

# Riassunto Dynamic ARP Inspection Open Source

Il presente elaborato di tesi affronta una delle criticità più persistenti e pervasive nella sicurezza delle reti locali (LAN): la vulnerabilità intrinseca dell'**Address Resolution Protocol (ARP)**. Progettato in un'epoca in cui la fiducia tra i nodi di rete era un assunto implicito, ARP manca di meccanismi nativi di autenticazione, esponendo le infrastrutture moderne a rischi severi quali l'**ARP Cache Poisoning** e i conseguenti attacchi **Man-in-the-Middle (MITM)**. Sebbene l'industria del networking abbia risposto con soluzioni efficaci, in primis la *Dynamic ARP Inspection* (DAI) integrata negli apparati di fascia Enterprise (es. Cisco Catalyst), l'accesso a tali tecnologie rimane precluso a una vasta porzione di 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, e potenzialmente estendere, le logiche di validazione delle soluzioni proprietarie utilizzando software aperto, trasparente e verificabile, svincolando l'amministratore di rete dal **vendor lock-in** e restituendo il controllo sull'integrità del traffico locale.

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 porta-

bilità. L'architettura del daemon sviluppato si basa sul pattern concorrente **Produttore-Consumatore**, una scelta progettuale critica per disaccoppiare l'acquisizione dei pacchetti ad alta frequenza dalla logica di validazione. Il sistema opera intercettando selettivamente le trame ARP Reply in transito sul gateway, sottoponendole a una verifica rigorosa: validazione di presenza nella tabella dei lease DHCP. Implementando una politica di sicurezza **Deny-by-Default**, il software considera qualsiasi messaggio ARP illegittimo fino a prova contraria, ovvero il presentare un'associazione  $\langle \text{IP}, \text{MAC} \rangle$  presente nelle Lease DHCP. Particolare enfasi è stata posta sull'ottimizzazione delle strutture dati e sulla gestione della memoria. L'implementazione di una coda circolare (**Ring Buffer**) thread-safe e l'uso di primitive di sincronizzazione (**Mutex** e **Condition Variables**) hanno permesso di eliminare le attese attive, massimizzando l'efficienza 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  $\mu\text{s}$** ), un miglioramento di due ordini di grandezza rispetto alle implementazioni sequenziali. Inoltre, il sistema ha dimostrato un'eccellente resilienza: anche in condizioni di **Denial of Service** su un segmento di rete, il traffico legittimo sugli altri segmenti viene preservato e processato senza perdite, confermando la robustezza della logica di isolamento dei flussi.

In conclusione, questo lavoro trascende la mera 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 ma spesso privi di budget dedicato, quali le **Piccole e Medie Imprese (PMI)**, gli ambienti domestici evoluti (**Home Lab** e **Smart Working**) e le **Reti Civiche**, concretizzando la visione di:

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