SICUREZZA NELLE RETI a. a. 2012/13 – Riassunto BGP

by Salvatore Fresta

Il **Border Gateway Protocol** (BGP) è un protocollo di **routing** per **Autonomous System** (AS) che adotta una politica di routing di dipo **path vector**, ovvero conosce già i possibili instradamenti che i pacchetti potrebbero prendere.

Non si basa dunque su una politica che prende in considerazione la distanza (*distant vector*) in quanto per il routing a questo livello **non** vengono applicati solo fattori di efficienza ma anche altri, tipo il costo o la politica (non voglio far passare il traffico americano da un AS russo ecc..).

I **concetti** alla base di BGP sono due:

1. Tutti i numeri IP che hanno i primi bit di un certo tipo (**prefisso**), sono **gestiti da un determinato AS.**

2. **AS path** è una **lista di AS da attraversare** per raggiungere un nodo con un determinato prefisso. Ad esempio per raggiungere l'Autonomous System A prima potrei dover passare dal C e poi dal B.

Il **funzionamento** avviene tramite query di **UPDATE** tra **diversi AS**:

1. Un AS denominato A **annuncia** (UPDATE) **ai propri AS vicini** di saper indirizzare i nodi con **prefisso** x, inviando il path **(A x)**.

2. B riceve il messaggio e lo ritrasmette ai propri vicini **(B A x)**: io sono B, posso raggiungere A che è in grado di raggiungere i nodi con prefisso x.

3. Ovviamente chi riceve un path che **contiene se stesso** non lo riannuncia.

Le connessioni avvengono sulla porta **TCP 179** (è curioso come un protollo di routing faccia uso di un protocollo transport).

I **problemi di sicurezza** sono:

- **Alterazione del canale di routing** (subverted link) da cui ci si difende con un'infrastruttura a **chiavi asimmetriche**.

- **Router maligni** (subverted router) per compromissione, spoofing (se non c'è PKI) o mal configurazione.

BGP inoltre **non prevede autenticazione della sorgente**, **integrità** dei messaggi e **non c'è controllo sull'ownerships dei prefissi** (nessuno vieta a B di annunciare di saper indirizzare la stessa rete di A anche se non è vero. Non c'è modo di attribuire sicuramente un prefisso ad un AS).

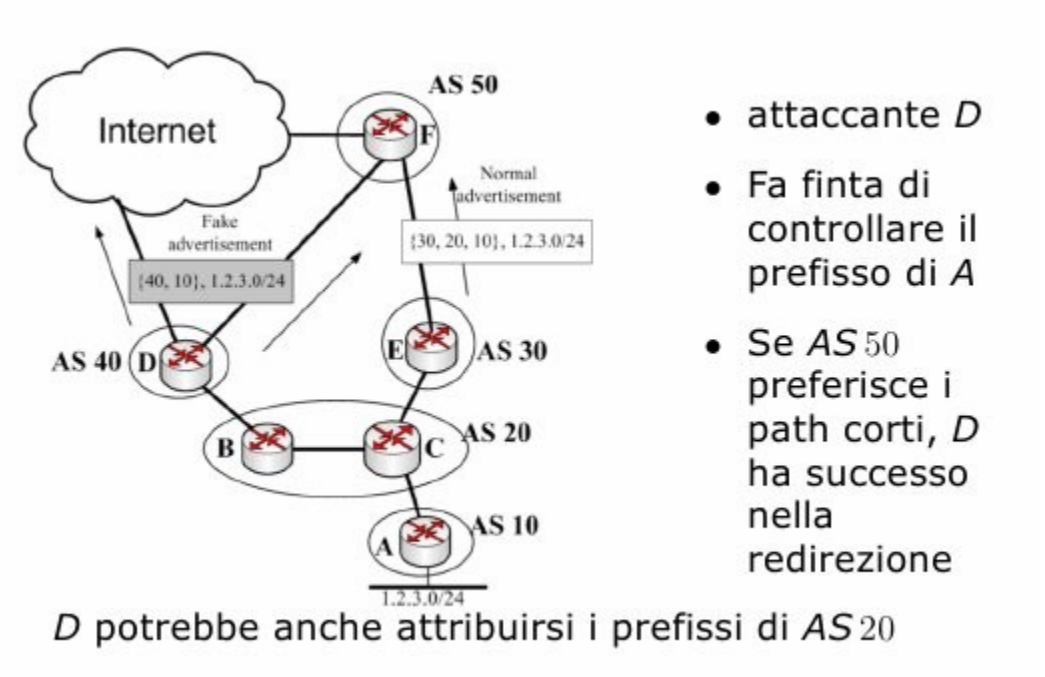
L'incoerenza delle informazioni **può anche essere normale** a causa del continuo evolversi della rete, ma se un attaccante conosce la topologia della rete, può creare informazioni **false ma coerenti**.

Quindi gli attacchi mirano a falsificare le informazioni per

- Redirezione del traffico
- Instabilità del routing
- Black hole (ricevere tutto il traffico e non inoltrarlo a nessuno, un po' come il funzionamento dei buchi neri che attirano la materia e non la rilasciano più)

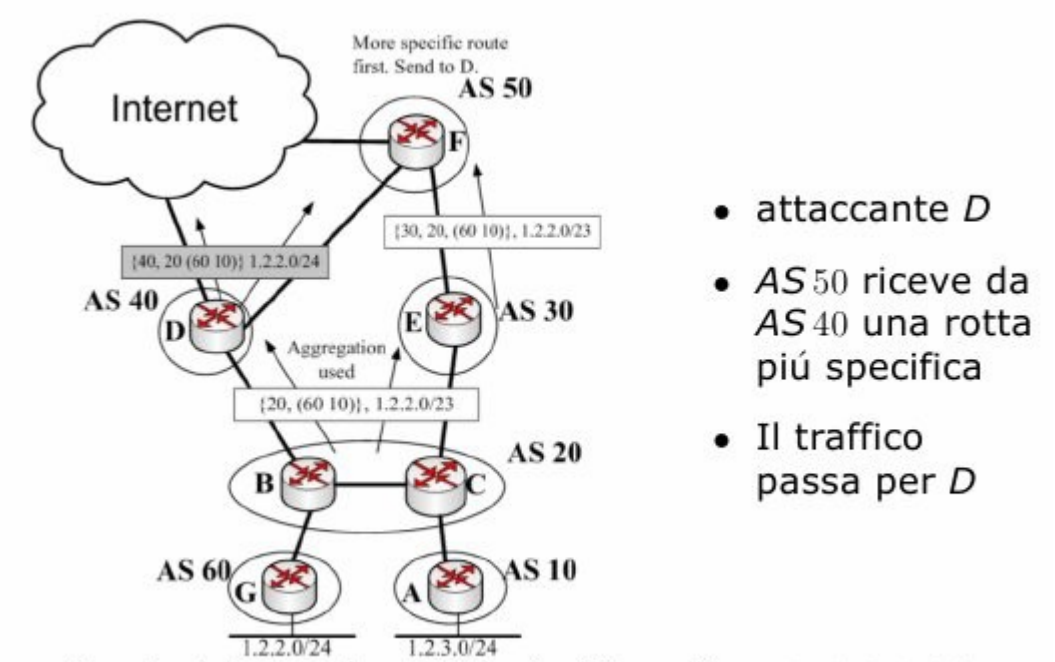
PREFIX HIJACKING

Annunciare **illecitamente** ai vicini la capacità di instradare un **prefisso** che in realtà **appartiene a qualcun altro**. In questo modo un AS può attribuirsi i prefissi che andrebbero ad un altro AS.



PREFIX DE-AGGREGATION

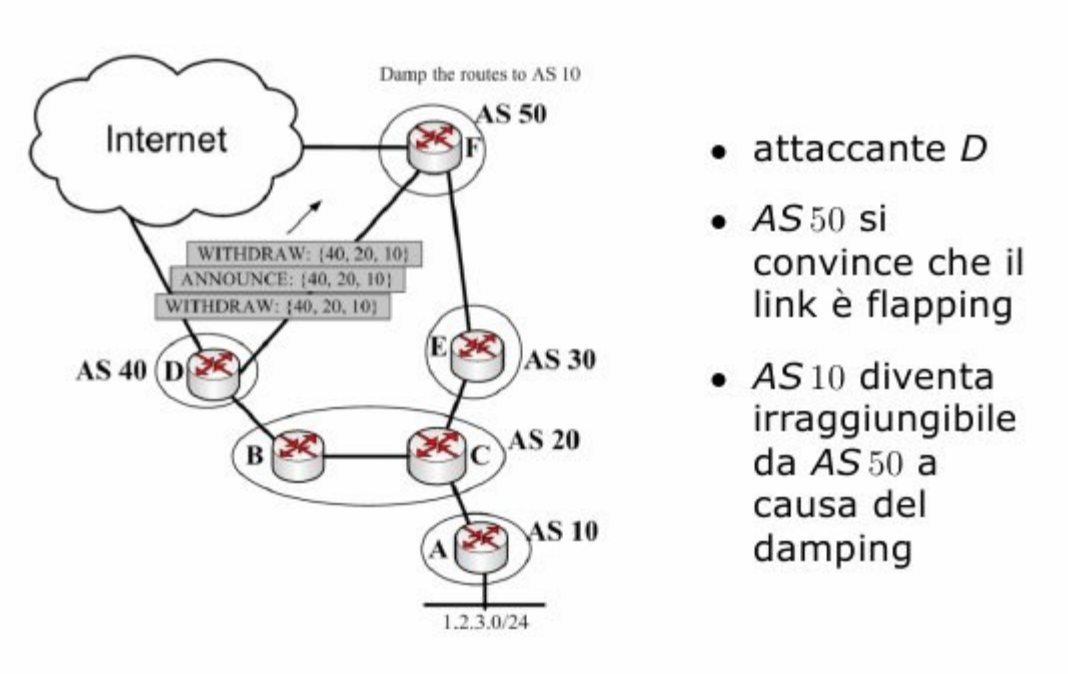
Disaggregare il prefisso ed annunciarlo ai vicini in modo tale che il protocollo decida di seguire questa nuova via in quanto è **più specifica** (precisa) di una con prefissi aggregati.



FLAPPING ATTACK

Può capitare che per diversi motivi **un link vada giù** per poi essere riattivato (**link flapping**). Ma se questo avviene di continuo si hanno delle instabilità di rete. Per evitare questo, un AS tiene conto di quante volte il link va giù e se il numero di volte è sempre in aumento, allora la via in questione viene utilizzata sempre più raramente. Questa tecnica è nota come **route damping**.

Se un AS malevolo inizia a comunicare continuamente degli up e down di un link di un AS benevolo, la vittima **si convince che si tratta di flapping** e lo disattiva dalla propria lista.



Oltre alle **evoluzioni** sicure di BGP, una contromisura a questi attacchi sono delle regole di **egress-ingress** che scartano i path relativi a prefissi imprevisti.