Cos’è eBPF?

* Spiegazione anagramma eBPF
* Dove e quando nasce:
  + Berkeley
  + BSD packet filter: macchina virtuale nel kernel per analizzare pacchetti (documento descrive come è fatta)
  + Documento: sistema di filtraggio pacchetti molto efficiente: pacchetti analizzati direttamente nel kernel
* Limiti di BPF:
  + Poca flessibilità a fronte di evoluzioni tecnologiche di hardware, protocolli di rete e architetture di rete
  + Non c’erano meccanismi di sicurezza per eseguire codice utente nel kernel
* Introduzione ad eBPF
  + Più registri a 64 bit (per andare incontro alle nuove architetture)
  + Programmi usati per scopi diversi, non solo per filtraggio pacchetti -> maggiore flessibilità
  + Aggiunta di meccanismi di sicurezza
  + Nuova chiamata di sistema per chiamare le funzioni del kernel più rapidamente (si vedrà in seguito)
  + Programmi hanno una memoria limitata
* Risultato: eBPF è una tecnologia che permette di eseguire programmi in maniera sandbox (isolati) in un contesto privilegiato, quale il kernel di un sistema operativo.

Pertanto, eBPF fornisce un approccio sicuro ed efficiente per estendere le funzionalità del kernel senza la necessità di modificare il codice sorgente del kernel o caricare i moduli del kernel scritti con le API native del kernel.

* Al giorno d’oggi costituisce il nome di una tecnologia, ma di fatto non è ancora diventato uno standard.
* Casi d’uso tra i più svariati nell’ambito dell’osservabilità di sistemi (uso risorse, chiamate di sistema,… per fare cyber security) e di performance, di ambienti cloud e container, oltre che a continuare a fare da filtraggio di pacchetti.
* Però è stata fondata l’eBPF foundation: istituire un comitato (Google, Meta, Netflix,…) per guidare la crescita di eBPF -> espandere conoscenza, definire requisiti, creare una community

Processo di esecuzione di un programma

Ci sono diversi modi per iniziare ad usare eBPF

* Usare dei tool da linea di comando
* Scrivere bytecode eBPF
* Scrivere programmi in un linguaggio di programmazione di alto-livello e sfruttare dei compilatori appositi (Clang-LLVM estesi per programmi eBPF) per generare il bytecode eBPF

Una volta che si ha il bytecode eBPF, questo va caricato nel kernel:

* Verifica: il programma deve essere safe per essere eseguito all’interno del kernel
  + Direct Acyclic Graph check -> programma termina
  + Analisi di profondità del Control Flow Graph -> controllo di tutte le istruzioni (no accesso ad aree di memoria proibite e complessità finita del programma)

Lo fa in modo smart

Programmi con istruzioni irraggiungibili o loop infiniti non passano il check.

No soluzione ad Halting problem (il verificatore usa dei particolari costrutti di eBPF per dire se un programma termina o meno)

* Hardening: aggiunge misure di sicurezza
  + Memoria del kernel tenuta dal programma eBPF è resa read-only
  + Tentativi di modificare il programma fanno crashare il kernel
  + Costanti rese non modificabili per evitare JIT spraying attacks (come JS injection)
* Compilazione JIT
  + Traduce il bytecode eBPF verificato in codice macchina nativo che corrisponde all'architettura della CPU di destinazione che può essere eseguita direttamente da processore
  + Risultato: programma efficiente come se fosse del codice kernel compilato in modo nativo e caricato come un LKM
* Caricamento ed esecuzione
  + Il programma è caricato nel kernel con una chiamata di sistema e viene eseguito

Peculiarità di un programma eBPF

Un programma eBPF scritto con un linguaggio di programmazione di alto livello deve sfruttare dei costrutti sintattici per permettere al verificatore di svolgere il suo lavoro:

* Dire in quale punto del kernel attaccare il programma ed il tipo di programma -> hook point
* Usare delle strutture dati per scambiare dati tra utente e kernel -> mappe (quasi tutte sono chiave-valore, tranne un tipo che permette all’utente solo di leggere da una zona di dati comune)
* Usare delle funzioni per chiamare le funzioni nel kernel (non si possono chiamare direttamente per impedire la correlazione stretta tra funzioni eBPF e funzioni kernel che dipenderebbero dal particolare kernel)
  + Alcuni helper per tipo di programma si possono chiamare
  + Non più di 5 argomenti
  + Non introducono overhead -> i programmi eBPF chiamano direttamente la versione compilata dell’helper
* Inoltre helper e mappe si usano in combinazione per performare le “tail call”: dato che i programmi eBPF hanno una memoria limitata, se si vuole usare un programma che richiede più memoria si usano helper e mappe particolari che ad un certo punto cambiano il contesto d’esecuzione da un programma al successivo

La chiamata di sistema

* Serve per caricare il programma nel kernel.
* È un’interfaccia fornita da Linux per permettere agli utenti di usare le funzionalità di eBPF all’interno del kernel
  + Header contiene la definizione di macro, funzioni e struct che si usano con eBPF
  + Cmd: operazione da svolgere (fornisce un API per dire dove il programma si attaccherà nel kernel e quali helper potrà chiamare)
  + Attr serve per passare dati da lato utente a lato kernel
  + Size è la dimenzione di attr.
* Non va chiamata direttamente nel codice: usiamo gli helper che durante il processo di compilazione JIT chiameranno indirettamente quella syscall

Il problema della portabilità

* Definizione (A.N.)
* Problema: struct e campi cambiano tra versioni del kernel successive
* Soluzione temporanea: BCC
  + Toolkit per creare programmi eBPF
  + Per assicurarsi il layout della memoria del kernel è lo stesso previsto dal programma eBPF, quando l'applicazione viene eseguita dall'host, BCC chiama il suo compilatore incorporato, che consiste nella combinazione Clang-LLVM, inserisce le intestazioni nel kernel e esegue la compilazione al volo.
  + Problemi:
    - Distribuire il compilatore insieme al programma
    - Difficile lavorare in modo agile perché gli errori si hanno solo in compilazione

BPF CO-RE

* Insieme di cose per far funzionare il concetto
  + BPF Type Format (BTF), un formato di metadati compatto ma sufficientemente espressivo che descrive le informazioni dei programmi C e viene utilizzato per migliorare le capacità del verificatore;

Con BPF CO-RE, i programmi eBPF sono compilati in un formato più compatto e in una rappresentazione intermedia di un file binario che può essere caricato ed eseguito su più versioni e configurazioni del kernel.

Ciò riduce la necessità di ricompilare i programmi diverse versioni del kernel, rendendo i programmi eBPF più portabili ed efficienti.

* + Un supporto per il compilatore, come Clang, un compilatore front-end per programmi C e C++, esteso con built-in che consentissero la cattura di campi o set, esistenza e dimensione, dimensione del tipo e rilocazione, valori enumerazione ed esistenza;

Se un programma vuole accedere ad un certo campo in a struct all'interno del kernel e questo campo è stato spostato in un offset diverso all'interno della stessa struct o anche in una struttura diversa, lo sviluppatore può trovare quel campo semplicemente tramite il suo nome e informazioni sul tipo.

* + Il kernel compatibile con CO-RE.

Servono le informazioni BTF del kernel: si trovano nel file vmlinux.h che contiene tutti i tipi usati dal kernel in esecuzione sulla macchina nel suo codice sorgente

Dopo che abbiamo le 3 cose, un loader, chiamato libbpf, prende il file oggetto BPF generato dopo il file processo di compilazione del programma e innesca le fasi di caricamento e verifica;

consente la portabilità dei programmi eBPF risolvendoli e abbinandoli a tutti i tipi e i campi nel kernel e aggiorna necessari offset e altri dati riposizionabili.

* Libbpf: libreria per interagire con l’ecosistema eBPF nel kernel Linux -> implementazione BPF CO-RE
  + Permette agli utenti di preoccuparsi solo del codice, gestendo le relocations, verifica e caricamento nel kernel, creazione di mappe, hook points,…
  + Astrae molti concetti tramite la sua API per creare programmi eBPF
  + Richiede di conoscere solo le informazioni BTF del kernel e del programma

Risultato: programmi compilati una volta possono essere eseguiti su ogni kernel

* + Inoltre fornisce gli skeleton header files, un’interfaccia alternativa alle API di libbpf per gestire gli programmi eBPF dal lato utente (open, load, attach, tear down)

Linux: BumbleBee

* Progetto open source incentrato sulla semplificazione dell'esperienza dell'utente nella creazione di strumenti eBPF.
* Aiuta gli sviluppatori a creare, eseguire e distribuire programmi eBPF utilizzando il concetto di container tramite immagini Open Container Initiative (OCI).
* Basta clonare un repo su VM Ubuntu
* Scelte e creazione programma
* Limiti: solo 2 hook points e 2 mappe
* Usa dei costrutti per gestire in modo automatico il lato utente che non esistono se si scrivono programmi con libbpf (esempio: formato di output)

Linux: libbpf-bootstrap

* Progetto open source creato per setuppare più cose possibile per i novizi di eBPF
* Basta clonare un repository
* Processo
  + Scrittura programma eBPF
  + Compilazione: generazione file oggetto e skeleton file
  + Importare skeleton file nel programma lato utente per fare ciclo di vita del programma
  + Avviare programma

Windows: ebpf-for-windows

* Difficoltà nel setup dell’ambiente non indifferente: un ambiente adatto per lo sviluppo in Windows con eBPF è molto più difficile che in Linux (PUNTO CRITICO)
  + Linux: clonare repo e assicurarsi che ci siano le informazioni BTF del kernel
  + Windows: processo installazione VM complesso
    - Il requisito di avviare Windows in modalità di test e la necessità di utilizzare driver (programma per far comunicare sistema operativo e hardware del computer, senza il quale il pc non potrebbe svolgere molte funzioni) firmati digitalmente (o dal produttore o come test) o un certificato di test quando si lavora con eBPF su Windows sono dovuti a motivi di sicurezza e controllo dei driver nel sistema operativo.

Requisiti progettati per proteggere la stabilità e la sicurezza del sistema operativo Windows.

Tuttavia, è importante notare che questi requisiti possono essere gestiti dagli sviluppatori e dagli utenti avanzati, ma dovrebbero essere trattati con cautela, soprattutto quando si utilizzano driver non firmati o certificati di test solo in ambienti di sviluppo e test, evitando di compromettere la sicurezza del sistema in produzione.

* + - Avviare la VM con un KD attaccato

Sviluppo e debugging + tracciamento e analisi + sicurezza

Un kernel debugger consente agli sviluppatori di ispezionare in tempo reale il comportamento dei programmi eBPF in esecuzione nel kernel di Windows.

Un kernel debugger è fondamentale quando si lavora con eBPF su Windows perché fornisce agli sviluppatori gli strumenti necessari per sviluppare, testare, analizzare e risolvere i problemi dei programmi eBPF in modo efficace e sicuro.

* Consentire agli sviluppatori di utilizzare le familiari toolchain eBPF e le interfacce di programmazione delle applicazioni (API) oltre alle versioni esistenti di Windows.
* Basandosi sul lavoro di altri, questo progetto prende diversi progetti open source eBPF esistenti e aggiunge il "collante" per farli funzionare su Windows.
* Come mostrato nel diagramma, le toolchain eBPF esistenti come clang possono essere utilizzate per generare bytecode eBPF dal codice sorgente in varie lingue. Il bytecode risultante può quindi essere utilizzato da qualsiasi applicazione o manualmente tramite lo strumento da riga di comando netsh di Windows, che utilizzano entrambi una libreria condivisa che espone le API Libbpf, sebbene questo lavoro sia ancora in corso.
* La libreria invia il bytecode eBPF a un verificatore statico (il verificatore PREVAIL) che è ospitato in un processo protetto in modalità utente, che è un ambiente di sicurezza Windows che consente a un componente del kernel di considerare attendibile un demone in modalità utente firmato da una chiave che esso si fida. Se il bytecode supera tutti i controlli di sicurezza del verificatore, il bytecode può essere caricato nell'interprete uBPF in esecuzione in un contesto di esecuzione in modalità kernel di Windows o compilato dal compilatore just-in-time uBPF e avere il codice nativo caricato in modalità kernel contesto di esecuzione.
* I programmi eBPF installati nel contesto di esecuzione in modalità kernel possono collegarsi a vari hook per gestire eventi e chiamare varie API di supporto esposte dallo shim eBPF, che racchiude internamente le API pubbliche del kernel di Windows, consentendo l'uso di eBPF su versioni esistenti di Windows. Finora sono stati aggiunti due hook (XDP e socket bind) e, sebbene si tratti di hook specifici della rete, prevediamo che nel tempo verranno aggiunti molti altri hook e helper, non solo relativi alla rete.
* eBPF è una tecnologia nota ma rivoluzionaria, che offre programmabilità, estensibilità e agilità. eBPF è stato applicato a casi d'uso come la protezione dalla negazione del servizio e l'osservabilità. Nel corso del tempo, attorno a eBPF è stato costruito un significativo ecosistema di strumenti, prodotti ed esperienze. Sebbene il supporto per eBPF sia stato implementato per la prima volta nel kernel Linux, c'è stato un crescente interesse nel consentire l'utilizzo di eBPF su altri sistemi operativi e anche per estendere servizi e demoni in modalità utente oltre al solo kernel.
* Il progetto eBPF for Windows sfrutta progetti open source esistenti, come [IOVisor uBPF](https://github.com/iovisor/ubpf" \t "_blank) e il verificatore [PREVAIL,](https://github.com/vbpf/ebpf-verifier) che vengono eseguiti on top of Windows aggiungendo cose specifiche epr l’ambiente Windows per il codice.
* Obiettivo: fornire compatibilità per i codici che usano hook points e helpers che possono essere applciati su sistemi operativi diversi (ovviamente non quelli specifici per linux che ha molti hook points e helpers)
* Espone API libbpf per fornire codice sorgente compatibile per applicazioni che interagiscono con programmi eBPF

Windows: windows-ebpf-starter

* Progetto open source che vuole essere come libbpf-bootstrap ma per windows
* Richiede comunque il setup dell’ambiente
* Lato kernel funziona come spiegato da ebpf-for-windows
* Lato utente dovrebbe automatizzare il ciclo di vita di un programma eBPF senza sfruttare degli skeleton file, ma usando dei metodi per manipolare oggetti eBPF presenti all’interno dell’API di ebpf-for-windows.

Inoltre ci sono dei problemi con i vari “include” degli header file perché il progetto non riconosce quelli al di fuori della libreria ebpf-for-windows.

Potenziale di eBPF

* In Linux e Windows:
  + Nuovi hook points, mappe, helpers
  + Windows: raggiungere Linux
* Usi futuri:
  + Proseguire con quanto iniziato
  + IoT perché è leggero ed efficiente (gateways per filtraggio pacchetti in modo intelligente),
  + Cloud e container -> maggiore scalabilità
  + Osservabilità e tracciamenti di sistemi distribuiti -> visualizzare eventi
  + Gestire cyber-minacce -> sistemi di detection e applicazioni in sicurezza
  + AI e ML per decision-making intelligente e gestione risorse in modo dinamico
  + Nuovi frameworks prodotti dalla community

1. Sicurezza del Sistema Operativo: Windows è progettato per garantire la sicurezza e la stabilità del sistema operativo. L'esecuzione di driver non firmati o non verificati potrebbe rappresentare un rischio per la sicurezza del sistema. Per mitigare questo rischio, Windows richiede di default che i driver siano firmati digitalmente da un'autorità attendibile.
2. Controllo dell'Integrità del Kernel: I driver del kernel, inclusi quelli utilizzati per interagire con eBPF, hanno un impatto diretto sull'integrità e sulla stabilità del kernel di Windows. La firma digitale dei driver fornisce un meccanismo di controllo dell'integrità che aiuta a garantire che i driver siano affidabili e non compromettano il funzionamento del sistema operativo.
3. Evitare Exploit: L'esecuzione di driver non firmati o non verificati potrebbe consentire a software dannoso o a exploit di compromettere il sistema operativo. Richiedere la firma digitale dei driver aiuta a prevenire queste situazioni.
4. Certificazione di Test: Il "certificato di test" è una sorta di permesso temporaneo che consente ai driver di essere caricati in modalità di test. Questo è utile per gli sviluppatori che stanno sviluppando e testando driver eBPF senza doverli firmare digitalmente con un certificato valido. Tuttavia, questa modalità dovrebbe essere utilizzata solo in ambienti di sviluppo o test e non in produzione.