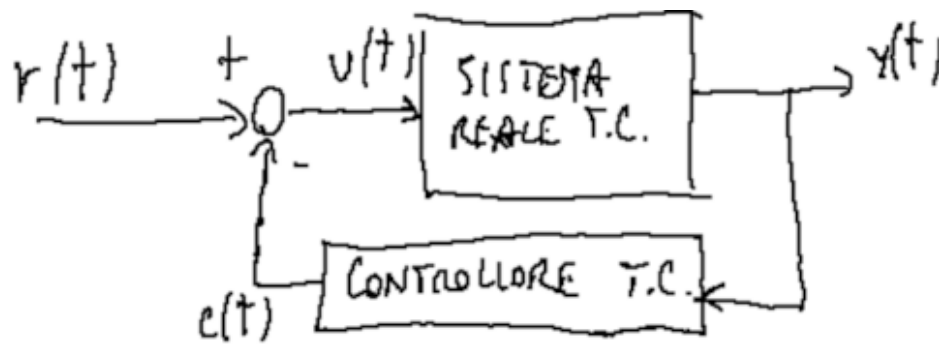


Cassandra Crossing 667- In morte del sistema operativo



$c(t)$ CORRENDO

$r(t)$ RIFERIMENTO

$$u(t) = r(t) - c(t)$$

CONTROLLORE: CERCA DI RENDERE $y(t) \approx y_{des}(t)$
USCITA
DESIDERATA

Sistema di controllo dinamico TC - Luca Ghio - [CC BY-SA 3.0](#)

(667) - Il mondo di chi utilizza tecnologie informatiche sta subendo una trasformazione tanto importante quanto impercettibile. Android 17 e Windows 11 cesseranno lentamente di eseguire le nostre istruzioni ed inizieranno, sempre lentamente, ad eseguire quelle di altri, il tutto nell'indifferenza generale.

22 maggio 2026 - Anche per una profetessa che ben conosce il suo mestiere è difficile puntare il dito contro qualcosa che non si percepisce, e che non ha nessuna intenzione di farsi percepire per quello che è. Non è una situazione come quella del cavallo di legno; i greci che vi erano nascosti noi troiani alla fine li abbiamo ben “percepiti”.

Ma quello che si sta compiendo in questi mesi a livello dei sistemi operativi più diffusi, Android e Windows, è destinato ad avere un impatto enorme sulla popolazione planetaria.

Ed ancora una volta, per capire, dobbiamo prima di tutto riavvolgere il nastro e partire dall'inizio di questa storia.

I Sistemi Operativi sono stati inventati poco dopo i computer. “Spiegare” ad un computer cosa fare programmandolo direttamente è cosa complessa e tediosa. Un sistema operativo permette di eseguire facilmente le operazioni di base come lanciare un programma, accedere ad un file, e tutte quelle operazioni che oggi diamo per “naturali” in qualsiasi computer.

Realizza questo definendo un semplice “linguaggio” fatto di comandi dal nome descrittivo per “colloquiare” col computer, senza bisogno di scrivere programmi, per fare le operazioni più elementari e, se mi consentite il termine, più “informatiche”.

Lo fa senza nascondere cosa si sta facendo, ma semplicemente semplificandolo, gestendo e diminuendo la complessità informatica di ogni singola operazione.

Questa è la sua caratteristica principale. Fare quello che l'utente chiede, e farlo solo quando gli viene richiesto, altrimenti non fare nulla.

Un esecutore passivo, insomma.

Attenzione, questo non vuol dire che il sistema operativo non possa fare azioni da solo. Tutti i sistemi operativi non primitivi hanno funzioni più o meno avanzate che permettono di eseguire operazioni ripetitive o periodiche, automatizzandole; quindi un sistema operativo può anche *“lavorare da solo”*. Non è questo il problema.

Il problema nasce quando cominciano ad avvenire due cose, solo apparentemente innocue.

- 1) il sistema operativo fa cose all'insaputa dell'utente.
- 2) il sistema operativo esegue i comandi per l'utente in maniera influenzata da fattori esterni, non percepiti dall'utente e non esplicitati.

Che un sistema operativo faccia cose da solo non appena installato non è di per se pericoloso. Richiedere ad un utente di conoscerlo completamente per poterlo installare ed utilizzare sarebbe irragionevole. Ma allo stesso tempo è indispensabile che qualsiasi utente interessato possa conoscere, a qualsiasi livello di conoscenza informatica si trovi, cosa fa il sistema operativo.

Che un sistema operativo esegua comandi in maniera “creativa”, senza che questo sia esattamente percepibile dall'utente, nega invece la sua stessa funzione primaria. Trasforma il sistema operativo in uno strumento attivo, che può essere anche utilizzato per rovesciare i ruoli e “comandare” l'utente.

Questo è esattamente il punto della questione. Ad esempio lo smartphone che avete in tasca probabilmente contiene un sistema operativo piuttosto noto, almeno di nome, GNU/Linux (e se avete un iOS, derivato da kernel Mach e da FreeBSD), che, per vostro conto, appena acceso fa partire una quantità di programmi che l'utente non conosce e che non può conoscere, perché gli vengono, in tutti i modi possibili, tenuti “nascosti”.

Il motivo addotto è che questo semplifica la vita dell'utente, ma si tratta di una giustificazione di comodo; nulla impedirebbe che questo venisse fatto documentando in maniera accessibile a tutti, ed adeguata a vari livelli di competenza, tutte queste caratteristiche “nascoste”.

Ma questo, vedi caso, non avviene. Solo gli utenti più esperti possono avere un'idea di quello che accade, utilizzando fonti di informazione inaccessibili alla maggior parte degli altri utenti.

E questa era la storia che dovevamo ricordare. Veniamo al punto. Cosa è successo negli ultimi anni?

Descriverlo non è semplice e può essere persino tendenzioso, ma proviamoci comunque perché è indispensabile.

Gli smartphone, dotati tutti di sistemi operativi derivati da Unix, se fossero stati sicuri come computer “normali”, avrebbero permesso facilmente di accedere in maniera anche distruttiva alle infrastrutture delle reti cellulari, che non sono pensate per essere gestite in sicurezza; queste reti sono un “colabrodo” anche se costano un pacco di soldi,

Installando in Android SELinux, una particolare estensione di Linux per sistemi ad alta sicurezza, proteggendo il processo di boot, e soprattutto eliminando la possibilità di interagire da terminale, il sistema operativo è stato reso inaccessibile alla maggioranza degli utenti, e quindi più “sicuro” per garantire l'integrità delle reti cellulari (anche iOS ha attraversato fasi del tutto simili).

Come importantissimo effetto collaterale, però, questo ha reso possibile a chi produce cellulari, a chi fornisce il sistema operativo ed addirittura a chi scrive app, di eseguire operazioni arbitrarie sullo smartphone senza che l'utente potesse percepirlo, impedirlo o semplicemente saperlo.

E questo permette di “estrarre” dai proprietari quelle informazioni personali che una volta memorizzate ed elaborate permettono di esercitare un controllo sugli utenti (vedi Cambridge Analytica) ma per fortuna non consentono ancora un controllo diretto ed atomico sul singolo utente del singolo smartphone.

Però la prossima generazione di Android ed iOS, e le future prossime generazioni di qualunque oggetto connesso, integreranno funzionalità guidate dagli LLM e da altre tecnologie di IA.

Questo permetterà agli utenti di impartire comandi allo smartphone in linguaggio naturale od anche con semplici gesti. Permetterà quindi di impartire istruzioni imprecise ed incomplete, lasciando all'IA il compito di precisare in relazione al contesto ed eseguirle.

Ma questa è la metà “positiva” di questa novità. Quella negativa, quella che peggiorerà una situazione informatica già largamente compromessa, quella che mozza il respiro a Cassandra quando ci pensa o ne parla è la possibilità, diretta e distribuita, di controllare il pensiero e le azioni dell'utente tramite la manipolazione delle funzionalità IA che sta utilizzando.

La possibilità di controllare il “comportamento” degli LLM in modo da fornire risposte manipolate a richieste degli utenti è non solo dimostrata, ma è stata oggetto di [pubblicazioni universitarie](#) e progetti di ricerca. Manca davvero poco perché metodi di controllo impercettibile della volontà e dei pensieri degli utenti siano presenti in tutto quello che abbiamo attorno ed in tasca.

La presenza negli smartphone di queste funzionalità, inevitabili come il Male, e l'utilizzo che solamente chiunque lo voglia potrà farne, faranno impallidire i metodi attuali di tecnocontrollo, utilizzati attraverso i social per controllare la popolazione in situazioni particolari come le elezioni (vedi il caso di [Cambridge Analytica](#) e quello che ne scriveva [Cassandra](#)).

E ciò che una volta veniva chiamato “sistema operativo” e rappresentava un utile strumento per fare cose ben precise sotto la guida di una mente umana, si fonderà con altre meraviglie tecnologiche moderne, creando uno strumento di tecnocontrollo individuale, per assurdo anche gradito e finanziato dagli stessi controllati.

In assenza di una presa di coscienza che potremmo definire democratica, ma **che è prima di tutto individuale**, sembra inevitabile che gli oggetti connessi intorno a noi, nelle nostre tasche, appesi od all'interno dei nostri corpi, vengano utilizzati come connettori uomo-macchina bidirezionali, che saranno inevitabilmente utilizzati anche per il tecnocontrollo pervasivo ed ubiquo degli esseri umani.

[Scrivere a Cassandra](#) - [Mastodon](#) - [Buttondown.com](#)

[Videorubrica “Quattro chiacchiere con Cassandra”](#)

[Lo Slog \(Static Blog\) di Cassandra](#)

[L'archivio di Cassandra: scuola, formazione e pensiero](#)

[Cassandra per i posteri: l'archivio](#) su [Internet Archive](#)

Licenza d'utilizzo: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0), tutte le informazioni di utilizzo del materiale sono disponibili a [questo link](#).