→ **Analisi** → significa osservare un sistema per dedurne alcune proprietà di sicurezza

Dinamica

↓

eseguita in runtime

(**sistemi fuzz in**)

↓

utilizzati per cercare dati in grado di scatenare attacchi di tipo buffer overflow

Statica

↘ viene effettuata quando il sistema non è in esecuzione

↘ guardando una sua "rappresentazione"

↘ codice sorgente

↘ esempio: l'analisi di un sistema firewall per il filtraggio di pacchetti, avrà una descrizione che sarà data dalle regole di filtraggio impostate

→ **Analisi statica**

↓ **vantaggi**

↓

potrebbe essere esaustiva

→ **svantaggi** → l'analisi dinamica è più realistica

↓ anercsa

↓ è un'approssimazione di come il sistema si comporta

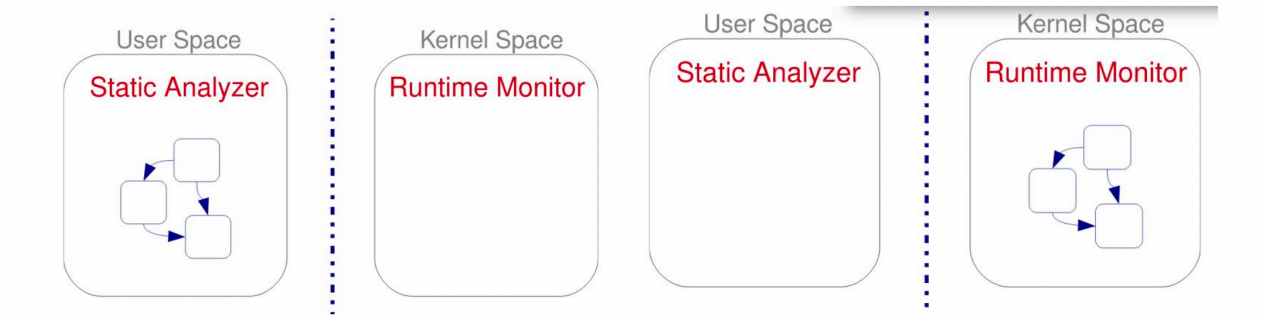
↓ model checking → solo alcune proprietà vengono testate

→ **Korset** → sfrutta una fase di anali statica e una fase di analisi dinamica.

↓ la "sorveglianza" è fatta da una parte di sistema operativo che non è in mano all'utente.

↓ Il punto di passaggio da User spa ie e Kernel space è dato dalla System call. (code Injection)

Runtime | Sistema Operativo



→ Il sistema Korset organizza questa infrastruttura di "sorveglianza" e "sorvegliati" passando da una parte statica a una dinamica

→ **Analisi Statica** → avviene attraverso una definizione di quello che è un comportamento normale del mio sistema andando ad analizzare staticamente il Control flow. → codice C

Abbiamo un lato User Space e l'esecuzione di un analizzatore statico che analizza il codice sorgente per produrre → **una rappresentazione sotto forma di automa a stati finiti**

approssimazione

Dal lato Kernel utilizzeremo tale automa

→ Di tutto il codice vengano selezionate solo le informazioni realmente utili.

→ Avviene un confronto tra modello a stati finiti e syscall

→ **Stage 1 : creazione automa**

- Assunzione: le chiamate di sistema sono l'unico modo per infliggere danno

- Principio: System call sequences => Paths in the graph,
No path in the graph? => Invalid system call sequence (Malfunzionamento, possibile attacco?)

-> Stage 2: monitoraggio a runtime

Ogni volta che arriva una system call dallo user space, si va a valutare quale operazione è stata effettuata e si aggiorna lo stato del sistema definito dall'automa

Questo passaggio prevede di passare l'automa al sistema operativo

-> Tool per implementare -> Flawfinder
-> Boon