Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2013/14

[1] © 2011–14 M. Monga. Creative Commons Attribuzione — Condividi allo stesso modo 4.0 Internazionale. http://creativecommons.org/licenses/by-sa/4.0/deed.it. Derivato con permesso da © 2010 M. Cremonini.

Lezione XVIII: BGP

L'infrastruttura di Internet

Internet è una reti di reti locali.
Il routing a livello globale, però è gestito fra Autonomous System (AS), insiemi di reti locali con un'autonomia amministrativa.

In un AS valgono routing policy specifiche, non necessariamente concordate con gli altri
Il routing fra AS è affidato a protocolli particolari.

BGP

Il Border Gateway Protocol è un protocollo usato per il routing fra AS

- path vector: l'instradamento è fatto conoscendo una serie di path
- le decisioni non sono prese con riferimento alle "distanze", ma a politiche di routing

Testo di riferimento: A. Wong, A. Yeung, *Network Infrastructure Security*, Springer

Concetti di BGP

- I nodi indirizzabili da un AS sono quelli con un determinato *prefisso*
- Un *AS path* è la lista degli AS da attraversare per raggiungere un nodo con un dato prefisso
  1. Un AS A annuncia (`UPDATE`) ai vicini quali prefissi x sa indirizzare ($A\,x$)
  2. Il vicino B annuncia ($B\,A\,x$)
  3. Chi riceve un path che contiene sè stesso non lo riannuncia
  4. I path contengono anche attributi utilizzabili nelle policy

BGP

Le comunicazioni BGP fra AS avvengono tramite una connessione TCP (porta 179). I principali pericoli sono:

- Alterazione dei dati di routing (subverted link)
- Router maligni (subverted router)

Attacchi esterni

Dai subverted link ci si può difendere con un'infrastruttura a chiavi asimmetriche (non presente nel protocollo di base). Come al solito, la gestione delle PKI è complessa, ma molto efficace. (Non difende dall'*interruzione* del collegamento, naturalmente)

Attacchi interni

Un router maligno, per:

- compromissione
- spoofing (se non c'è PKI)
- mal configurato

Vulnerabilità di BGP

Senza opportune precauzioni (estensioni PKI), BGP:

- non prevede autenticazione della sorgente, né integrità dei messaggi
- non c'è controllo sull'ownership dei prefissi
- non c'è controllo sulle informazioni di path

Controlli di coerenza

A volte è possibile rilevare un'incoerenza nelle informazioni di routing

- non sono necessariamente dovute a compromissioni
- quasi mai si riesce a determinare l'informazione corretta
- se l'attaccante conosce la topologia della rete, generalmente può produrre informazioni false, ma coerenti

Riassumendo

Il protocollo BGP per il routing fra AS

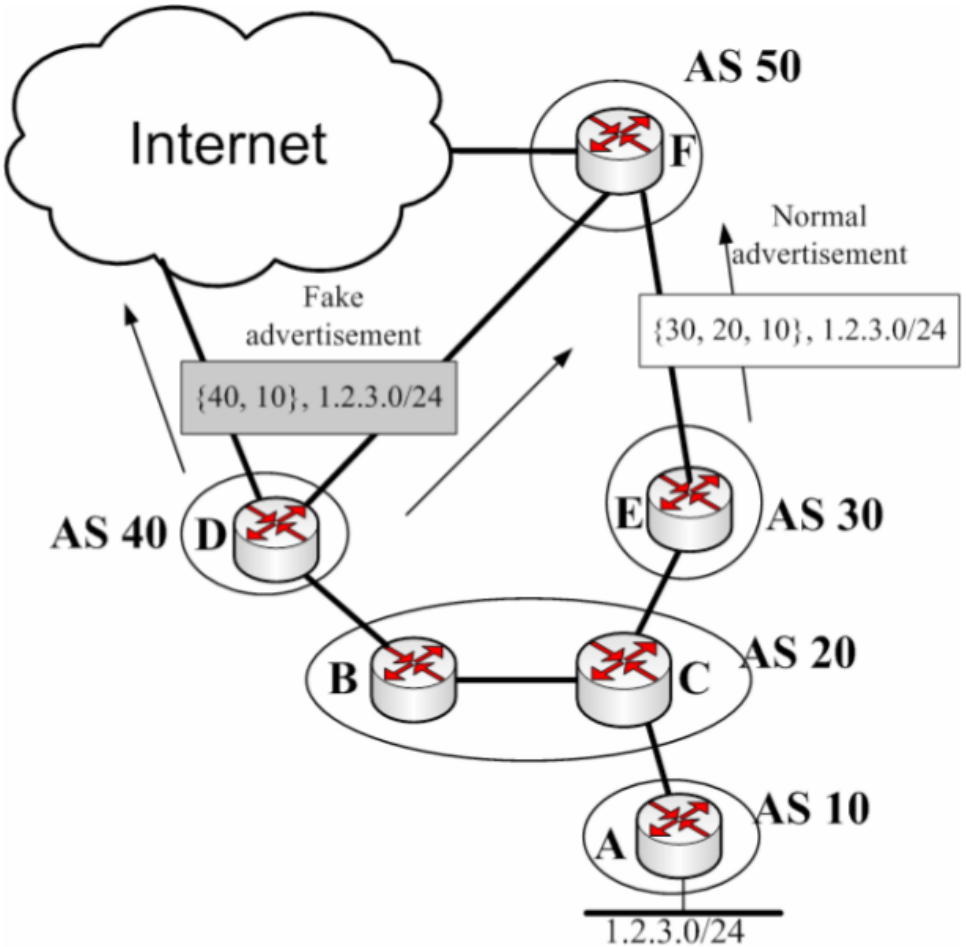
- È un protocollo path vector che permette di fare routing in base a policy complesse (non solo secondo la "distanza")
- Nella versione base non prevede garanzie di sicurezza

Obiettivi degli attacchi

La falsificazione delle informazioni di routing può servire per

- Redirezione del traffico
- Instabilità del routing
- Black hole

Prefix Hijacking



D potrebbe anche attribuirsi i prefissi di *AS* 20

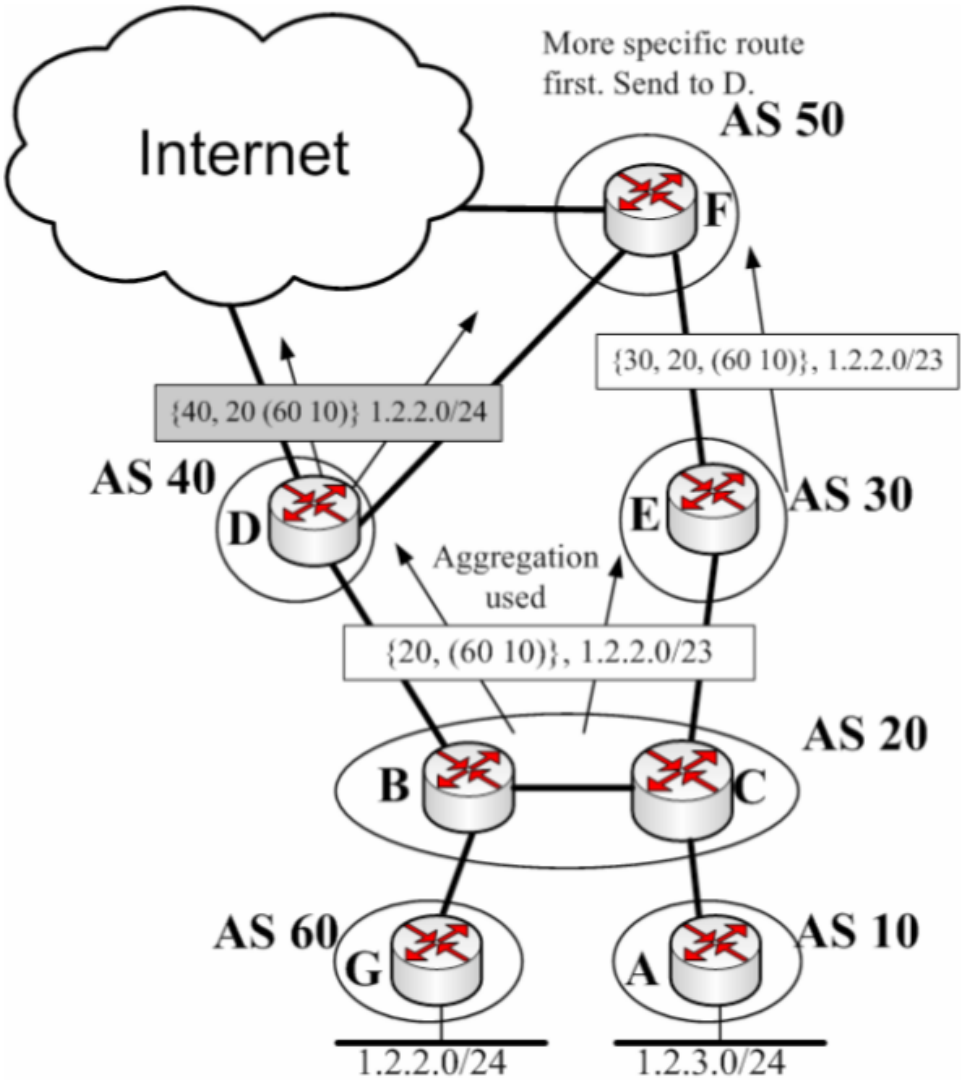
- attaccante *D*
- Fa finta di controllare il prefisso di *A*
- Se *AS* 50 preferisce i path corti, *D* ha successo nella redirezione

Prefix aggregation

Quando piú prefissi condividono un certo numero di bit è conveniente aggregarli

- `10.42.2.0/24` e `10.42.3.0/24` condividono i primi 23 bit
- aggregati in `10.42.2.0/23` (o `10.42.3.0/23`) permettono di accorciare i path
- allo scopo si usa un *AS set*

Prefix De-aggregation



- attaccante D
- $AS\,50$ riceve da $AS\,40$ una rotta piú specifica
- Il traffico passa per D

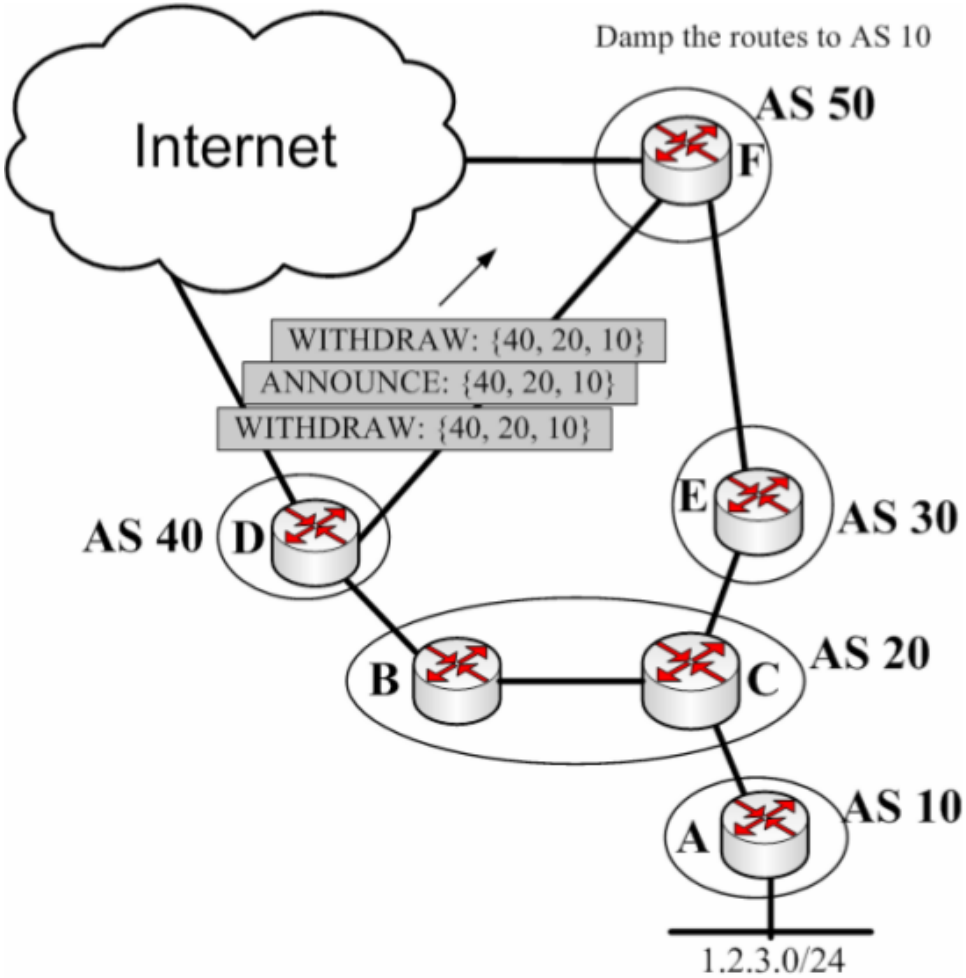
D potrebbe anche attribuirsi il prefisso `1.2.3.0/24`

Route flapping

A livello Internet è perfettamente normale avere una topologia estremamente dinamica: BGP permette di scartare e annunciare nuove rotte con facilità.

- link flapping un link viene disattivato e poi riattivato (normale)
- Se succede spesso però, crea instabilità nella rete perché gli instradamenti sono in continua variazione
- route damping la riattivazione di una rotta viene accettata con tempi crescentemente piú lunghi

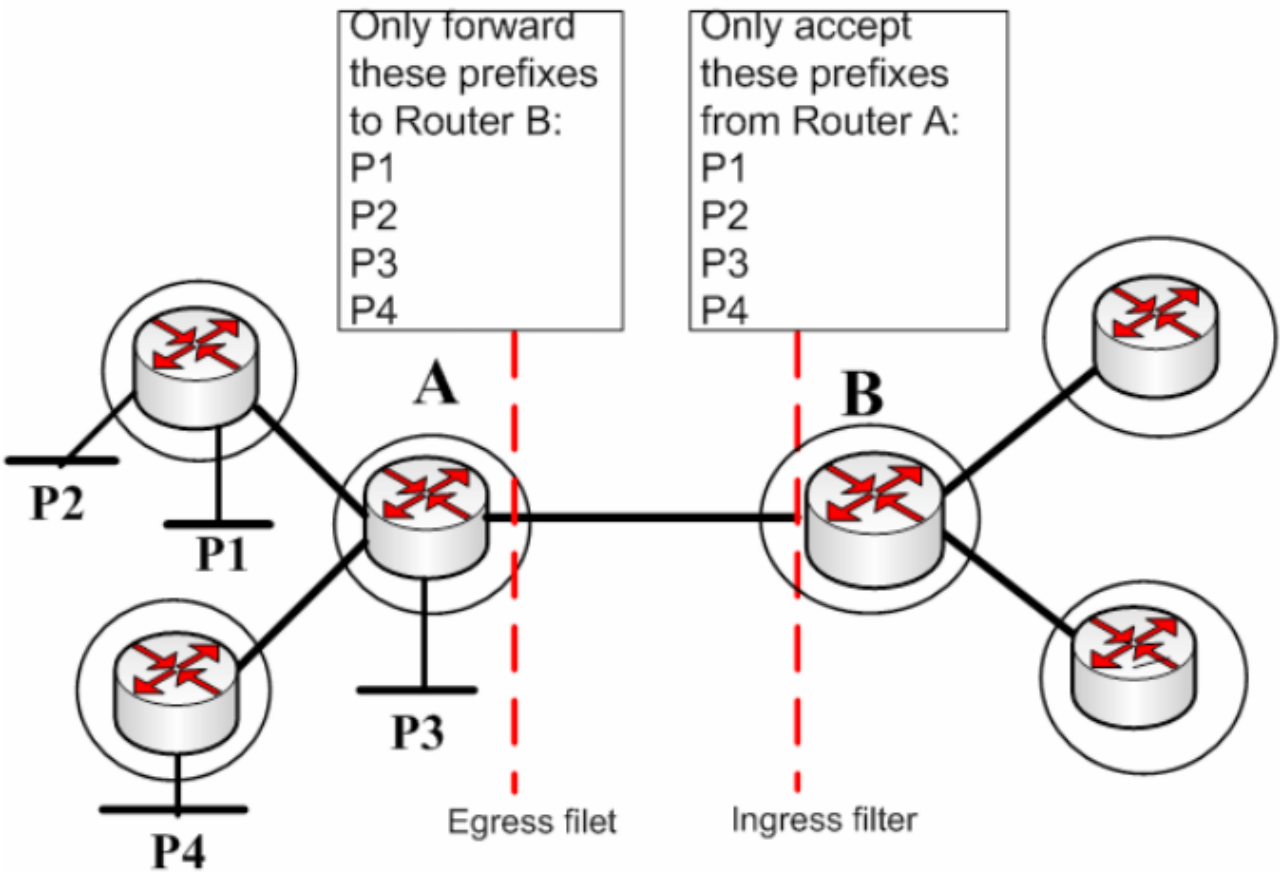
Flapping attack



- attaccante D
- $AS\,50$ si convince che il link è flapping
- $AS\,10$ diventa irraggiungibile da $AS\,50$ a causa del damping

Contromisure

La contromisura piú semplice è l'attivazione di filtri ingress e egress che scartano i path relativi a prefissi "imprevisti" Internet Routing Registry (IRR) (http://www.irr.net)



Versioni sicure di BGP

Ci sono diverse evoluzioni sicure di BGP

- S-BGP: PKI e IPsec
- Secure Origin BGP (Cisco): PKI, nuovi messaggi BGP
- IRV: indipendente dal protocollo (non solo BGP), basta un livello di trasporto sicuro

Riassumendo

Il protocollo BGP senza precauzioni è vulnerabile

- Prefix hijacking
- Prefix de-aggregation
- Flapping attack