Gestione di Reti: sniffer SSDP

Claudio Fadda

Marzo 2017

1 Introduzione

Oggigiorno nella quasi totalità delle reti di computer troviamo connesse, oltre ai classici calcolatori, una grande varietà di periferiche condivise quali stampanti, NAS, videocamere di sorveglianza IP e molto altro ancora. Tali dispositivi utilizzano un protocollo comune per permettere di essere rilevati e identificati: il protocollo SSDP (Simple Service Discovery Protocol).
Lo scopo di questo progetto è la realizzazione di un programma che permetta di riconoscere tutti i dispositivi "plug&play" connessi alla rete catturando i pacchetti SSDP inviati e stampandone le informazioni principali.

2 Il protocollo SSDP

SSDP è un protocollo di rete basato sulla suite di Protocolli Internet (Internet Protocol suite, detta anche "suite protocolli TCP/IP") e serve a scoprire e pubblicizzare tra tutti i nodi di una rete la presenza di una o più periferiche condivise e utilizzabili.
Grazie al protocollo SSDP, il riconoscimento e il collegamento con la periferica sono di fatto automatizzati: non è necessario l'intervento dell'amministratore di sistema o dell'amministratore di rete per poter sfruttare le funzionalità della periferica, anche se dovrà comunque essere installata sulla macchina. Il Simple service discovery protocol, infatti, funziona senza l'assistenza di un meccanismo preimpostato sul server o sul router, come ad esempio il protocollo DHCP o il sistema DNS, e senza che l'amministratore di sistema debba assegnarli degli indirizzi IP privati e statici.

3 Realizzazione

Il programma di monitoraggio è stato realizzato in C utilizzando le librerie "libpcap" per la cattura dei pacchetti TCP/IP. Fondamentalmente si tratta di uno sniffer che seleziona solamente i pacchetti UDP aventi come porta sorgente la numero 1900.
Come prima cosa viene fatta una scansione dei device di rete disponibili all'analisi, se l'operazione va a buon fine viene stampata sullo standard output la lista dei device e si chiede all'utente di selezionare uno di essi per l'analisi. A questo punto il programma "stimola" la rete eseguendo il comando "gssdp-discover" sull'interfaccia selezionata; in questo modo vengono inviati, in broadcast sulla

porta 1900, dei pacchetti SSDP di richiesta di tipo "M-SEARCH". Alla ricezione di tali richieste i dispositivi "UPnP" condivisi rispondono con un pacchetto SSDP di tipo "NOTIFY" che viene catturato e catalogato dal programma. Il filtraggio avviene accettando in primo luogo solamente i pacchetti con campo "udph.source == 1900", dopodiché vengono presi in considerazione solo i pacchetti aventi campo "Request Method != M-SEARCH", quindi solamente quelli di risposta. Il payload dei pacchetti SSDP è "text-based", direttamente leggibile senza bisogno di particolari interpretazioni. Da ogni payload vengono selezionati i due campi più importanti per l'identificazione del dispositivo connesso: Il campo Server e il campo Location. Quest'ultimo contiene l'URL relativo alla descrizione del dispositivo. Tale indirizzo porta infatti ad una pagina in formato XML contenente le caratteristiche dettagliate quali produttore, modello, numero di serie, tipo del dispositivo e tante altre. Le due informazioni vengono associate al loro indirizzo ip sorgente e memorizzate nel file "log.txt" dopo un controllo volto a evitare la scrittura di duplicati.
Il programma resta in ascolto fino alla terminazione con la combinazione di tasti "ctrl+c" e stampa infine su standard output la lista dei dispositivi condivisi rilevati visualizzando per ognuno di essi IP, Server e Location nel formato:

——— Source device: 192.168.1.254 ———

LOCATION:http://192.168.1.254:80/upnp/IGD.xml
SERVER:Thomson TG 585 v8 8.2.7.A UPnP/1.0 (58-98-35-A8-7E-5A)