Dynamic ARP Inspection Open Source una soluzione accessibile e adattabile al servizio della sicurezza degli apparati di rete e degli utenti

Alessandro Meloni (matricola 984857)

Relatore: Prof. Ernesto Damiani

Il presente elaborato di tesi affronta una delle criticità più persistenti nella sicurezza delle reti locali (LAN): la vulnerabilità intrinseca dell'**Address Resolution Protocol (ARP)**. Progettato in un'epoca di fiducia implicita tra i nodi, ARP manca di meccanismi nativi di autenticazione, esponendo le infrastrutture a rischi severi quali l'**ARP Cache Poisoning** e i conseguenti attacchi **Man-in-the-Middle (MITM)**. Sebbene l'industria abbia risposto con soluzioni efficaci come la *Dynamic ARP Inspection* (DAI) integrata negli apparati Enterprise (es. Cisco Catalyst), l'accesso a tali tecnologie rimane precluso a una vasta utenza a causa degli elevati costi di licenza e hardware.

L'obiettivo primario di questo lavoro è colmare tale divario tecnologico ed economico, proponendo un cambio di paradigma: la democratizzazione della sicurezza di livello 2 attraverso lo sviluppo di una soluzione **Dynamic ARP Inspection Open Source**. Come discusso approfonditamente nel capitolo 2, e in particolare nella sezione 2.4, la sicurezza non deve essere un privilegio accessorio riservato alle grandi infrastrutture aziendali, ma un requisito fondamentale integrabile in dispositivi eterogenei e accessibili. Questo progetto dimostra come sia possibile replicare le logiche di validazione delle soluzioni proprietarie utilizzando software aperto, trasparente e verificabile, svincolando l'amministratore di rete dal **vendor lock-in**.

Sotto il profilo ingegneristico, la tesi descrive l'intero ciclo di vita del software, dalla progettazione architetturale all'implementazione in linguaggio **C**. La scelta del linguaggio e l'adozione di librerie standard come **Libpcap** e **POSIX Threads** rispondono a requisiti stringenti di performance e portabilità. L'architettura del daemon sviluppato si basa sul pattern concorrente **Produttore-Consumatore**, implementando un **thread ricevitore** dedicato per ogni interfaccia di ascolto e un **pool di thread analizzatori** per la gestione parallela del carico delle validazioni. Tale configurazione rappresenta una scelta progettuale critica per disaccoppiare l'acquisizione dei pacchetti ad alta frequenza dalla logica di validazione, ottimizzando l'allocazione delle risorse di calcolo.

Il sistema intercetta selettivamente le trame ARP Reply in transito sul gateway, sottoponendo le loro associazioni $\langle$IP, MAC$\rangle$ a una verifica rigorosa. Implementando una politica di sicurezza **Deny-by-Default**, il software considera qualsiasi messaggio ARP illegittimo fino a prova contraria, ovvero la presenza di un'associazione $\langle$IP, MAC$\rangle$ equivalente nelle Lease DHCP.

Particolare enfasi è stata posta sull'ottimizzazione delle strutture dati e sulla gestione delle risorse. L'implementazione di una coda circolare (**Ring Buffer**) thread-safe e l'uso mirato di primitive di sincronizzazione (**Mutex** e **Condition Variables**) hanno permesso di eliminare le attese attive, garantendo l'utilizzo essenziale della CPU.

La validazione sperimentale, condotta in un ambiente virtualizzato complesso che simula topologie multi-LAN e scenari di attacco reali, ha prodotto evidenze quantitative significative. I test di carico hanno dimostrato come l'architettura multi-thread sia in grado di sostenere flood di oltre **34.000 PPS** mantenendo una latenza media di elaborazione nell'ordine dei microsecondi (**13-15 μs**), un miglioramento di due ordini di grandezza rispetto alle implementazioni sequenziali.

Tali risultati confermano la risoluzione delle criticità di saturazione, prevenendo il fenomeno del **Bufferbloat** e garantendo che l'aumento della dimensione della coda si traduca in resilienza effettiva anziché in latenza aggiuntiva. Inoltre, il sistema ha dimostrato eccellente capacità di isolamento: anche in condizioni di **Denial of Service** massiccio su un segmento di rete, il traffico legittimo sugli altri segmenti viene preservato e processato senza perdite, confermando la robustezza del design anche in scenari di routing complesso.

In conclusione, questo lavoro trascende l'implementazione tecnica per delineare una strategia concreta di democratizzazione della sicurezza. I risultati empirici confermano il raggiungimento di prestazioni **Real-Time** su hardware non professionale, colmando l'attuale divario tra le costose soluzioni Enterprise e i dispositivi consumer intrinsecamente vulnerabili. La compatibilità nativa con l'ecosistema Linux Embedded, e in particolare la sinergia con la gestione dei lease di **Dnsmasq**, elegge piattaforme comunitarie come **OpenWrt** a servizio del futuro del progetto.

Tale integrazione permetterebbe di estendere una protezione avanzata di livello 2 a contesti critici: supportando le **Piccole e Medie Imprese (PMI)** nell'abbattimento delle barriere economiche verso la sicurezza infrastrutturale aziendale; blindando gli ambienti domestici evoluti (**Home Lab** e **Smart Working**) con tutele professionali su dispositivi commerciali; e potenziando le **Infrastrutture della Pubblica Amministrazione Locale**, dove l'efficienza su hardware a risorse limitate permette di garantire la sicurezza della rete territoriale come diritto fondamentale del cittadino, concretizzando la visione di:

"Una sicurezza informatica non più intesa come privilegio economico, ma come bene comune accessibile al servizio degli utenti finali".