

Pemodelan Risiko dan Upaya Mitigasi Serangan Route Hijacking Terhadap Sistem Informasi Akademik Kampus Dengan RPKI

Risk Modeling and Mitigation Efforts for Route Hijacking Attacks on a Campus Academic Information System Using RPKI

Raja Hafiza Ramanda Putra^{a,1}, Linna Oktaviana Sari^{b,2}

^{a,b}Program Studi S1 Teknik Informatika, Universitas Riau, Pekanbaru, Jl. H. R. Soebrantas, Km.12,5, 2829, Indonesia

raja.hafiza5965@student.unri.ac.id¹, linnaoasari@lecturer.unri.ac.id²

ABSTRAK

Serangan route hijacking pada Border Gateway Protocol (BGP) merupakan ancaman serius bagi keandalan layanan Sistem Informasi Akademik Kampus. Salah satu bentuknya adalah route origin change, yaitu ketika Autonomous System (AS) tidak sah mengumumkan prefiks IP milik pihak lain. Penelitian ini bertujuan memodelkan risiko dan menganalisis dampaknya terhadap ketersediaan layanan. Metode yang digunakan adalah pemodelan topologi routing yang mencakup router internal, transit, eksternal, dan penyerang dalam lingkungan terkontrol. Kontribusi utama penelitian ini adalah pengembangan skenario pemodelan serangan yang merepresentasikan kondisi nyata layanan akademik serta evaluasi efektivitas mitigasi berbasis RPKI secara eksperimental. Hasil menunjukkan bahwa prefiks dari AS tidak sah dapat diterima dan menggantikan rute valid karena tidak adanya validasi asal rute, sehingga lalu lintas dialihkan ke jalur yang salah. Hal ini berisiko menyebabkan pengalihan akses, pencurian kredensial, dan penurunan keandalan layanan. Mitigasi menggunakan Resource Public Key Infrastructure (RPKI) melalui ROA dan ROV terbukti mampu menolak rute tidak valid dan menjaga lalu lintas tetap pada jalur yang sah.

Kata Kunci : Border Gateway Protocol (BGP), Route Hijacking, Route Origin Change, Resource Public Key Infrastructure (RPKI), Route Origin Authorization (ROA), Route Origin Validation (ROV), Keamanan Jaringan, Sistem Informasi Akademik.

ABSTRACT

Route hijacking attacks on the Border Gateway Protocol (BGP) pose a serious threat to the reliability of Academic Information System services. One common form is route origin change, where an unauthorized Autonomous System (AS) announces IP prefixes belonging to another party. This study aims to model the risk and analyze its impact on service availability. The method involves routing topology modeling that includes internal, transit, external, and attacker routers within a controlled environment. The main contribution of this study is the development of an attack modeling scenario that represents real-world academic service conditions, along with an experimental evaluation of RPKI-based mitigation effectiveness. The results show that prefixes from unauthorized ASes can be accepted and replace valid routes due to the absence of route origin validation, causing traffic to be redirected to incorrect paths. This condition may lead to traffic hijacking, credential theft, and reduced service reliability. Mitigation using Resource Public Key Infrastructure (RPKI) through ROA and ROV is proven effective in rejecting invalid routes and maintaining traffic on legitimate paths.

Keywords : Border Gateway Protocol (BGP), Route Hijacking, Route Origin Change, Resource Public Key Infrastructure (RPKI), Route Origin Authorization (ROA), Route Origin Validation (ROV), Network Security, Academic Information System.

Disubmit:

Info Artikel :
Direview:

Diterima :

Copyright © 2026 – CSRID Journal. All rights reserved.

1. PENDAHULUAN

Keamanan jaringan komputer merupakan pilar fundamental dalam penyelenggaraan layanan digital modern guna memastikan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data [29], [30]. Seiring meningkatnya ketergantungan institusi pendidikan tinggi pada layanan berbasis jaringan, ancaman terhadap infrastruktur komunikasi juga berkembang semakin kompleks. Laporan keamanan siber global menunjukkan adanya peningkatan signifikan terhadap intensitas serangan siber dalam beberapa tahun terakhir, baik secara global maupun nasional [8], [9]. Fenomena ini menuntut penguatan keamanan tidak hanya pada lapisan aplikasi, tetapi juga pada lapisan infrastruktur routing internet.

Salah satu ancaman paling signifikan pada lapisan routing adalah route hijacking. Insiden ini terjadi ketika sebuah *Autonomous System* (AS) mengumumkan prefiks IP yang bukan miliknya melalui *Border Gateway Protocol* (BGP), sehingga trafik internet salah diarahkan ke jaringan penyerang [1], [7]. Dampak dari route hijacking sangat destruktif, mulai dari penyadapan data sensitif, manipulasi trafik melalui serangan man-in-the-middle, hingga pemutusan layanan secara total (*blackholing*) [10], [11]. Data pengamatan global juga menunjukkan bahwa insiden pembajakan rute masih sering terjadi dan menjadi ancaman nyata bagi stabilitas internet [4], [5], sehingga tanpa mekanisme autentikasi bawaan pada BGP, infrastruktur internet tetap berada dalam risiko tinggi [2].

Di lingkup akademis, Sistem Informasi Akademik (SIKAD) pada salah satu perguruan tinggi negeri di Indonesia menjadi tulang punggung pelayanan data mahasiswa, dosen, dan tenaga kependidikan. Sistem ini mengelola informasi sensitif seperti Kartu Rencana Studi (KRS), Transkrip Nilai, serta identitas pribadi yang mencakup NIM dan tanggal lahir. Saat ini, SIKAD tersebut telah mengimplementasikan lapisan keamanan ganda, yakni di sisi aplikasi menggunakan kerangka kerja (*framework*) serta di sisi pengiriman konten menggunakan layanan Content Delivery Network (CDN) untuk mitigasi serangan dan optimasi performa [29].

Namun, terdapat celah keamanan krusial yang belum teratasi sepenuhnya. Penggunaan CDN dan keamanan tingkat aplikasi tidak cukup kuat untuk mencegah serangan pada lapisan routing. Hal ini dikarenakan serangan route hijacking terjadi pada mekanisme pertukaran rute antar AS yang berada di luar kendali langsung aplikasi maupun penyedia CDN. Berbagai studi menunjukkan bahwa insiden route leak dan anomali BGP dapat berdampak luas terhadap layanan global [18], [20]. Jika anomali BGP menargetkan infrastruktur yang menaungi SIKAD, maka seluruh data sensitif sivitas akademika berisiko terintersepsi sebelum mencapai server tujuan yang sah.

Sebagai langkah mitigasi, komunitas internet global mendorong adopsi Resource Public Key Infrastructure (RPKI) melalui mekanisme Route Origin Authorization (ROA) [3], [6]. Berbagai penelitian menunjukkan bahwa implementasi RPKI mampu meningkatkan keamanan routing dengan memvalidasi asal prefiks serta mengurangi kemungkinan diterimanya rute ilegal [13], [16]. Meskipun demikian, tantangan dalam implementasi serta tingkat adopsi yang belum merata masih menjadi perhatian dalam pengamanan infrastruktur jaringan [14], [18].

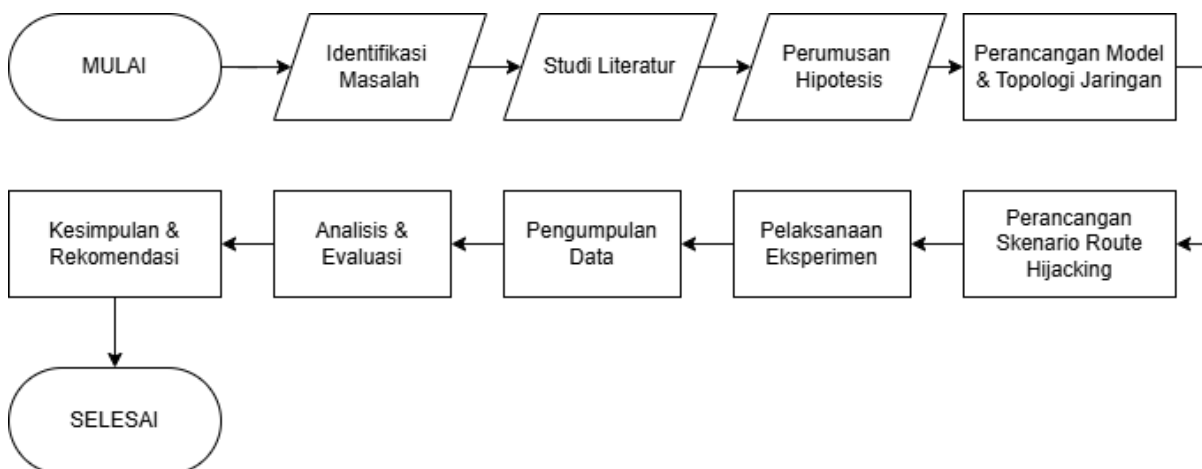
Berdasarkan latar belakang tersebut, penelitian ini berfokus pada evaluasi tingkat kerentanan infrastruktur jaringan Sistem Informasi Akademik terhadap ancaman route hijacking. Melalui pendekatan analisis BGP, pemanfaatan data publik, serta kajian mitigasi berbasis teknologi RPKI dan prefix filtering, penelitian ini diharapkan dapat memberikan kontribusi dalam merumuskan strategi keamanan jaringan yang komprehensif bagi institusi pendidikan tinggi serta meningkatkan ketahanan terhadap ancaman pada lapisan routing internet [7], [19].

Penelitian ini memiliki kebaruan pada pendekatan pemodelan risiko serangan *route hijacking* yang difokuskan pada skenario *route origin change* serta analisis dampaknya terhadap potensi *credential harvesting* pada layanan Sistem Informasi Akademik. Berbeda dengan penelitian terdahulu yang umumnya hanya berfokus pada deteksi atau mitigasi serangan BGP secara umum [7], [12], penelitian ini

mengintegrasikan analisis risiko berbasis CIA Triad dengan pemodelan topologi jaringan yang merepresentasikan kondisi nyata layanan akademik. Selain itu, penelitian ini juga melakukan evaluasi terhadap penerapan Resource Public Key Infrastructure (RPKI) secara langsung dalam skenario serangan terkontrol [13], [16], sehingga menghasilkan kontribusi berupa pendekatan komprehensif yang menggabungkan aspek keamanan routing dan perlindungan data pengguna. Pendekatan ini melengkapi studi sebelumnya yang lebih menitikberatkan pada analisis global atau implementasi parsial tanpa mempertimbangkan keterkaitan langsung dengan risiko keamanan informasi pengguna [14], [18].

1. METODE

Penelitian ini menerapkan pendekatan eksperimental laboratoris dengan melakukan pemodelan serangan dalam lingkungan yang terkontrol. Metode ini dipilih untuk mengevaluasi kerentanan infrastruktur routing pada Sistem Informasi Akademik (SIKAD) tanpa mengganggu stabilitas operasional layanan yang sedang berjalan. Fokus utama eksperimen ini adalah menguji ketahanan protokol routing terhadap ancaman route hijacking dengan meninjau validitas prefix IP dan efektivitas mekanisme Resource Public Key Infrastructure (RPKI). Rangkaian proses penelitian ini divisualisasikan pada Gambar 1 berikut.



Gambar 1. Flowchart Alur Penelitian

A. Penelitian Terkait

Dalam lima tahun terakhir, insiden *route hijacking* masih kerap terjadi dan memberikan dampak besar terhadap kestabilan internet global. Pada April 2021, Vodafone Idea (AS55410) melakukan kesalahan pengumuman lebih dari 30.000 prefix yang bukan miliknya sehingga menimbulkan gangguan routing berskala besar. Beberapa bulan kemudian, pada Oktober 2021, AS212046 (MEZON) juga tercatat melakukan mis-origin ribuan prefix yang mengacaukan lalu lintas di berbagai negara. Kasus-kasus ini menunjukkan bahwa permasalahan pengumuman prefix yang salah masih menjadi salah satu kerentanan serius dalam protokol Border Gateway Protocol (BGP).

Memasuki tahun 2022, *route hijacking* tidak hanya menyebabkan gangguan teknis, tetapi juga digunakan sebagai sarana kejahatan siber. Pada Februari 2022, layanan KLAYswap di Korea Selatan mengalami kerugian sekitar 1,9 juta dolar akibat manipulasi routing yang memungkinkan penyerang menyisipkan kode berbahaya melalui pengumuman BGP palsu. Selanjutnya pada Maret 2022, RTComm (AS8342) mengumumkan prefix milik *Twitter* (104.244.42.0/24) yang membuat trafik pengguna salah rute selama sekitar 45 menit, meskipun propagasinya terbatas karena penerapan *Resource Public Key Infrastructure* (RPKI). Selain itu, pada periode konflik geopolitik Ukraina–Rusia, berbagai laporan juga menunjukkan adanya anomali routing dan indikasi *hijack* terhadap layanan kritis.

Lebih baru, insiden *route leak* yang terjadi pada Juni 2024 memengaruhi layanan 1.1.1.1 milik Cloudflare. Dalam kasus ini, sebagian pengguna kehilangan akses atau mengalami latensi tinggi akibat pengumuman prefix yang salah. Rangkaian kasus tersebut menegaskan bahwa *route hijacking* masih menjadi ancaman nyata, baik untuk tujuan kriminal maupun politik. Oleh karena itu, penelitian mengenai mekanisme mitigasi, khususnya melalui pemanfaatan RPKI sebagai lapisan validasi routing, sangat relevan dilakukan guna memperkuat keamanan infrastruktur jaringan internet.

Berbagai penelitian dalam lima tahun terakhir menunjukkan bahwa meskipun BGP telah lama menjadi tulang punggung *routing* internet, kerentanan terhadap hijack maupun *route leak* masih sering terjadi. Tabel 1 berikut merangkum beberapa penelitian yang relevan untuk menjadi acuan dalam menentukan arah penelitian ini.

Tabel 1. Penelitian Terkait

No	Peneliti (Tahun)	Judul (Metode)	Masalah	Hasil	Perbedaan
1	Jaw, Müller, Hesselman, Nieuwenhuis (2024)	<i>Serial BGP Hijackers: A Reproducibility Study and Assessment of Current Dynamics</i> (Analisis data empiris & reproducibility study)	Hijack berulang oleh AS tertentu sulit dideteksi dan terus muncul dalam data global	Ditemukan pola hijack berulang dan perlunya deteksi historis otomatis	Penelitian ini berfokus pada kerentanan layanan akademis SIA dan mitigasi pada lingkungan kampus
2	Li, Li, Chung (2025)	<i>ImpROV: Measurement and Practical Mitigation of Collateral Damage in RPKI ROV</i> (Eksperimen pengukuran & sistem mitigasi)	ROV menimbulkan collateral damage meskipun prefiks valid	ImpROV menurunkan kesalahan validasi hingga 70% tanpa mengganggu konektivitas	Penelitian ini menggunakan RPKI standar sebagai mitigasi praktis di lingkungan universitas
3	Holterbach et al. (2024)	<i>A System to Detect Forged-Origin BGP Hijacks</i> (Pengembangan sistem deteksi)	Hijack dengan origin palsu dapat lolos meskipun RPKI diterapkan	Deteksi forged-origin melalui korelasi AS-path	Penelitian ini tidak mengembangkan sistem deteksi global, tetapi menganalisis risiko dan mitigasi lokal
4	Mirdita, Schulmann, Waidner (2024)	<i>SoK: An Introspective Analysis of RPKI Security</i> (Systematization of Knowledge)	RPKI memiliki kelemahan operasional dan risiko misconfiguration	Ditekankan perlunya audit dan pemantauan otomatis	Penelitian ini berfokus pada penerapan RPKI sebagai proteksi layanan akademis
5	Hlaváček, Jeitner, Mirdita, Schulmann, Waidner (2022)	<i>Stalloris: RPKI Downgrade Attack</i> (Eksperimen keamanan & attack modeling)	Serangan downgrade dapat menonaktifkan fungsi RPKI	Disarankan redundansi dan pemantauan ROA	Penelitian ini menggunakan RPKI sebagai mitigasi, bukan mengkaji serangan downgrade
6	Scott et al. (2024)	<i>A Survey of Advanced BGP Attack Detection Techniques</i> (Studi literatur / survei 178 metode)	Banyak teknik deteksi belum efektif terhadap serangan canggih	ML efektif tetapi belum efisien real-time	Penelitian ini fokus pada satu pemodelan hijacking pada domain SIA
7	(Anon / arXiv) (2025)	<i>A New Efficient RPKI Design (iRPKI)</i> (Proposal desain arsitektur)	RPKI tradisional lambat dan overhead tinggi	iRPKI meningkatkan efisiensi validasi	Penelitian ini tidak mengembangkan protokol baru
8	Testart, Wolff, Gouda,	<i>Identifying Current Barriers in RPKI</i>	Adopsi RPKI masih rendah secara global	Hambatan teknis dan organisasi	Penelitian ini menganalisis mitigasi pada lingkup jurusan

	Fontugne (2024)	<i>Adoption</i> (Studi empiris & wawancara)		menjadi faktor utama	
9	Höger et al. (2025)	<i>Mitigating BGP Route Leaks With Attributes and Communities</i> (Analisis protokol & Pemodelan)	Route leak sulit dibedakan dari hijack	Community routing menurunkan kasus route leak	Penelitian ini fokus pada route origin hijacking
10	Rodday, Cunha, Bush, Katz-Bassett, Wählich (2023–2024)	<i>The RPKI: A Survey on Measurements and Future Prospects</i> (Survei & meta-analisis)	Kurangnya pemetaan kekuatan dan keterbatasan RPKI	Adopsi global RPKI sekitar 40%	Penelitian ini mengkaji kasus lokal SIA
11	Hasan Albana (2025)	<i>Implementasi BGP Menggunakan Cisco Packet Tracer pada Jaringan PT Artha Media Lintas Nusa</i> (Pemodelan)	Implementasi BGP belum dipahami secara praktis	Pemodelan membantu pemahaman routing BGP	Tidak membahas aspek keamanan dan serangan BGP
12	Nanda Iryani, Jafaruddin G. A. Ginting, Dyas Dendi Andika (2022)	<i>Analisis Performansi BGP Resource Public Key Infrastructure</i> (Pengukuran performa)	Dampak RPKI terhadap performa jaringan	RPKI memengaruhi latensi dan CPU router	Fokus performa, bukan Pemodelan serangan
13	Valen Brata Pranaya, Theophilus Wellem (2020)	<i>Implementasi BGP dan RPKI menggunakan BIRD</i> (Implementasi sistem)	Kerentanan BGP terhadap hijacking	Integrasi BIRD dan RPKI validasi origin	Penelitian ini fokus pada layanan akademis
14	Tri Budi Rahayu, Imam Suharjo (2024)	<i>Implementasi BGP dengan RPKI pada MikroTik RouterOS</i> (Studi kasus)	Tidak adanya validasi asal rute	RPKI meningkatkan keabsahan routing	Fokus lingkungan perusahaan
15	Oscar Wong (2024)	<i>Classifying and Identifying BGP Hijacking Attacks on the Internet</i> (Klasifikasi serangan)	Kurangnya taksonomi hijacking	Klasifikasi jenis serangan hijacking	Penelitian ini menerapkan satu jenis hijack pada model SIA
16	Sandro Lutz (2023)	<i>Towards a Full Implementation of RPKI in the Mini-Internet</i> (Thesis / Pemodelan mini-Internet)	Implementasi RPKI belum menyeluruh	RPKI end-to-end pada mini-Internet	Penelitian ini fokus layanan akademis nyata

Berdasarkan literatur yang ditinjau, terlihat bahwa isu keamanan BGP masih menjadi tantangan serius hingga saat ini. Upaya mitigasi melalui RPKI telah menunjukkan kemajuan, namun tetap menghadapi keterbatasan baik dari sisi teknis, operasional, maupun adopsi global. Perbedaan pendekatan dalam penelitian-penelitian sebelumnya menunjukkan adanya ruang untuk kontribusi lebih lanjut, khususnya pada konteks penerapan mitigasi yang adaptif dan sesuai dengan kondisi infrastruktur jaringan yang ada. Oleh karena itu, penelitian ini berfokus pada pemanfaatan RPKI sebagai mekanisme validasi *routing* untuk memperkuat keamanan jaringan terhadap ancaman *route hijacking*.

B. Pemodelan Topologi

Perancangan topologi jaringan pada penelitian ini bertujuan untuk merepresentasikan kondisi operasional layanan Sistem Informasi Akademik Kampus dalam lingkungan pemodelan. Topologi yang dibangun mengadopsi konsep interkoneksi antar *Autonomous System* (AS) berbasis protokol *Border Gateway Protocol* (BGP), di mana sistem akademik dimodelkan sebagai AS *legitimate* yang

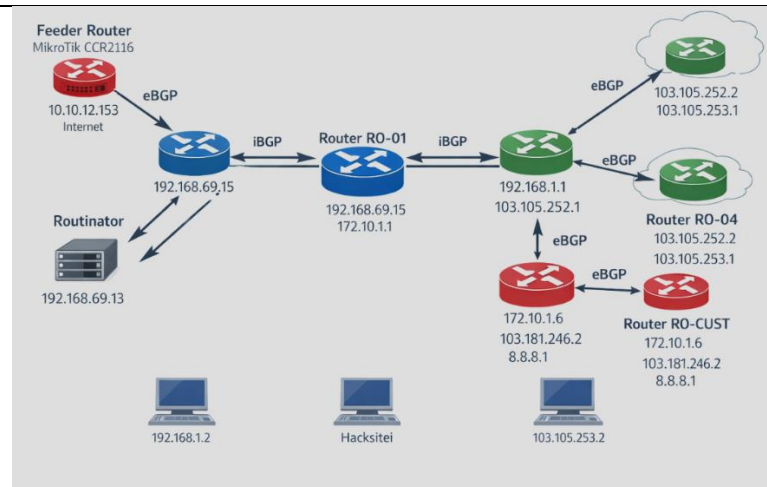
mengiklankan prefiks jaringan resminya. Selain itu, terdapat beberapa entitas AS lain yang berperan sebagai upstream provider serta satu AS *attacker* yang digunakan untuk mensimulasikan skenario serangan *route hijacking*. Perancangan ini dimaksudkan untuk menghasilkan lingkungan pemodelan yang mampu merepresentasikan proses distribusi rute secara realistis, baik pada kondisi normal maupun saat terjadi gangguan keamanan.

Dalam topologi tersebut juga diintegrasikan mekanisme *Resource Public Key Infrastructure* (RPKI) sebagai sistem validasi terhadap keaslian prefiks yang diumumkan. Implementasi RPKI dilakukan melalui komponen *validator* yang memberikan status valid, invalid, atau not found terhadap setiap rute yang diterima oleh *router*. Integrasi ini memungkinkan model tidak hanya digunakan untuk mensimulasikan serangan, tetapi juga untuk mengevaluasi efektivitas mekanisme mitigasi yang diterapkan. Struktur topologi dan relasi antar entitas dirancang secara sistematis guna mempermudah proses observasi terhadap perubahan jalur routing serta dampak yang ditimbulkan, baik oleh serangan maupun oleh mekanisme pengamanan. Berikut adalah Tabel 2 yang menjelaskan perangkat dan perannya dalam topologi serta kontribusinya terhadap pembentukan dan validasi tabel routing.

Tabel 2. Skema table routing dan perannya

No	Perangkat	Jenis	OS / Versi	Interface	Fungsi dalam SIA
1	Feeder Router	MikroTik CCR2116-12G-4S+	RouterOS	SSTP-1	Router border utama SIA, penghubung ke Internet
2	Routinator	Virtual Machine	Linux + Routinator	Eth0	Validator RPKI (ROA & Route Origin Validation)
3	Router RO-01	MikroTik CHR	RouterOS v7.11.2	Ether1	Router inti SIA koneksi ke Routinator
4	Router RO-02	MikroTik CHR	RouterOS v6.49.13	Ether2	iBGP internal SIA
				Ether1	Router transit / ISP Pemodelan
				Ether2	eBGP ke AS lain
				Ether3	Koneksi antar router
5	Router RO-03	MikroTik CHR	RouterOS v7.11.2	Ether4	Koneksi ke feeder
				Ether1	Edge router SIA
				Ether2	Pengumuman prefix SIA
6	Router RO-04	MikroTik CHR	RouterOS v7.11.2	Ether1	AS eksternal (Internet Pemodelan)
				Ether2	Distribusi rute ke user
				Ether1	Router penyerang (route hijacking)
7	Router RO-CUST	MikroTik CHR	RouterOS v6.49.13	Ether2	Prefix palsu
				Ether3	Arah ke fake service
				Ether0	User internal SIA
8	PC-01	Virtual PC	–	Eth0	User internal SIA
9	PC-02	Virtual PC	–	Eth0	User eksternal
10	Attacker	Virtual PC	–	Eth0	Target palsu hasil hijacking

Selanjutnya, dilakukan pengembangan model topologi jaringan secara lebih rinci dan terstruktur. Tahap ini mencakup penyempurnaan konfigurasi antar AS, penentuan skema distribusi prefiks, serta implementasi mekanisme validasi RPKI pada setiap node jaringan. Dengan demikian, model yang dihasilkan dapat digunakan sebagai dasar dalam pelaksanaan eksperimen serta analisis risiko secara komprehensif dan terukur. Gambaran dari rancangan topologi jaringan tersebut disajikan pada Gambar 2, yang memperlihatkan hubungan antar AS, alur distribusi prefiks, serta posisi implementasi mekanisme RPKI dalam sistem.



Gambar 2. Topologi Jaringan

Berdasarkan perancangan dan pengembangan topologi jaringan yang telah dilakukan, model yang dihasilkan telah mampu merepresentasikan kondisi operasional jaringan secara terstruktur, baik dalam skenario normal maupun saat terjadi serangan route hijacking. Keberadaan komponen RPKI dalam topologi juga memberikan landasan untuk mengevaluasi efektivitas mekanisme mitigasi terhadap ancaman perubahan asal rute. Dengan tersedianya lingkungan pemodelan yang representatif dan terkontrol, tahap selanjutnya dalam penelitian ini difokuskan pada pemodelan risiko untuk mengidentifikasi, menganalisis, dan mengevaluasi tingkat risiko yang ditimbulkan oleh serangan route origin change terhadap layanan Sistem Informasi Akademik Kampus, sehingga dapat dirumuskan strategi mitigasi yang tepat dan terukur.

C. Pemodelan Risiko

Pada tahap ini, pemodelan risiko pada serangan route hijacking adalah route origin change. Serangan ini terjadi ketika Autonomous System (AS) penyerang mengiklankan prefiks jaringan milik sistem yang sah dengan memanipulasi informasi origin ASN, sehingga seolah-olah rute tersebut berasal dari sumber yang valid. Kondisi ini memanfaatkan kelemahan mendasar pada Border Gateway Protocol (BGP) yang tidak memiliki mekanisme autentikasi terhadap sumber pengumuman rute. Akibatnya, setiap AS berpotensi mengiklankan prefiks tertentu tanpa proses verifikasi keabsahan, sehingga memungkinkan penyisipan informasi routing palsu ke dalam jaringan.

Dalam skenario yang dimodelkan, rute palsu yang diumumkan oleh AS penyerang berpotensi dipilih sebagai jalur terbaik apabila memiliki atribut yang lebih menguntungkan, seperti panjang AS path yang lebih pendek atau preferensi kebijakan routing tertentu. Pemilihan rute tersebut menyebabkan lalu lintas pengguna yang sebelumnya menuju sistem yang sah dialihkan ke jaringan penyerang. Dampak dari kondisi ini tidak hanya terbatas pada penurunan ketersediaan layanan, tetapi juga membuka peluang terjadinya serangan lanjutan seperti credential harvesting, di mana penyerang dapat melakukan penyadapan atau manipulasi terhadap data autentikasi pengguna yang melewati jalur yang telah dikompromikan.

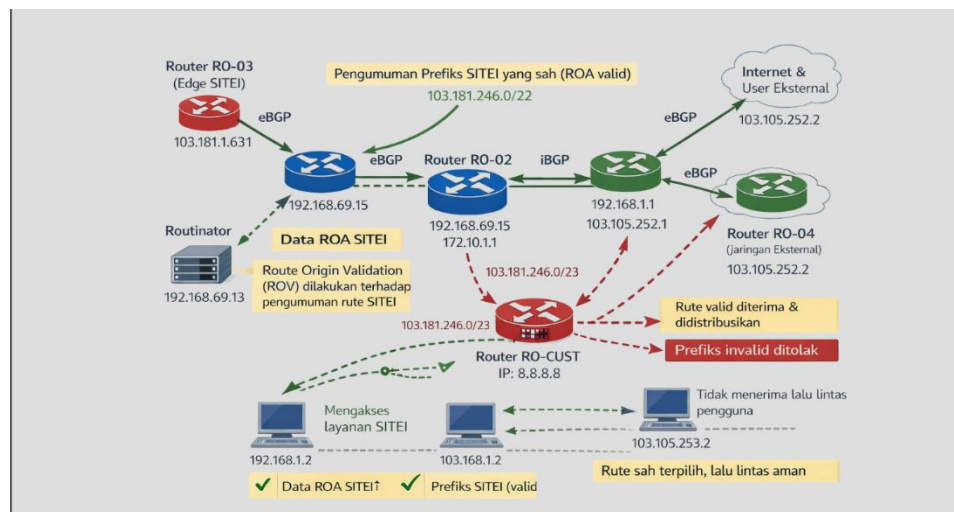
Dengan demikian, pemodelan pada tahap ini tidak hanya berfokus pada mekanisme terjadinya route origin change, tetapi juga pada identifikasi dan analisis risiko yang ditimbulkan terhadap keamanan informasi pengguna. Untuk memperjelas alur serangan dan dampaknya terhadap proses routing, ilustrasi skenario pengalihan rute dalam lingkungan pemodelan disajikan pada Gambar 3 sebagai dasar untuk analisis risiko pada tahap selanjutnya.

Gambar 3. Pemodelan Risiko terhadap Topologi Jaringan

D. Pemodelan Mitigasi Dengan RPKI

Dalam skenario pemodelan ini, ketika AS penyerang mencoba mengumumkan prefiks milik sistem yang sah dengan ASN yang tidak sesuai, rute tersebut akan teridentifikasi sebagai invalid. Router yang telah menerapkan kebijakan Route Origin Validation (ROV) akan menolak rute tersebut dan tidak memasukkannya ke dalam tabel routing. Dengan demikian, hanya rute yang memiliki status valid yang akan diproses dan digunakan sebagai jalur utama dalam pengiriman trafik. Kondisi ini memastikan bahwa lalu lintas pengguna tetap diarahkan ke sistem yang sah, sehingga serangan route hijacking tidak berhasil mengalihkan jalur komunikasi maupun membuka peluang terjadinya serangan lanjutan seperti *credential harvesting*.

Hasil pemodelan ini selanjutnya digunakan sebagai dasar dalam mengevaluasi efektivitas penerapan RPKI dalam menurunkan tingkat risiko yang telah diidentifikasi pada tahap sebelumnya.



Gambar 4. Mekanisme mitigasi menggunakan RPKI dengan ROA dan ROV

2. HASIL DAN PEMBAHASAN

Berdasarkan pemodelan skenario serangan route origin change serta penerapan mekanisme mitigasi menggunakan RPKI, diperoleh gambaran awal mengenai perilaku jaringan dalam menghadapi ancaman route hijacking. Perbedaan kondisi sebelum dan sesudah penerapan RPKI menunjukkan adanya perubahan signifikan pada proses pemilihan rute dan distribusi trafik dalam jaringan. Oleh karena itu, tahap selanjutnya difokuskan pada analisis hasil pengujian yang telah dilakukan untuk mengevaluasi dampak serangan terhadap ketersediaan dan keamanan layanan, serta mengukur efektivitas mekanisme mitigasi yang diterapkan. Pembahasan ini akan menguraikan temuan secara sistematis berdasarkan data hasil eksperimen, sehingga dapat memberikan pemahaman yang komprehensif mengenai tingkat risiko dan keberhasilan pengendalian yang diusulkan.

A. Hasil Pemodelan Risiko

Hasil pengujian pada skenario route hijacking tanpa penerapan mekanisme keamanan menunjukkan bahwa rute yang diumumkan oleh Autonomous System (AS) penyerang berhasil diterima dan diproses oleh jaringan sebagai jalur yang valid. Hal ini terjadi karena protokol Border Gateway Protocol (BGP) tidak melakukan validasi terhadap asal prefiks yang diumumkan, sehingga router cenderung memilih rute berdasarkan atribut terbaik, seperti nilai AS path yang lebih pendek atau preferensi kebijakan tertentu. Akibatnya, lalu lintas pengguna yang seharusnya menuju sistem yang sah dialihkan ke jaringan milik penyerang. Meskipun layanan internal tetap berjalan normal, pengalihan jalur ini menyebabkan terganggunya akses pengguna serta meningkatkan risiko keamanan, termasuk potensi penyadapan dan manipulasi data. Temuan ini menunjukkan bahwa tanpa mekanisme validasi tambahan, BGP sangat rentan terhadap serangan route hijacking, khususnya dalam skenario route origin change, yang dapat berdampak langsung terhadap keandalan dan keamanan layanan jaringan.

Untuk mendukung analisis hasil pengujian, dilakukan pengamatan terhadap lalu lintas jaringan menggunakan *packet capture* guna mengidentifikasi perubahan jalur komunikasi yang terjadi selama skenario *route hijacking*. Hasil tangkapan paket tersebut memberikan bukti empiris mengenai proses pengalihan trafik dari rute yang sah ke rute yang diumumkan oleh AS penyerang. Ilustrasi hasil *packet capture* disajikan pada gambar yang menunjukkan perbedaan pola komunikasi sebelum dan sesudah serangan terjadi.

No	Time	Source AS	Prefix	AS Path	Info
1	1	AS65001	10.10.0.0/24	65001	BGP UPDATE (Valid)
2	2	AS65005	10.10.0.0/24	65005	BGP HIJACK
3	3	AS65002	10.10.0.0/24	65002 65005	BGP HIJACK
4	4	AS65003	10.10.0.0/24	65003 65002 65005	BGP HIJACK

BGP UPDATE DETAIL					
Prefix: 10.10.0.0/24					
Origin AS: 65002					
AS_Path: 65002 65001					
Status: BGP UPDATE (Valid)					
ROA Validation:					
- ROA: VALID					
- Action: ACCEPTED					
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF					
00 3C 02 00 00 00 00 40 01 01 00					

Gambar 5. Hasil Capture Package saat serangan Route Hijacking

Selain itu, untuk mengevaluasi tingkat risiko yang ditimbulkan, dilakukan penyusunan tabel analisis risiko yang mempertimbangkan aspek kemungkinan (*likelihood*) dan dampak (*impact*) dari serangan *route origin change*. Tabel tersebut digunakan untuk mengklasifikasikan tingkat risiko serta menjadi dasar dalam menilai urgensi penerapan mekanisme mitigasi yang telah diusulkan.

Tabel 3. Analisis Risiko Serangan *Route Hijacking*

No	Skenario Ancaman	Deskripsi Risiko	Likelihood	Impact	Tingkat Risiko
1	Route Origin Change	AS penyerang mengiklankan prefiks tidak sah sehingga rute valid tergantikan	Tinggi	Tinggi	Tinggi
2	Pengalihan Trafik	Trafik pengguna dialihkan ke jaringan penyerang tanpa disadari	Tinggi	Tinggi	Tinggi
3	Penurunan Ketersediaan	Layanan tidak dapat diakses atau mengalami gangguan akibat perubahan rute	Sedang	Tinggi	Tinggi
4	Credential Harvesting	Penyerang menyadap data autentikasi pengguna melalui jalur yang dikompromikan	Sedang	Tinggi	Tinggi
5	Manipulasi Data	Data yang dikirimkan dapat diubah oleh pihak tidak berwenang	Rendah	Tinggi	Sedang
6	Ketidakkuratan Routing	Router menyimpan informasi rute yang tidak valid dalam tabel routing	Tinggi	Sedang	Tinggi

Selain dampak terhadap aspek routing yang ditampilkan pada tabel 3, serangan *route origin change* juga berpotensi menimbulkan ancaman lanjutan terhadap keamanan informasi, khususnya dalam bentuk *credential harvesting*. Pengalihan jalur komunikasi yang berhasil dilakukan oleh penyerang membuka peluang untuk melakukan penyadapan terhadap data sensitif yang dikirimkan oleh pengguna, כגון informasi autentikasi. Oleh karena itu, analisis risiko tidak hanya difokuskan pada ketersediaan layanan, tetapi juga mencakup aspek kerahasiaan dan integritas data. Untuk memberikan evaluasi yang lebih komprehensif, risiko *credential harvesting* dianalisis menggunakan pendekatan *CIA Triad* yang meliputi *Confidentiality*, *Integrity*, dan *Availability*. Hasil analisis tersebut disajikan dalam bentuk tabel 4 untuk mengidentifikasi tingkat dampak terhadap masing-masing aspek keamanan informasi serta sebagai dasar dalam menentukan prioritas mitigasi yang diperlukan.

Tabel 4. Analisis Dampak Risiko Credential Harvesting

No	Aspek Keamanan	Dampak terhadap Pengguna	Dampak terhadap Sistem SIA
1	Kerahasiaan (<i>Confidentiality</i>)	Kredensial akun pengguna berpotensi dicuri dan diketahui oleh pihak tidak berwenang	Data sensitif pengguna dapat diakses tanpa otorisasi

2	Integritas (<i>Integrity</i>)	Akun pengguna dapat disalahgunakan untuk melakukan perubahan data	Terjadi risiko manipulasi data akademik atau informasi sistem
3	Ketersediaan (<i>Availability</i>)	Pengguna dapat kehilangan akses ke akun akibat pengambilalihan	Layanan berpotensi terganggu akibat penyalahgunaan akun
4	Keamanan Akun	Risiko pengambilalihan akun (<i>account takeover</i>) meningkat	Meningkatnya jumlah insiden keamanan internal
5	Privasi Pengguna	Informasi pribadi pengguna dapat terekspos	Pelanggaran kebijakan perlindungan data
6	Kepercayaan Pengguna	Menurunnya kepercayaan terhadap layanan SIA	Reputasi institusi pengelola sistem terdampak
7	Potensi Serangan Lanjutan	Akun yang dikompromikan dapat digunakan untuk serangan lanjutan	Mempermudah eskalasi serangan ke sistem lain
8	Kepatuhan Keamanan	–	Berpotensi melanggar standar dan kebijakan keamanan informasi

Berdasarkan hasil analisis risiko yang telah dilakukan, baik dari sisi gangguan routing maupun potensi *credential harvesting* berdasarkan pendekatan CIA Triad, dapat disimpulkan bahwa serangan *route origin change* memiliki dampak yang signifikan terhadap aspek kerahasiaan, integritas, dan ketersediaan layanan. Tingkat risiko yang tergolong tinggi pada beberapa skenario menunjukkan bahwa mekanisme keamanan bawaan BGP belum mampu memberikan perlindungan yang memadai terhadap ancaman tersebut. Oleh karena itu, diperlukan suatu pendekatan mitigasi yang mampu melakukan validasi terhadap keabsahan informasi routing secara sistematis dan terukur. Dengan demikian, pembahasan selanjutnya difokuskan pada penerapan mekanisme keamanan berbasis Resource Public Key Infrastructure (RPKI) sebagai solusi untuk meminimalkan risiko yang telah diidentifikasi serta meningkatkan keamanan dan keandalan layanan jaringan secara keseluruhan.

B. Hasil Mitigasi Dengan RPKI

Sebagai respons terhadap risiko yang telah diidentifikasi, penelitian ini mengusulkan penerapan *Resource Public Key Infrastructure* (RPKI) sebagai mekanisme mitigasi untuk meningkatkan keamanan pada proses pertukaran informasi routing. RPKI merupakan kerangka kerja kriptografi yang dirancang untuk memverifikasi keabsahan kepemilikan prefiks IP serta keterkaitannya dengan *Autonomous System* (AS) yang berwenang. Melalui mekanisme ini, setiap pengumuman rute dapat divalidasi sebelum diproses oleh router, sehingga mengurangi kemungkinan diterimanya rute tidak sah dalam jaringan.

Implementasi RPKI dalam penelitian ini dilakukan melalui dua komponen utama, yaitu *Route Origin Authorization* (ROA) dan *Route Origin Validation* (ROV). ROA digunakan untuk mendefinisikan pasangan antara prefiks IP dan ASN yang berhak mengiklankannya, sedangkan ROV berfungsi sebagai mekanisme pada router untuk memvalidasi pengumuman rute berdasarkan informasi ROA yang tersedia. Proses validasi dilakukan oleh validator RPKI, seperti Routinator, yang memberikan status valid, invalid, atau not found terhadap setiap rute yang diterima. Router kemudian menerapkan kebijakan tertentu, di mana rute dengan status invalid akan ditolak, sementara rute valid diprioritaskan dalam proses pemilihan jalur.

Dengan diterapkannya mekanisme ini, pengumuman prefiks oleh AS penyerang yang tidak sesuai dengan data ROA akan teridentifikasi sebagai tidak valid dan tidak akan diproses lebih lanjut oleh router. Hal ini secara langsung mencegah terjadinya pengalihan jalur komunikasi yang menjadi dasar dari serangan *route hijacking*. Selain itu, penerapan RPKI juga berkontribusi dalam menjaga integritas jalur routing serta melindungi data pengguna dari potensi penyadapan, termasuk serangan *credential harvesting*. Untuk memperjelas hasil penerapan mekanisme mitigasi tersebut, Gambar 6 disajikan guna menunjukkan kondisi jaringan setelah implementasi RPKI, termasuk proses validasi rute dan penolakan terhadap pengumuman prefiks yang tidak sah.

No	Time	Source AS	Prefix	AS Path	Info
1	1	AS65001	10.10.0.0/24	65001	BGP UPDATE (Valid)
2	2	AS65005	10.10.0.0/24	65005	BLOCKED by RPKI
3	3	AS65002	10.10.0.0/24	65002 65005	BLOCKED by RPKI
4	4	AS65002	10.10.0.0/24	65002 65001	BGP UPDATE (Valid)
5	5	AS65003	10.10.0.0/24	65003 65002 65001	BGP UPDATE (Valid)

BGP UPDATE DETAIL					
Prefix: 10.10.0.0/24					
Origin AS: 65002					
AS_Path: 65002 65005					
Status: BLOCKED by RPKI					
RPKI Validation:					
ROA: INVALID					
Action: REJECTED					

FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF					
00 3C 02 00 00 00 00 40 01 01 00					

Gambar 6. Hasil *Capture Package* saat *Prefix* tidak sah ditolak oleh RPKI

Hasil pengujian menunjukkan bahwa penerapan Resource Public Key Infrastructure (RPKI) secara efektif mampu menolak pengumuman prefiks yang tidak sah dalam skenario *route hijacking*. Ketika Autonomous System (AS) penyerang mencoba mengiklankan prefiks milik sistem yang sah dengan ASN yang tidak sesuai, validator RPKI mengidentifikasi rute tersebut dengan status *invalid*. Router yang telah menerapkan kebijakan *Route Origin Validation* (ROV) kemudian secara otomatis menolak rute tersebut dan tidak memasukkannya ke dalam tabel routing. Akibatnya, rute palsu tidak dapat digunakan sebagai jalur komunikasi, sehingga lalu lintas pengguna tetap diarahkan melalui rute yang valid. Kondisi ini membuktikan bahwa mekanisme RPKI mampu mencegah terjadinya pengalihan trafik yang sebelumnya menjadi celah utama dalam serangan *route origin change*.

Berdasarkan hasil tersebut, diperlukan pemahaman yang lebih mendalam mengenai mekanisme kerja RPKI dalam melakukan proses validasi dan pengambilan keputusan terhadap rute yang diterima. Oleh karena itu, pembahasan selanjutnya difokuskan pada mekanisme RPKI, khususnya interaksi antara *Route Origin Authorization* (ROA), validator RPKI, dan kebijakan *Route Origin Validation* (ROV) pada router, sehingga dapat dijelaskan secara sistematis bagaimana proses identifikasi dan penolakan terhadap rute tidak sah dilakukan dalam jaringan. Tabel 5 berikut adalah mekanisme RPKI dengan ROA dan ROV untuk validasi prefix yang sah

Tabel 5. Mekanisme RPKI dengan validasi ROA dan ROV

No	Komponen	Fungsi	Proses	Output/Status
1	ROA (<i>Route Origin Authorization</i>)	Mendefinisikan AS yang berhak mengumumkan suatu prefiks IP	Pemilik prefiks membuat ROA yang berisi prefix dan ASN yang diizinkan	Data ROA
2	RPKI Repository	Menyimpan data ROA secara publik	ROA dipublikasikan ke repository oleh pemilik sumber daya IP	ROA tersedia publik
3	RPKI Validator	Mengambil dan memverifikasi data ROA dari repository	Validator mengunduh dan memvalidasi keaslian ROA menggunakan sertifikat digital	Data tervalidasi
4	Router (BGP)	Menerima rute dari peer dan melakukan pengecekan terhadap ROA	Router mencocokkan prefix dan ASN dengan data dari validator (RTR protocol)	Status validasi
5	Proses Validasi	Menentukan keabsahan rute yang diterima	Perbandingan antara origin AS pada BGP dengan ROA yang tersedia	Valid / Invalid / Not Found
6	Kebijakan Routing	Menentukan tindakan terhadap rute berdasarkan hasil validasi	Router menerapkan filtering atau preferensi terhadap rute	Rute diterima/ditolak

Berdasarkan tabel analisis yang telah disajikan, dapat disimpulkan bahwa penerapan mekanisme RPKI memberikan dampak signifikan dalam menurunkan tingkat risiko yang sebelumnya tergolong tinggi akibat serangan route hijacking. Validasi terhadap asal prefiks memungkinkan sistem untuk mengidentifikasi dan menolak rute yang tidak sah, sehingga risiko pengalihan trafik, gangguan layanan, serta potensi credential harvesting dapat diminimalkan. Selain itu, terjadi peningkatan pada aspek keamanan informasi yang mencakup kerahasiaan, integritas, dan ketersediaan layanan, yang menunjukkan bahwa RPKI berperan penting dalam memperkuat ketahanan jaringan terhadap ancaman berbasis routing.

Selanjutnya, pembahasan difokuskan pada analisis lebih mendalam terhadap hasil penerapan RPKI, termasuk evaluasi kinerja mekanisme validasi dalam berbagai skenario pengujian serta implikasinya terhadap stabilitas dan keandalan jaringan. Analisis ini juga akan mengkaji perbandingan kondisi sebelum dan sesudah penerapan mitigasi, sehingga dapat memberikan gambaran yang komprehensif mengenai efektivitas RPKI dalam mengatasi risiko serangan route hijacking secara menyeluruh.

C. Pembahasan

Secara keseluruhan, hasil penelitian menunjukkan bahwa serangan route hijacking dalam bentuk route origin change memiliki dampak yang signifikan terhadap keandalan dan keamanan layanan jaringan. Pada kondisi tanpa mekanisme pengamanan, protokol *Border Gateway Protocol* (BGP) cenderung menerima pengumuman rute tanpa melakukan verifikasi terhadap keabsahan asal prefiks, sehingga memungkinkan *Autonomous System* (AS) penyerang untuk mengiklankan rute palsu yang kemudian dipilih sebagai jalur terbaik. Hal ini menyebabkan terjadinya pengalihan trafik pengguna ke jaringan yang tidak sah, yang tidak hanya mengganggu ketersediaan layanan, tetapi juga membuka potensi serangan lanjutan seperti credential harvesting. Analisis risiko yang dilakukan menunjukkan bahwa ancaman ini memiliki tingkat risiko tinggi, terutama pada aspek kerahasiaan dan integritas data berdasarkan pendekatan CIA Triad.

Penerapan *Resource Public Key Infrastructure* (RPKI) sebagai mekanisme mitigasi terbukti mampu meningkatkan keamanan routing secara signifikan. Melalui implementasi *Route Origin Authorization* (ROA) dan *Route Origin Validation* (ROV), setiap pengumuman prefiks dapat divalidasi sehingga rute dengan asal yang tidak sah dapat diidentifikasi dan ditolak oleh router. Hasil pemodelan menunjukkan bahwa mekanisme ini efektif dalam mencegah pengalihan jalur komunikasi, menjaga trafik tetap berada pada rute yang valid, serta menurunkan tingkat risiko terhadap serangan route hijacking dan eksploitasi lanjutan. Dengan demikian, penelitian ini menegaskan bahwa integrasi RPKI dalam infrastruktur jaringan merupakan langkah yang tepat untuk meningkatkan keandalan, keamanan, serta keberlangsungan layanan, khususnya pada sistem informasi berbasis jaringan yang bersifat kritis. Tabel 6 berikut membandingkan keadaan sebelum dan sesudah RPKI sebagai mitigasi

Tabel 6. Perbandingan keadaan routing sebelum dan sesudah RPKI sebagai mitigasi

Aspek Analisis	Tanpa RPKI (Sebelum)	Dengan RPKI (Sesudah)	Keterangan Dampak
Validasi Asal Prefiks	Tidak tersedia	Tersedia (ROA & ROV)	Meningkatkan kepercayaan rute
Penerimaan Rute Tidak Sah	Diterima oleh router	Ditolak (<i>invalid</i>)	Mengurangi risiko hijacking
Pemilihan Jalur Routing	Berdasarkan atribut BGP (AS Path, dll)	Berdasarkan validasi + atribut BGP	Lebih aman dan terkontrol
Pengalihan Trafik	Terjadi	Tidak terjadi	Menjaga keaslian jalur komunikasi
Risiko Credential Harvesting	Tinggi	Rendah	Data pengguna lebih terlindungi
Ketersediaan Layanan	Terganggu	Stabil	Layanan tetap dapat diakses
Integritas Data	Berpotensi terkompromi	Terjaga	Menghindari manipulasi data

Keamanan Routing	Rendah	Tinggi	Ketahanan jaringan meningkat
------------------	--------	--------	------------------------------

Tabel tersebut menunjukkan perbandingan kondisi jaringan sebelum dan sesudah penerapan RPKI secara kualitatif. Terlihat bahwa tanpa mekanisme validasi, jaringan rentan terhadap penerimaan rute tidak sah yang berujung pada pengalihan trafik dan peningkatan risiko keamanan. Sebaliknya, setelah penerapan RPKI, seluruh rute yang tidak valid dapat diidentifikasi dan ditolak, sehingga proses routing menjadi lebih aman dan terkendali. Perbaikan ini tidak hanya berdampak pada aspek teknis routing, tetapi juga secara langsung meningkatkan perlindungan terhadap data pengguna dan menjaga stabilitas layanan secara keseluruhan. Temuan ini memperkuat hasil analisis sebelumnya bahwa RPKI merupakan solusi mitigasi yang efektif dalam mengatasi risiko serangan *route hijacking*.

Berdasarkan hasil pemodelan, analisis risiko, serta evaluasi penerapan mekanisme mitigasi yang telah dilakukan, dapat diperoleh gambaran menyeluruh mengenai dampak serangan *route hijacking* dan efektivitas pengamanan yang diusulkan. Temuan penelitian menunjukkan adanya perbedaan yang signifikan antara kondisi sebelum dan sesudah penerapan RPKI, baik dari sisi keamanan routing maupun perlindungan terhadap data pengguna. Oleh karena itu, untuk merangkum seluruh hasil dan temuan yang telah dibahas, bagian selanjutnya akan menyajikan kesimpulan penelitian yang mencakup poin-poin utama serta kontribusi yang dihasilkan dalam upaya peningkatan keamanan jaringan.

D. Evaluasi

Pada tahap evaluasi, analisis dilakukan dengan membandingkan perilaku jaringan pada tiga kondisi, yaitu routing normal, *route hijacking* tanpa mitigasi, dan *route hijacking* dengan penerapan Resource Public Key Infrastructure (RPKI). Hasil pengujian menunjukkan bahwa perbedaan utama tidak hanya terletak pada keberhasilan atau kegagalan serangan, tetapi pada mekanisme pengambilan keputusan routing itu sendiri. Pada kondisi tanpa RPKI, proses seleksi rute sepenuhnya bergantung pada atribut BGP seperti AS path, yang secara inheren tidak mempertimbangkan keabsahan asal prefiks. Hal ini menyebabkan rute yang diumumkan oleh penyerang dapat diterima dan diprioritaskan, sehingga mengindikasikan bahwa kelemahan autentikasi pada BGP menjadi faktor dominan dalam keberhasilan *route hijacking*. Sebaliknya, pada kondisi dengan RPKI, terjadi perubahan fundamental dalam proses seleksi rute, di mana validitas origin menjadi parameter tambahan yang menentukan penerimaan rute melalui mekanisme *Route Origin Validation (ROV)*. Dengan demikian, rute dengan status *invalid* secara sistematis dieliminasi sebelum masuk ke dalam tabel routing, sehingga menggeser paradigma dari *performance-based routing* menjadi *validation-aware routing*.

Lebih lanjut, hasil evaluasi menunjukkan bahwa penerapan RPKI tidak hanya berdampak pada stabilitas jalur routing, tetapi juga memiliki implikasi langsung terhadap keamanan komunikasi jaringan. Tidak ditemukannya pengalihan trafik pada hasil *traceroute* dan analisis paket menggunakan Wireshark mengindikasikan bahwa kontrol pada lapisan routing mampu mencegah eksposur trafik terhadap entitas yang tidak sah. Hal ini memperlihatkan adanya keterkaitan yang kuat antara keamanan routing dan perlindungan data pengguna, khususnya dalam mengurangi potensi *credential harvesting*. Dengan kata lain, pengamanan pada lapisan infrastruktur jaringan berkontribusi secara langsung terhadap peningkatan keamanan pada lapisan aplikasi, sehingga pendekatan keamanan tidak dapat dipandang secara terpisah antar lapisan.

Namun demikian, hasil evaluasi juga mengungkap keterbatasan struktural dari penerapan RPKI. Ketergantungan terhadap ketersediaan dan konsistensi data *Route Origin Authorization (ROA)* menyebabkan masih adanya prefiks dengan status *not found*, yang tidak dapat divalidasi secara penuh. Kondisi ini menunjukkan bahwa keberhasilan RPKI tidak hanya ditentukan oleh implementasi lokal, tetapi juga oleh tingkat adopsi secara global. Oleh karena itu, meskipun RPKI mampu memperkuat mekanisme validasi routing, efektivitasnya dalam skala luas sangat bergantung pada kolaborasi antar operator jaringan. Untuk memberikan gambaran yang lebih sistematis terhadap hasil evaluasi tersebut,

Tabel menyajikan perbandingan parameter yang diamati pada kondisi tanpa mitigasi dan dengan penerapan RPKI.

Tabel 7. Evaluasi Model

Parameter Evaluasi	Tanpa RPKI	Dengan RPKI	Keterangan Evaluasi
Penerimaan Rute Palsu	Diterima	Ditolak	RPKI mampu memfilter rute tidak sah
Validasi Origin Prefix	Tidak ada	Ada (ROA & ROV)	Validasi meningkatkan kepercayaan routing
Status Prefix	Tidak tervalidasi	VALID / INVALID	Prefix attacker terdeteksi INVALID
Stabilitas Routing	Tidak stabil	Stabil	Routing kembali normal setelah RPKI
Perubahan AS Path	Terjadi perubahan	Tidak berubah	Jalur tetap sesuai rute sah
Pengalihan Trafik	Terjadi	Tidak terjadi	Trafik tetap ke tujuan asli
Hasil Traceroute	Mengarah ke attacker	Mengarah ke SIA	Jalur kembali normal
Hasil Wireshark	Tujuan berubah (attacker)	Tujuan sesuai (SIA)	Tidak ada manipulasi trafik
Akses Layanan	Fake SIA (phishing)	SIA asli	Pengguna terlindungi
Risiko Keamanan	Tinggi	Rendah	Risiko menurun signifikan
Potensi Credential Harvesting	Ada	Tidak ada	Serangan lanjutan dapat dicegah
Efektivitas Mitigasi	Tidak efektif	Sangat efektif	RPKI berhasil mencegah hijacking

Berdasarkan tabel evaluasi yang telah disajikan, dapat dianalisis bahwa terdapat perbedaan yang sangat signifikan antara kondisi jaringan tanpa RPKI dan dengan penerapan RPKI dalam menghadapi serangan *route hijacking*. Pada pemodelan tanpa RPKI, jaringan menunjukkan berbagai kelemahan, seperti diterimanya rute palsu, tidak adanya validasi terhadap origin prefix, perubahan jalur routing, serta pengalihan trafik ke jaringan penyerang. Hal ini berdampak langsung pada meningkatnya risiko keamanan, termasuk potensi terjadinya *credential harvesting* melalui layanan palsu. Sebaliknya, pada pemodelan dengan RPKI, seluruh parameter menunjukkan perbaikan yang signifikan, di mana rute palsu berhasil ditolak, jalur routing tetap stabil, serta trafik pengguna tetap mengarah ke tujuan yang sah. Mekanisme validasi menggunakan ROA dan ROV terbukti mampu menjaga integritas routing dan mencegah manipulasi oleh pihak tidak berwenang.

Dengan demikian, hasil evaluasi ini menunjukkan bahwa penerapan RPKI memiliki efektivitas yang tinggi dalam memitigasi serangan *route hijacking* serta meningkatkan keamanan jaringan secara keseluruhan. Perbandingan antar parameter memperlihatkan bahwa RPKI tidak hanya berperan dalam menolak rute palsu, tetapi juga melindungi aliran data pengguna dari potensi penyalahgunaan. Oleh karena itu, berdasarkan hasil analisis yang telah dilakukan, tahap selanjutnya akan merumuskan kesimpulan dari penelitian ini serta memberikan rekomendasi terkait penerapan RPKI sebagai solusi dalam meningkatkan keamanan infrastruktur jaringan.

3. KESIMPULAN

Berdasarkan hasil penelitian, implementasi, dan pengujian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

- 1) Serangan *route hijacking* dalam bentuk *route origin change* memanfaatkan kelemahan pada *Border Gateway Protocol* (BGP) yang tidak memiliki mekanisme validasi asal rute, sehingga memungkinkan *Autonomous System* (AS) tidak sah mengiklankan prefiks secara bebas.
- 2) Pada kondisi tanpa pengamanan, rute palsu dapat diterima dan dipilih sebagai jalur terbaik oleh router, yang menyebabkan pengalihan trafik pengguna ke jaringan penyerang.
- 3) Dampak serangan tidak hanya mengganggu ketersediaan layanan, tetapi juga meningkatkan risiko keamanan informasi, terutama potensi *credential harvesting* yang memengaruhi aspek kerahasiaan dan integritas data.

- 4) Analisis risiko menunjukkan bahwa serangan ini memiliki tingkat risiko tinggi, khususnya pada aspek *Confidentiality* dan *Integrity* dalam pendekatan CIA *Triad*.
- 5) Penerapan *Resource Public Key Infrastructure* (RPKI) melalui mekanisme *Route Origin Authorization* (ROA) dan *Route Origin Validation* (ROV) terbukti mampu memvalidasi keabsahan asal rute secara efektif.
- 6) Rute dengan status *invalid* berhasil diidentifikasi dan ditolak oleh *router*, sehingga mencegah pengalihan jalur komunikasi yang tidak sah.
- 7) Implementasi RPKI mampu menurunkan tingkat risiko secara signifikan serta meningkatkan keamanan routing, stabilitas jaringan, dan perlindungan terhadap data pengguna.
- 8) Secara keseluruhan, RPKI direkomendasikan sebagai solusi mitigasi yang efektif untuk meningkatkan keandalan dan keamanan layanan jaringan, khususnya pada sistem informasi yang bersifat kritis.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Ibu Linna Oktaviana Sari, S.T., M.T., selaku Dosen Pembimbing yang telah memberikan arahan, masukan, dan bimbingan yang sangat berarti selama proses penelitian. Selain itu, penulis juga mengucapkan terima kasih kepada Jurusan Teknik Informatika, Universitas Riau atas dukungan yang diberikan selama penyusunan penelitian ini.

REFERENSI

- [1] Rekhter, Y., Li, T., & Hares, S. (2021). *A Border Gateway Protocol 4 (BGP-4)*. RFC 4271. Internet Engineering Task Force (IETF).
- [2] Huston, G. (2022). *BGP Routing Security*. Asia Pacific Network Information Centre (APNIC).
- [3] Bush, R., & Austein, R. (2021). *The Resource Public Key Infrastructure (RPKI) to Router Protocol*. RFC 6810. Internet Engineering Task Force (IETF).
- [4] CAIDA. (2022). *BGPStream Project*. The Cooperative Association for Internet Data Analysis.
- [5] RIPE NCC. (2022). *Routing Information and RPKI Validation*. RIPE Network Coordination Centre.
- [6] Mutually Agreed Norms for Routing Security (MANRS). (2022). *Best Current Operational Practices for Routing Security*. Internet Society.
- [7] Zhang, Z., et al. (2022). *A Survey of BGP Security Issues and Solutions*. IEEE Communications Surveys & Tutorials, 24(3), 1240–1268.
- [8] BSSN. (2022). *Laporan Tahunan Keamanan Siber Indonesia*. Badan Siber dan Sandi Negara, Jakarta.
- [9] ID-SIRTII. (2022). *Laporan Statistik Keamanan Internet Indonesia*. Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika.
- [10] Vervier, P.-A., Thonnard, O., & Dacier, M. (2021). *Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks*. Proceedings of NDSS Symposium 2021.
- [11] Sermpezis, P., Kotronis, V., & Dimitropoulos, X. (2020). *Hijacks in the Wild: An Analysis of BGP*

-
- Prefix Hijacking Incidents*. Computer Communications, 149, 136–147.
- [12] Zhang, L., Yan, J., & Wu, J. (2020). *Detection of BGP Hijacking Attacks Based on Real-Time Monitoring*. IEEE Access, 8, 184563–184574.
- [13] Giotsas, V., & Dietzel, C. (2021). *Towards a More Secure Interdomain Routing: Evaluating the Impact of RPKI Deployment*. ACM SIGCOMM Computer Communication Review, 51(3), 20–27.
- [14] Mikians, J., Konte, M., & Bush, R. (2021). *Practical Challenges in Deploying RPKI at Scale*. Proceedings of ACM SIGCOMM 2021, 25–37.
- [15] Nikkhah, M., & Ganjali, Y. (2021). *Mitigating Route Hijacking Attacks Using SDN-Based Detection and Response*. IEEE Transactions on Network and Service Management, 18(2), 1234–1247.
- [16] Sun, Y., Zhao, J., & Chen, X. (2022). *RPKI Deployment in Practice: Measurement and Security Implications*. IEEE Transactions on Dependable and Secure Computing, 19(4), 2501–2515.
- [17] Kim, H., & Lee, S. (2022). *BGP Hijacking as a Cybercrime Vector: Case Study on Cryptocurrency Theft*. Journal of Cybersecurity, 8(2), taac012.
- [18] Van Beijnum, I., & Bush, R. (2023). *Operational Lessons from Global RPKI Adoption*. RIPE NCC Technical Report, 2023-02, 1–15.
- [19] Tran, Q., & Shafiee, H. (2023). *Machine Learning Approaches for Real-Time BGP Hijack Detection*. Future Internet, 15(6), 187.
- [20] Kühner, M., Wählisch, M., & Richter, P. (2024). *Route Leaks and Their Impact on the Global Internet: Analysis and Mitigation*. Proceedings of ACM Internet Measurement Conference (IMC 2024), 50–63.
- [21] Canonical Ltd. (2022). *Ubuntu Documentation*. Canonical.
- [22] Negus, C. (2020). *Linux Bible* (10th ed.). Wiley.
- [23] Sobell, M. G. (2021). *A Practical Guide to Ubuntu Linux* (5th ed.). Addison-Wesley.
- [24] Lyon, G. F. (2022). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Nmap Project.
- [25] Kaur, R., & Singh, M. (2021). *A Study on Port Scanning Techniques Using Nmap for Network Security*. International Journal of Computer Applications, 183(28), 15–20.
- [26] Zhang, Y., & Lin, J. (2023). *Evaluation of Open-Source Network Scanners for Cybersecurity Testing*. Journal of Network and Computer Applications, 213, 103582.
-

- [27] Tanenbaum, A. S., & Bos, H. (2021). *Modern Operating Systems* (5th ed.). Pearson.
- [28] Canonical Ltd. (2023). *Ubuntu Documentation*. Canonical.
- [29] Laudon, K. C., & Laudon, J. P. (2022). *Management Information Systems: Managing the Digital Firm* (17th ed.). Pearson.
- [30] Stair, R., & Reynolds, G. (2021). *Principles of Information Systems* (14th ed.). Cengage Learning.
- [31] Bush, R., & Austein, R. (2021). *The Resource Public Key Infrastructure (RPKI) to Router Protocol*. RFC 6810. Internet Engineering Task Force (IETF).