terziarie.  
In fondo oggi come memorie terziarie quello che si usa più normalmente sono memorie allo stato solido removibili, mentre una volta c'erano nastri, CD rom, DVD rom che hanno perduto sempre più utilizzo perché risultano più costosi, più scomodi di unità allo stato solido. Parliamo del concetto di cache importantissima.

Che cos'è uno CACHE?

Una cache è una porzione di memoria più veloce che viene usata per mantenere temporaneamente i dati più utili di una memoria più lenta. Facendo così statisticamente potrò capitare frequentemente di poter ritrovare il dato senza andare ad accedere alla memoria più lenta, ma trovandolo già disponibile nella memoria più veloce. OK? Questo è un concetto astratto che potete applicare a tutti i livelli quindi per esempio nelle CPU nei processori ci sono delle cache del contenuto della memoria, se guardate quando acquistate un processore o acquistate una macchina con dentro un processore, nelle caratteristiche tecniche del processore c'è scritto quanta cache c'è. OK? Questa cache che vedete là su (in figura n. 23) tra i registri e la memoria centrale è costruita con le tecnologie dei registri quindi molto veloce e questa cache è gestita direttamente dal processore quindi normalmente è trasparente ai sistemi operativi. Quindi il sistema operativo / il programma applicativo non si accorge della cache se non dal punto di vista prestazionale, quando si accede alla memoria centrale automaticamente la cache fa il suo mestiere e tenta di mantenere i dati più recentemente usati. Tutti questi meccanismi si basano su un principio di... viene spesso detto in informatica di località, se volette è l'equivalente informativo dell'inerzia. Ci si aspetta che dati limitrofi

in memoria, logicamente limitrofi in memoria e dati recentemente utilizzati vengano utilizzati nel prossimo futuro, che non è una regola generale. È possibile costruire dei programmi per fare in modo che la cache lavori peggio possibile, però statisticamente le cose vanno bene. Non è totalmente indolare fare una cache, non è così banale, infatti è stato un trappismo ingegneristico non banale, perché per esempio se avete un sistema multiprocessore, ognuno con la sua cache, occorrono dei meccanismi, che i processori implementano, per invalidare la cache degli altri processori se uno modifica un dato nella cache, perché se no risulta disallineato... Una delle garanzie che deve dare una cache è che sia trasparente, che non si veda, che nessun programma abbia risultati diversi se eseguito in un sistema con la cache o senza.

E quindi siccome la semantica di accesso, l'astrazione nell'accesso alla memoria centrale è una semantica immediata, cioè mi aspetto che se un programma scrive a quella locazione un dato dal momento in cui è stato fatto l'operazione tutti gli altri possono leggere lo stesso dato, occorre che la cache garantisca questa cosa, e per farlo deve invalidare i contenuti delle cache degli altri processori.

Come c'è una cache tra la memoria centrale e i registri, si può fare una cache dei contenuti dei dischi nella RAM. Ancora una volta pensiamo la RAM ha velocità un milione di volte superiore a quella del disco. Se andate a comprare della RAM, le caratteristiche tecniche dicono tempi di accesso 8, 10, 10 è già scarsissima, 8 nanosecondi: ( $1 \text{ nanosecondo} = 1 \text{ ns} = 1 \cdot 10^{-9} \text{ s}$ ) NANO  $\Rightarrow$  miliardesimi, milli ( $10^{-3}$ ) micro ( $10^{-6}$ ), nano ( $10^{-9}$ ), pico ( $10^{-12}$ ), fento ( $10^{-15}$ ), atto ( $10^{-18}$ ). Prima allora visto i dischi millisecondi sono millesimi:

quindi: 2 miliardi diviso 1000 togliete 3 zeri 1 milione.

Ordini di grandezza, ma pensate che così il rapporto di un milione. Pensate che cosa succede in 1 secondo e che cosa succede in un milione di secondi OK?

Allora se si riescono a tenere i dati più utili nel prossimo futuro, si riescono a tenere in RAM e non su disco, il sistema avrà un aumento di prestazioni spaventoso. OK?

Ecco questa cache, in realtà, nonostante il concetto sia lo stesso, questa deve venire implementata dal sistema operativo, non è una cache hardware, è una cache software. ovviamente si può pensare di fare la stessa cosa ad alto livello, per esempio se una delle unità in cloud, che vanno benissimo però hanno una latenza notevole, perché quando andate ad accedere alla rete, non so che latenza abbiate voi nelle vostre connessioni di rete, ma se vi va bene sono almeno 10-15 millisecondi di "RAM trick?" giusto per mandare il dato lì e tornare. Quindi può essere conveniente creare delle cache locali in RAM o anche su dischi locali del materiale che c'è in giro.

Addirittura vedremo ci sono dei file system sperimentali, tipo Andrew File System, che sono file system i cui dati sono sparsi per il pianeta, potete avere server che vi formano un unico file system sparsi, e lì addirittura c'è la cache dell'intero file, e lì hanno dovuto cambiare la semantica d'accesso perché se no era inusabile.

Comunque l'importante è che vi sia chiaro il concetto di CACHE.

(pag 30) Ok, questo più o meno l'ho detto.

(pag 31) Problemi da considerare. Tutte le volte che abbiamo una cache c'è l'algoritmo di replacement.

Dato la caratteristica della memoria, quella più veloce e più accessibile è in quantità minore ed è più costosa e man mano si va a scemare. Quella disponibile a tempi più elevati è normalmente più lenta, enormemente meno costosa e disponibile in quantità molto più ampia. Quindi, concetto chiaro, la cache ha una dimensione standard più piccola dell'unità che andiamo a ottimizzare. All'inizio è facile, tutto ciò a cui accediamo lo mettiamo anche nella cache, ma poi a un certo punto la cache si riempirà e occorrerà capire "chi butta giù dalla torre?" quale dato presumibilmente non sarà utile nell'immediato futuro e quindi si potrà pensare di scaricarlo dalla cache, e questi sono i così detti ALGORITMI di REPLACEMENT, (di rimpiazzo, per cambiare). OK? E a questo punto vedremo meccanismi per varie funzionalità del Sistema Operativo. Occorre creare un CURISTICO che abbia senso, non c'è "la" soluzione. Allora per esempio uno può pensare di cercare la pagina accessuta meno recentemente (la pagina ... l'elemento di cache che è lì da più tempo e che non è stato accedito, quindi si presuppone che non sia utile) oppure si può pensare di guardare la FREQUENZA di accesso (quell'elemento della cache è stato accedito frequentemente quindi nel futuro si pensa che...)

vedete è un "processo" di NERZIA, si tenta di vedere qual'è il comportamento nel prossimo futuro analizzando il comportamento nel passato prossimo, alliamo parlarne delle previsioni del tempo, il concetto è lo stesso. Quindi l'algoritmo di replacement decide qual'è l'elemento da eliminare nella cache quando bisogna aggiungerne un altro, ovviamente l'elemento

che deve essere eliminato deve essere aggiornato nella memoria reale se sono avvenute delle operazioni di modifica.

Come si sceglie l'algoritmo di replacement?

C'è un trade-off fra quello più statisticamente performante e le strutture dati che bisogna mantenere per poter fare funzionare quell'dato. Che ne so, se uno vuole tenere traccia mano mano di quelli meno meno recentemente utilizzati deve tenere una struttura dati da aggiornare ad ogni accesso per fare una lista per vedere quale è il più utilizzato e quello meno, se uno deve tenere la frequenza deve tenere per ogni elemento un contatore che ad ogni accesso venga incrementato.

L'altro problema è la **coerenza**, siccome la cache è una copia, è una copia in una memoria più veloce, quindi quel dato che logicamente è lo stesso dato, è presente in più replicazioni in punti diversi della gerarchia di memoria.

Dove essere coerente. Come dicevo prima, deve fare in modo che la cache alla fine sia trasparente, esserci o non esserci il risultato non cambia se non il tempo per produrre il risultato.

(pag 32) Ancora l'hardware. I meccanismi di protezione.

I processi in esecuzione su un sistema operativo non devono interferire tra loro, devono poter comunicare e ... . Quindi una cosa sono i servizi forniti dal Sistema Operativo per operazioni ordinarie, decite, una cosa è se accidentalmente o volontariamente un processo può riuscire a perturbare/disturbare/rovinare.

l'esecuzione di un altro processo o addirittura del sistema operativo stesso. Come si fa ad evitare che ci siano queste interazioni non volute? Sicuramente non è possibile farlo totalmente via software, occorre una mano dell'hardware. Studente: Questo perché potrebbe fallire via software, quindi allora bisogna di un "ultima spiaggia"?

Occorre creare una barriera "cosa può fare il processo e cosa no?" se un processo potesse direttamente accedere all'unità di I/O potrebbe rovinare il lavoro degli altri, se un processo potesse accedere direttamente alla memoria degli altri potrebbe rovinarne il funzionamento. Esiste del codice che deve poter accedere alla memoria degli altri, il Kernel, quindi quello che dobbiamo chiedere al sistema è che si dia il modo di riconoscere gli umani dagli dei, di riconoscere i processi che possono fare poche cose, i processi che possono essere cattivi, possono essere ... sono quelli da controllare e che non devono produrre danni e i controlleri, cioè la parte di codice che è affidabile e controlla il resto delle cose. Quindi il punto chiave che la cosiddetta "modalità protetta", quando hanno inventato i Personal Computer, con il 6502, penso ad Apple 2, oppure con i 8086, 8088 Intel, penso ai PC IBM, questi erano processori che non avevano modalità protetta. Cos'è la modalità protetta? Il processore ha un bit (pag 33) (o simili, prendiamo 1 bit, poi vi spiego che in Intel c'è una cosa leggermente diversa) comunque ha 1 bit, se quel bit è modalità Kernel il codice che è in esclusione può fare tutto quello che vuole e

ha pieno accesso al sistema, se invece il bit è spento in modalità user, in modalità user il codice, il processore è configurato in maniera tale che ci sono solo le operazioni NON privilegiate in funzione. Quando un processo è in modalità Kernel può volontariamente fare tutto, tra le varie operazioni, può anche dire "adesso vado in modalità user". Un processo in modalità user può fare solo quello che gli è concesso e l'unica cosa che può succedere è che arrivi un interrupt o una trap e nella gestione dell'interrupt o della trap, non per volontà diretta del processo, o meglio non con codice sotto controllo del processo ... il processo può chiedere System call, però a quel punto il resto della gestione viene fatta dal Kernel. Vi dico, i primi PC avevano dei processori che non avevano queste funzionalità e quindi non era fisicamente possibile scrivere sistemi operativi affidabili, sicuri. A seconda dell'autore o del processore troverete la modalità Kernel indicata come modalità privilegiata, modalità supervisor, ring 0. Ecco gli Intel hanno questa idea, 4 livelli di priorità, ring 0, ring 1, ring 2, ring 3, di fatto ring 0 è la modalità Kernel e le altre sono modalità non privilegiate a scolare. Normalmente i Sistemi Operativi che ho visto su Intel usano 0 e 3 come ring. Per esempio le istruzioni per disabilitare gli interrupt è privilegiata. Un processo che è in esecuzione in modalità user non può disabilitare gli interrupt, se disabilitasse gli interrupt diventerebbe monopolista della CPU; non può cambiare le mappe di memoria della MMU. In realtà nei

sistemi moderni l'accesso alla memoria è non privilegiato perché è la configurazione della MMU che è privilegiata. Quindi il processo accede liberamente alla memoria, ma siccome gli indirizzi che genera sono indirizzi logici e la MMU glieli traduce, lui può generare tutti gli indirizzi che vuole, quelli che la MMU non li consente non li vedrà mai. ok? E per cambiare la mappa di configurazione della MMU ci vogliono operazioni privilegiate, quindi lui non le può fare, lo può fare solo il Kernel. (pag 34)

Alla partenza il processore è in modalità Kernel.

[... domanda studente e docente risposta... (min 52:50-53:45) ...].

Al bootstrap (quando si inizia) il sistema è in modalità Kernel. Quindi normalmente il sistema parte, fa l'inizializzazione, crea a mano lo stato del primo processo, chiama lo scheduler, lo scheduler di CPU è chiamato a dire "adesso qual'è il prossimo processo che va avanti", al boot non ha molte scelte c'è n'è solo uno, guardacaso sceglierà quello, e a quel punto cede il controllo al primo processo, e siccome lui può farlo cede il controllo e lo mette in modalità user. Il primo processo allora inizia ad eseguire, a fare il codice che deve fare, è in modalità user, non può fare altro che fare calcoli ed accedere alla memoria, e a quel punto delle due uno:

1. o accade un Interrupt 2. o accade una trap.

A quel punto quando accade l'interrupt o la trap, l'hardware passa da modalità utente a modalità Kernel ad eseguire il codice Kernel, e il gioco continua, viene gestito l'interrupt o la trap, si chiama lo scheduler,

si fa partire un processo o quello o un altro in modalità user e continua così il ciclo del sistema operativo. (pag 35)  
Questo è il meccanismo su cui si basano tutte le altre protezioni. Accedere direttamente ai device in modalità user è vietato, uno lo deve chiedere tramite una system call di fare l'operazione. Quindi il fatto che il Kernel funzioni in modalità privilegiata e controlli tutto, fa in modo che il Kernel possa, senza poter ricevere interferenze dal processo utente, decidere quello che si può e quello che non si può fare. Quando arriva una system call che dice "voglio accedere a quel file", dice "no, non è tuo e non hai il permesso", ma non c'è nulla sul disco, non c'è nulla hardware che faccia la protezione a livello del file-system, semplicemente è protetta la system call e la system call viene eseguita in modalità Kernel e il codice del Kernel va poi a vedere con tabelle sue, sue strutture dati quello che si può o non si può fare e risponde "picche" o risponde "ok" alla richiesta di operazioni. Questo è il nucleo centrale di protezione, mi raccomando modo Kernel e modo user sono modi del processore, non c'entra niente anche se c'è scritto supervisore, modo supervisore è una cosa del processore. Superuser ROOT sono cose del filesystem, sono utenti generati dal sistema, sono astrazioni che vi dà il sistema operativo. OK? Anche un processo di root è in modalità user, è un processo come gli altri, solo che la systemcall open va a vedere chi è l'utente (che

è un concetto implementato dal sistema operativo)  
"chi è l'utente che fa questa operazione?" dice "ah è root,  
allora a root è concesso". Se un processo che è in  
esecuzione come root vuole accedere a /dev/sda1  
(direttamente al disco) il processo è in modalità  
user in realtà non accede direttamente al disco. Il  
processo fa una system call open, la system call viene  
eseguita in modalità Kernel, dice "Può accedere in scrittura  
a /dev/sda1?" "sì" allora da l'OK alla open e va  
ad agire sul file. Ma il processo di root funziona  
in modalità user. (pag 36) ok, per l'ACCESSO alla  
MEMORIA la protezione, come si diceva, avviene attraverso  
la Memory Management Unit (MMU).

Perché c'è questo meccanismo? Se i processi potessero  
accedere alla memoria all'indirizzo che vogliono  
potrebbero modificare il codice, o gli altri degli processi,  
modificare i dati e il codice del sistema operativo,  
modificare l'interrupt vector e mettere il proprio  
gestore dell'interrupt. Comunque, come si diceva, la MMU  
fa la traduzione degli indirizzi logici in indirizzi fisici,  
è una funzione che ha il suo Dominio e il suo Codominio.  
Se voi applicate una funzione un dato potrà generare solo  
risoluzioni / valori nel Codominio. Se la memoria vietata non  
appartiene al Codominio potete dare tutti i dati che volete  
alla funzione e non succederà mai nulla. (pag 37) ok.

(pag 38) Le istruzioni di I/O sono privilegiate. Come fa un

processo utente a fare operazioni privilegiate? Chiama le **System call**, ovvero sono troppe generate da istruzioni specifiche. Nei vecchi sistemi Intel proprio il processo corrente generava un interrupt, direi 0x80, cioè aveva l'istruzione per fare un interrupt come quello dell'hardware. Nei moderni sistemi c'è una chiamata apposta, chiamata **SYSTEM CALL**, che risulta essere più efficiente. (pag 39, figura) Quindi: la systemcall si comporta come la gestione degli interrupt che abbiamo visto prima, software ma è un interrupt, quindi quando fa la syscall si salvano i registri, si gestisce, si fa l'operazione, si ripristinano i registri e si fa continuare il processo, oppure se è bloccante fra il ripristino servizi e il ritorno dell'interrupt viene scelto un altro processo se c'è di monda avanti.

Ecco mi fa venire in mente una cosa che vi dico prima della pausa, perché questo è l'ultimo lucido di questo parco. Probabilmente cambia appena non è lucido, ecco ho pensato che aggiornere questo lucido queste scrive qua a sinistra, invece che scrivere perché gli interrupt possono essere interrupt del hardware o del software. Qui mettendo queste parole fa confusione.

(pag 6)

Al posto delle parole hardware metterò processore, al posto delle parole software scrivete codice. Gli interrupt possono essere sia dei dispositivi sia per errori o systemcall. Per ciascuno di questi tipi c'è una parte di elaborazione fatta dal processore (in alto) e una parte che viene fatta dal codice. OK così non c'è sbruffamento. pausa (registrazioni misurate 1:03:45).

fine della pausa. (02-arch-os.pdf pag 1).