“Best Practice” per IPV6

Francesco Prelz
3 Maggio 2010

Introduzione

La disponibilità e l'attivazione per default del protocollo IPv6 su vari sistemi, oltre al supporto di tale protocollo da parte del nostro service provider (GARR), suggeriscono una integrazione delle “best practice” di sicurezza raccolte nei documenti del gruppo “Harmony”.

Seguendo la struttura di tali documenti, dopo una premessa generale indichiamo qui le possibili integrazioni per:

a) Host security

b) Sicurezza delle LAN

c) Firewall e Router

Caratteristiche di IPv6 rilevanti per la sicurezza.

Seguendo la traccia del documento (1) indicato in bibliografia, queste sono le caratteristiche di IPv6 maggiormente differenti **rispetto a IPv4**:

- Le funzioni di *neighbor discovery*, autenticazione e cifratura (IPsec), *network* e *host mobility* vengono **tutte** assorbite a livello 3 nella definizione di IPv6 e degli header supportati. Ne consegue una maggiore complessità del protocollo e delle sue implementazioni, ed una maggiore dimensione dello header IP (che potrebbe non essere tutto contenuto nel primo frammento di un pacchetto). Inoltre tutti gli host che hanno il protocollo IPv6 abilitato e collegati allo stesso segmento di rete **devono** poter comunicare a livello 3 senza bisogno di ulteriore configurazione: configurano infatti automaticamente un indirizzo IPv6 *link local*.
- Lo spazio degli indirizzi è intrinsecamente più vasto (ogni sezione INFN avrà assegnati potenzialmente 2^{64} indirizzi, che sono 2^{32} internet V4...). Questo rende più difficile la scansione completa di una rete a “brute force”, ma rende allo stesso tempo più facile assegnare un indirizzo IPv6 casuale con trascurabile rischio di collisioni con altri indirizzi già assegnati.
- La MTU minima richiesta dal protocollo è di 1280 byte, e i dispositivi di rete intermedi **non** possono frammentare i pacchetti. La MTU massima lungo un dato percorso viene determinata prima via ICMPv6.

Da queste considerazioni consegue che l'introduzione di IPv6 **non consente di fare a meno di nessuna delle misure di sicurezza adottate oggi per IPv4** (le possibili vulnerabilità sono le stesse) e richiede di aggiornare alcune misure di sicurezza e procedure di monitoring, come elencato nel seguito.

Host security

Mentre è preferibile per ragioni di efficienza (se IPv6 è attivo vengono fatti tentativi di raggiungere

via IPv6 i servizi risolti in indirizzi IPv6 nel DNS) mantenere il protocollo IPv6 disabilitato se questo non è attivo nel collegamento con il GARR, deve essere evitato che i sistemi che hanno IPv6 attivo possano autoconfigurarsi e soprattutto che possano assumere il ruolo di "router IPv6 di default" inviando pacchetti di *router advertisement*.

La misura più efficace per evitare la comparsa di router "rogue" è avere un router IPv6 legittimo configurato ed attivo sulla rete locale (tipicamente il router di frontiera) che invia *Router Advertisement* **senza** il flag di *stateless autoconfiguration* (vedi sotto, paragrafo "Firewall e Router").

Sugli host **non** vanno configurati ed utilizzati meccanismi di transizione IPv4/IPv6 (6to4, Teredo o similari), e va attivato sufficiente monitoring IPv6 sulla rete locale per intercettare e identificare l'origine di *Router Advertisement* indesiderati (vedi sotto, paragrafo "Sicurezza delle LAN").

E' possibile che gli stack IPv6, solitamente di sviluppo nuovo e recente, siano sedi più probabili di bachi e vulnerabilità, ma le consuete raccomandazioni sull'aggiornamento dei sistemi operativi dovrebbero essere sufficienti a limitare i danni.

Sicurezza delle LAN

Le modalità di accesso e di configurazione dello stack IPv6, pur avvenendo tutte a livello 3, rimangono sostanzialmente le medesime. Al protocollo ARP si sostituiscono le operazioni ICMPv6 di *Neighbor Discovery* (NDP).

La possibilità di collisione di un indirizzo scelto casualmente con uno già assegnato sono invece minime, a causa del grande spazio di indirizzi disponibile. Quindi la possibilità che l'assegnazione di indirizzi IP sostituisca (impropriamente) la funzione di autenticazione o autorizzazione dell'accesso alla rete viene totalmente meno.

L'uso sistematico di meccanismi come 802.1x o *secure neighbor discovery* (SEND) pare essere la misura più appropriata per svolgere le funzione di autorizzazione all'accesso che dobbiamo offrire.

Dal punto di vista della sicurezza al livello di trasporto, IPv6 include nello standard i protocolli di IPSEC, e richiede a tutte le implementazioni di trattare gli header AH ed ESP. Quindi non cambia nulla rispetto alle possibilità presenti con IPv4.

Va infine verificato che tutti gli strumenti di monitoring di rete utilizzati (**arpwatch**, **ntop**, suite proprietarie ecc.) supportino il protocollo IPv6 (ad esempio ad **arpwatch** per IPv4 va affiancato uno strumento in grado di leggere gli scambi di *Neighbor Discovery* come **NDPmon**).

Firewall e Router

Se l'accesso IPv6 con il GARR **non** è ancora stato attivato, è necessario perlomeno disabilitare i meccanismi noti che permettono di collegarsi alla rete IPv6 via tunnel IPv4. Questi non hanno infatti alcuna utilità dal momento che l'accesso a IPv6 è disponibile a qualunque sede lo richieda.

Suggeriamo questi filtri:

1) blocco del protocollo IP (v4) '41' (ipv6), utilizzato per i tunnel;

2) blocco dell'accesso alla porta di 'Teredo' (UDP 3544).

Per i dettagli della configurazione per Cisco IOS e JunOS consultare la pagina:
http://www.mi.infn.it/ipv6/no_tunnels.html

Nel caso che l'accesso IPv6 sia stato attivato, è raccomandabile attivare la pubblicazione dei *Router Advertisemen*t **senza** il flag di autoconfigurazione abilitato (**`ipv6 nd ... no-autoconfig`** in Cisco IOS e **`no-autonomous`** in JunOS), a meno che altre misure di controllo dell'accesso di rete

siano attive (p.e.. IEEE 802.1x).

E' inoltre raccomandabile, sempre nel caso di accesso IPv6 attivo, applicare questi altri filtri sul router di frontiera:

3) filtrare il traffico che risulta proveniente da indirizzi multicast;

4) filtrare il traffico ICMPv6 secondo i criteri stabiliti in rfc 2463;

5) filtrare i pacchetti con extension header non necessari;

6) filtrare tutti i frammenti diretti ad un apparato di rete.

Questi filtri sono applicabili con Cisco IOS (versione ≥ 12.0(23)S o 12.2(13)T) e JunOS (versione ≥ 7.4). Per i dettagli consultare la pagina: http://www.mi.infn.it/ipv6/filters.html

Bibliografia

1) Sean Convery, Darrin Miller (Cisco), *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation*, Marzo 2004, http://seanconvery.com/v6-v4-threats.pdf

2) Janos Mohacsi (6net), *IPV6 security*, Gennaio 2005, http://www.6journal.org/archive/00000082/01/belgrade_mohacsi_security.pdf

3) Microsoft, *IPv6 Security Considerations and Recommendations* , Febbraio 2008, http://www.microsoft.com/technet/network/ipv6/ipv6sec.mspx

4) Sito del gruppo d'interesse INFN su IPv6: http://www.mi.infn.it/ipv6/