Routing Security Issues, Threats and Attacks

João Guedes, Paulo Sousa, and Renata Teixeira

[1] Universidade do Minho
[2] Braga, Portugal

Resumo Com a grande evolução da Internet nos últimos anos, tanto a nível de número de utilizadores como número de serviços dependentes desta, torna-se necessário garantir a fiabilidade e segurança de todos os dados que circulam nela. Assim, temos de ter em atenção os ataques e as ameaças que colocam em risco a sua segurança. Este trabalho descreve alguns problemas de segurança, mais especificamente ao nível de *routing*, e algumas ameaças e ataques conhecidos e perigosos, incluindo *DoS* e *route hijacking*.

Keywords: *Routing* · *Hijacking* · BGP.

1 Introdução

Cada vez há mais pessoas e mais dispositivos ligados à Internet todos os dias, trazendo consigo algumas questões relativamente à segurança.

O roteamento é fundamental para o funcionamento da Internet. Os seus protocolos direcionam o movimento de pacotes, determinando o caminho que os dados seguem para percorrer várias redes de sua origem até seu destino. O protocolo de roteamento da Internet, *Border Gateway Protocol* (BGP) é conhecido por ser suscetível a erros e ataques, se atacantes conseguirem ter acesso às tabelas de *routing*, pode haver roubos ou manipulação de dados, de identidade, ou até mesmo negação de serviço nas redes. Esses problemas podem literalmente derrubar redes inteiras da Internet ou desviar o tráfego para uma parte não intencional.

2 Problemas de segurança

Todos os dias as pessoas utilizam a Internet, seja para abrir *emails*, transferir dinheiro, navegar nas redes sociais ou até mesmo para abrir o portão da garagem [1]. Desta forma, é fundamental garantir que esses dados não são acedidos por pessoas sem autorização, pois, caso contrário, poderão originar-se todo o tipo de ilegalidades, incluindo roubo de informações ou até mesmo de identidade.

2.1 Problemas de segurança na *IoT*

Hoje em dia, tudo está ligado à internet, sejam televisões, telemóveis, frigoríficos, torradeiras, carros, etc.. Assim sendo, se um destes dispositivos for comprometido, toda a sua rede pode também o ser.

As redes de IOT são propensas a vários ataques como a *Denial of Service* (DoS), *eavesdropping*, *man-in-the-middle* (MITM), *sniffing*, etc. Vários ciber-ataques tornaram-se comuns e mais poderosos, causando perturbações significativas nos sistemas de Internet de alta velocidade. Além disso, alguns dos ataques de rede na IoT são herdados das redes de sensores sem fios (WSNs). Daí a necessidade de proteger as redes IdC de ataques e ameaças imagináveis. Principalmente, encaminhamento seguro no ambiente altamente dinâmico e distribuído da IoT continua a ser um desafio devido à heterogeneidade de dispositivos inteligentes.

2.2 Problemas de segurança no *Border Gatway Protocol* (BGP)

Sendo o protocolo de encaminhamento interdomínio de facto da Internet, o BGP (*Border Gateway Protocol*) é a cola que mantém unidas as partes díspares da Internet. Uma das principais limitações do BGP é a sua incapacidade de abordar adequadamente a segurança. As recentes interrupções e análises de segurança de alto perfil indicam claramente que a infra-estrutura de roteamento da Internet é altamente vulnerável. Além disso, a concepção do BGP e a ubiquidade da sua implantação têm frustrado os esforços do passado para garantir o encaminhamento entre domínios.

3 Ameaças e Ataques

Em [2], é definida uma ameaça como um potencial aproveitamento de uma falha na segurança, do/dos sistemas, que pode causar mal, quando existe uma acção concretizada da maneira correta. Assim, se um router possuir uma falha, um atacante poderá tirar o aproveitamento dela, conseguir acesso não autorizado, e causar danos a toda a rede.

Por isso [3], decidimos distinguir os ataques à integridade, dos ataques à disponibilidade.

3.1 Ameaças e Ataques à integridade

Um ataque à integridade é definido pela possibilidade de explorar falhas num sistema, fazendo alterações aos dados ou trocas de roteamento destes.

Routing Information Manipulation Um ataque *Routing Information Manipulation* consiste em manipular a informação que circula numa rede, através de um acesso não autorizado a um nodo, pondo em causa as decisões de encaminhamento tomadas na rede. Deste modo, a rede pode ficar num estado não ótimo, em que as rotas não são as mais eficientes, ou até num estado fracionado, em que apenas parte da rede está funcional. Além disso, uma rede não ótima pode-se tornar demasiado congestionada, levando até a uma falha do serviço.

Node Identity Misappropriation Um ataque *Node Identity Misappropriation* consiste em falsificar a identidade de um nodo, que pode causar a criação de rotas incorretas, criando uma topologia errada. Não existindo forma de garantir que a informação que circula na rede é válida e que os nodos participantes na topologia são verdadeiros, toda a rede pode estar comprometida.

3.2 Ameaças e Ataques à disponibilidade

Quando um atacante ganha acesso a uma network, mesmo que não modifique qualquer data, pode ainda assim monitorizar e roubar informação sensível, podendo não deixar qualquer rastro nem alterações na performance da rede. É aqui que podem ocorrer alguns dos ataques mais perigosos pois, se rastro é deixado, os defensores não têm razões para acharem que a rede foi comprometida.

***Denial of Service* (DoS)** Um ataque de *Denial of Service* a nível do BGP, consiste em manipular a tabela de *routing*, de forma a prevenir que o tráfego que sai da rede não chegue ao seu destino de forma aos utilizadores não conseguirem ter acesso à internet.

Route hijacking Este ataque é conhecido por ser um dos mais perigosos pois, o atacante, poderá manipular as rotas, de modo a que todo o tráfego passe por ele e continue a chegar ao destino. Isto implica que os utilizadores dessa rede nunca se irão aperceber que algo se está a passar, pois para eles, tudo estará a correr bem. Porém, perante esta situação, o(s) atacante(s) poderão fazer tudo o que quiserem com a informação.

4 Conclusão

A realização deste projeto possibilitou ao grupo explorar *routing* e os seus problemas de segurança, e ataques e ameaças que este pode sofrer. O roteamento é fundamental para o funcionamento da Internet. Se atacantes conseguirem ter acesso às tabelas de *routing*, pode haver roubos ou manipulação de dados, de identidade, ou até mesmo negação de serviço nas redes. Esses problemas podem literalmente derrubar redes inteiras da Internet ou desviar o tráfego.

Foi possível perceber que há problemas de segurança relacionados com a Internet das Coisas, pois estas são propícias a ataques comp DoS, MITM, etc. O encaminhamento seguro no ambiente altamente dinâmico e distribuído da IoT continua a ser um desafio devido à heterogeneidade de dispositivos inteligentes. Há também problemas no protocolo BGP sendo altamente vulnerável a ataques.

Estudamos, então, também as ameaças e ataques ao *routing*, tendo as dividido entre ameaças à integridade e à disponibilidade, aprofundando um pouco ataques como o *Routing Information Manipulation*, *Node Identity Misappropriation*, *Denial of Service* e *Route hijacking*.

Referências

1. Security issues, threats, and attacks - Pratical Network Scanning, https://subscription.packtpub.com/book/networking_and_servers/9781788839235/1/ch01lvl1sec15/security-issues-threats-and-attacks. Last accessed 2 Mar 2022
2. A. Barbir, S. Murphy, Y. Yang, "Generic Threats to Routing Protocols". 4 (2006)
3. T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, M. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)". 16–20 (2015)