# ABSTRAK

*Internet* saat ini merupakan sebuah jaringan komputer besar yang terdiri atas banyak A*utonomous System* (*AS*). *Border Gateway Protocol (BGP)* adalah protokol yang digunakan oleh semua *AS* agar dapat saling terhubung dan bertukar informasi. *BGP* sendiri berjalan diatas prinsip saling percaya dimana setiap *AS* diharapkan hanya melakukan *advertise prefix* yang dikelolanya saja. Prinsip ini sendiri kemudian menjadi sebuah celah yang menjadikan *BGP* rentan terhadap berbagai insiden seperti *BGP route leak* dan *BGP hijacking* dimana sebuah *AS* melakukan *advertise prefix* yang tidak dikelolanya. Insiden ini menyebabkan *traffic* data berjalan menuju tujuan yang tidak sebagaimana mestinya dan menjadi sebuah permasalahan keamanan.

Salah satu cara yang dikembangkan untuk menanggulangi permasalahan ini adalah *Resource Public Key Infrastructure* (*RPKI*). *RPKI* merupakan sebuah *public key infrastructure* yang memungkinkan pengelola *internet number resource* atau IP *public* untuk membuat sebuah statemen mengenai *AS* mana yang memiliki otorisasi untuk melakukan *advertise prefix* yang dikelolanya. *RPKI* dapat digunakan sebagai dasar untuk implementasi *Route Origin Validation* (*ROV*) sehingga *router* dapat melakukan *filtering routing prefix* yang diterimanya dan memblokir *routing prefix* yang tidak valid. Penelitian ini mensimulasikan implementasi *ROV* menggunakan *RPKI* menggunakan simulator jaringan *PNETLab* dengan menjalankan topologi yang terdiri dari tiga *AS*, lima *router* berbasis sistem operasi VyOS dan dua *server RPKI validator*.

Berdasarkan pengujian yang dilakukan didapatkan hasil bahwa implementasi *route origin validation* menggunakan RPKI dapat meminimalisir dampak dari insiden *BGP* yang terjadi dengan melakukan blokir terhadap *routing prefix* yang di-*advertise* oleh *AS* yang tidak memiliki otoritas. Salah satu yang menjadi faktor penentu keberhasil *route origin validation* menggunakan *RPKI* ini adalah tingkat adopsi *ROA*, semakin tinggi tingkat adopsi *ROA* akan mengurangi dampak dari insiden *BGP*.

*Kata Kunci : BGP, RPKI, Route Origin Validation, Autonomous System, ROA*

## *ABSTRACT*

*The Internet today is an extensive computer network consisting of many Autonomous Systems (AS). Border Gateway Protocol (BGP) is the protocol used by all ASs to be able to connect and exchange information. BGP itself runs on the principle of mutual trust, where each AS is expected only to advertise the prefix it manages. This principle becomes a loophole that makes BGP vulnerable to various incidents, such as BGP route leaks and BGP hijacking, where an AS advertises a prefix it does not manage. This incident caused data traffic to go to an inappropriate destination and became a security problem.*

*One way developed to overcome this problem is the Resource Public Key Infrastructure (RPKI). RPKI is a public key infrastructure that allows managers of internet number resources or public IPs to state which AS is authorised to advertise the prefix they manage. RPKI can be used as a basis for implementing Route Origin Validation (ROV), so routers can filter the routing prefixes they receive and block invalid routing prefixes. RPKI can be used as a basis for implementing Route Origin Validation (ROV), so routers can filter the routing prefixes they receive and block invalid routing prefixes.*

*Based on the tests carried out, it was found that implementing route origin validation using RPKI can minimize the impact of BGP incidents that occur by blocking the routing prefix advertised by an AS that does not have the authority. One of the success factor for route origin validation using RPKI is the adoption rate of ROA, higher ROA adoption rate will decrease the impact of BGP incident.*



***Keywords**: BGP, RPKI, Route Origin Validation, Autonomous System, ROA*