Protocolos em Redes de Dados – Crítica 10
João Vicente 44294 Ana Salvado 44299 Inês de Matos 43538

How Secure are Secure Interdomain Routing Protocols?

Desde muito cedo, quando a Internet começou a ganhar relevo, muitos protocolos foram introduzidos e a sua utilização continua a ser bastante presente. Um desses protocolos é o BGP (Border Gateway Protocol), que devido às suas falhas e más configurações começou a levantar problemas relativamente à falta de segurança e às deficiências (já conhecidas) do encaminhamento dos inter-AS (Autonomous Systems). Este protocolo tem sido o utilizado para fazer o encaminhamento entre os sistemas autónomos, como referido, desde 1990 e não teve nenhuma mudança significativa desde essa altura, o que é preocupante, visto que tem havido um grande crescimento da Internet e da sua complexidade. É alarmante também, visto, se apenas más configurações deste protocolo podem provocar um impacto tão grande na Internet, o que um ataque premeditado poderia fazer?

Com este artigo, o que os autores pretendem é descrever e comparar quatro abordagens para melhorar vários aspetos de segurança do encaminhamento entre sistemas autónomos.

Estes sistemas autónomos normalmente são usados para que grandes empresas ou prestadores de serviços consigam ter controlo e autoridade sobre a sua rede. Para estabelecer uma conexão com a Internet, um operador de AS utiliza os chamados *border* ou *gateway routers* que permite a troca de informação entre os AS *border routers* que encaminham o tráfego entre a parte interna dos AS e a Internet, ou servem de intermediários para o tráfego entre outros dois AS's. Os *border routers* estabelecem relações com outros *border routers* através do BGP. Este protocolo oferece suporte para importar e exportar políticas, que, respetivamente, controla que rotas dos nodos BGP são introduzidas numa base de dados de encaminhamento num *router* local e que rotas são anunciadas a esses mesmos nodos BGP. Basicamente, um *router* BGP agarra em todas as rotas que recebe dos seus *routers* BGPs vizinhos, faz uma verificação básica (sendo a mais importante a deteção de ciclos) e depois passa todas as rotas restantes por um processo de decisão que decide se as rotas são novas e/ou melhoras que as existentes.

Como foi referido, eles referem quatro propostas para melhorar a segurança do BGP, sendo elas: autenticação original, soBGP, S-BGP e verificação do plano de dados.

A autenticação original remonta ao problema de saber quem é o proprietário, pois no BGP qualquer AS pode reclamar a posse de qualquer prefixo, o que permite uma grande oportunidade para ataques de roubo de prefixos. É referido que a autenticação é uma precondição fundamental e necessária para qualquer infraestrutura segura de encaminhamento inter-AS, mas insuficiente.

A proposta do soBGP (Secure Origin BGP), diz que existe uma prova de validade de um caminho que teve origem num AS. Neste caso, a validade refere-se a um caminho físico que existe na Internet, a um caminho real que liga dois AS's. Esta validação é garantida através da disseminação da informação da topologia pelos *routers,* anunciando aos outros *routers* os seus nodos, estabelecendo um grafo global da topologia da rede.

O S-BGP oferece uma verificação dos caminhos, apenas permitindo a um AS anunciar um caminho se já lhe tiver sido anunciado esse caminho. Por exemplo, o AS a só pode anunciar a-b-c se o AS b já tiver anunciado ao a, b-c.

Relativamente á verificação do plano de dados, existe uma preocupação sobre o caminho que os dados realmente tomam quando são reencaminhados pelos *routers* BGP, pois um *router* pode anunciar um caminho mas enviar os dados para um diferente.

Este artigo teve por base um outro, em que foram descritos alguns destes métodos de segurança e que serviram para os autores conseguirem fazer esta avaliação das propostas de segurança. Eles puderam concluir que mesmo propostas que parecem seguras e algo sofisticadas podem ainda assim ser contornadas por ataques relativamente simples.