साइबर-सुरक्षा मिथक

परिचय

हालांकि पिछले कुछ दशकों में इंटरनेट ने ज़बरदस्त तरक्की की है, लेकिन यह आ□ भी कमज़ोर है और बड़े-छोटे हमलों का शिकार हो सकता है। यूज़र्स इसके □टिल कामका□ को लेकर कन्फ्यूज़ रहते हैं और □क्सर घुसपैठिए द्वारा किए गए हैक और प्रोटेक्टिव सॉफ्टवेयर में सेंध के बीच फर्क नहीं कर पाते हैं।

ऐसा ही एक हालिया मामला 18 नवंबर 2025 को हुआ, □ब क्लाउ□फ्लेयर में ग्लोबल आउटे□ हुआ, □ससे कुछ समय के लिए इंटरनेट का एक बड़ा हिस्सा बंद हो गया[1]। यह कोई □केली घटना नहीं थी। इससे पहले ऐसी घटना सिर्फ़ आठ महीने पहले हुई थी, और उससे पहले भी ऐसी कई घटनाएँ हुई थीं। इसी तरह, □मेज़न वेब सर्विसेज़ (AWS) भी □क्सर बाधित होती रही है[2]। इस तरह का इंटरनेट आउटे□ लगभग आम बात हो गई है और साइबर हमलों से बचाने के लिए □ज़ाइन की गई इन सर्विसेज़ की विश्वसनीयता पर सवाल उठने लगे हैं।

समस्या

इंटरनेट की कमज़ोरी दशकों से एक मुद्दा रही है। पिछले साल, फे□रल कम्युनिकेशंस कमीशन (FCC) ने एक नोटिस ऑफ़ प्रपोज़□ रूल मेकिंग (NPRM)[3] □ारी किया था, □समें बॉ□र गेटवे प्रोटोकॉल (BGP)[4] को रिस्क कम करने के लिए टारगेट बताया गया था। इंटरनेट कम्युनिटी का प्रतिनिधित्व करने वाले इंटरनेट आर्किटेक्चर बो□ (IAB) ने एक कमेंट के साथ □वाब दिया □समें चिंताएं □ताई गईं[5]। इसके बाव□ूद, व्हाइट हाउस ने एक रो□मैप[6] पब्लिश किया, □समें इंटरनेट राउटिंग सिक्योरिटी को बेहतर बनाने के तरीके के तौर पर BGP की इंटीग्रिटी पर फोकस किया गया था।

इस संबंध में, यह ध्यान रखना ज़रूरी है कि BGP का इस्तेमाल ऑटोनॉमस सिस्टम (ASes)[7] के बीच पैकेट ट्रांसपोर्ट करने के लिए किया □ाता है, □न्हें □ोमेन नेम सर्वर (DNS)[8] द्वारा चुना □ाता है, □ो □ायनेमिक होस्ट कंट्रोल प्रोटोकॉल (DHCP)[9] द्वारा सब्सक्राइबर को दिए गए IPv4 ए□्रेस पर आधारित होता है, □से IPv4 ए□्रेस की कमी से निपटने के लिए बनाया गया था। इस प्रोटोकॉल स्टैक के कारण एक □टिल सिस्टम आर्किटेक्चर बना है □ो कई तरफ से हमलों के प्रति संवेदनशील है, और हर हमले के □वाब में एक और पैच की ज़रूरत होती है।

समाधान

एक खराब सिस्टम कभी न खत्म होने वाले हैक्स और पैच को न्योता देता है। एक बहुत ज़्यादा मज़बूत इंटरनेट एक आसान और स्ट्रीमलाइन्ड आर्किटेक्चर से बन सकता है □ो IPv4 ए□्रेस की कमी की □सली व□ह को खत्म कर देता है, □ससे ऊपर बताए गए चार प्रोटोकॉल में से किसी की भी ज़रूरत नहीं रहती। ऐसा ही नती□ा EzIP[10] नाम के एक □टरमिनिस्टिक सिस्टम से मिलता है।

□ब इंटरनेट पहली बार शुरू हुआ, तो पाँच री□नल इंटरनेट रि□स्ट्री (RIRs) को □च्छी तरह से परिभाषित बड़े IPv4 एड्रेस ब्लॉक दिए गए थे। उदाहरण के लिए, हिल्बर्ट कर्ल्स[11] □ो शुरुआती दिनों के AFRINIC (□फ्रीका), APNIC (एशिया-पैसिफिक), ARIN (उत्तरी □मेरिका), LACNIC (लैटिन □मेरिका और कैरिबियन) और RIPE (यूरोप, मध्य पूर्व और मध्य एशिया) के आवंटन को दिखाते थे, उन्हें आसानी से पहचाना □ा सकता था[12]।

हालांकि हर RIR ने □पने इलाके में इंटरनेट एक्सेस प्रोवाइ□र्स (IAPs) को □पने □लॉट किए गए एड्रेस दिए, लेकिन IAPs को खुद इस नियम का पालन करना ज़रूरी नहीं था। इससे IP एड्रेस फ्रेगमेंटेशन का रास्ता खुल गया, □ससे सब्सक्राइबर की फि□कल लोकेशन उस इलाके से ज्योग्राफिकली □ुड़ी नहीं रह गई, □हाँ □सल में IP एड्रेस □लॉट किया गया था।

□ैसे-□ैसे IPv4 एड्रेस पूल कम होने लगा, DHCP ने उपलब्ध पब्लिक IPv4 एड्रेस को □ायनामिक रूप से दोबारा इस्तेमाल करके IAP ऑपरेशन्स को □ारी रखा। फिर DNS को ऐसे लगातार बदलते माहौल के कारण सब्सक्राइबरों पर पड़ने वाले बोझ को कम करने के लिए पेश किया गया। क्योंकि यह प्रोटोकॉल □ोड़ी उस समय की ज़रूरी ज़रूरतों को पूरा करती हुई लगी, इसलिए यह □फ़ॉल्ट इंटरनेट बिल्डिंग ब्लॉक बन गई। (इस □ □ीब □ोड़ी के नती□ों के लिए फुटनोट देखें।)

□ब शुरुआती संस्थानों ने IPv4 एड्रेस पूल खत्म होने के दबाव को कम करने के लिए सरप्लस IPv4 एड्रेस ब्लॉक को पब्लिक नीलामी के लिए □ारी करने पर सहमति □ताई, तो यह उम्मीद करना □ब प्रैक्टिकल नहीं रहा कि किसी IPv4 एड्रेस में कोई भी सार्थक फि□कल लोकेशन की □ानकारी होगी, □योलोकेटिंग सब्सक्राइबर की संभावना तो दूर की बात है। इस ज़रूरत को पूरा करने के लिए इं□स्ट्री की एक □लग ब्रांच का □न्म हुआ। हालांकि, इसकी रिपोर्ट का रिज़ॉल्यूशन और सटीकता □क्सर ज़्यादा से ज़्यादा संदिग्ध होती थी[13]।

इस दौरान, एक या ज़्यादा IPv4 एड्रेस ब्लॉक वाले IAP ने □पनी-□पनी IP पैकेट □लीवरी स्कीम □वलप कीं। एक ही ट्रांसपोर्ट पॉलिसी वाले एड्रेस ब्लॉक एक साथ मिलकर एक AS बनाते थे। क्योंकि हर AS की रें□ □लग-□लग होती है और □क्सर लिमिटे□ होती है, इसलिए AS बॉ□र्र के पार IP पैकेट फॉरव□ करने के लिए BGP पर भरोसा किया गया। □ैसे-□ैसे AS की संख्या बढ़ी, वैसे-वैसे BGP की कॉम्प्लेक्सिटी भी बढ़ी, □ो उन पैकेट के लिए ज़िम्मेदार था □ो □क्सर लोकल लेवल पर ही काफी दूरी तय करते थे, और उन पैकेट की तो बात ही छोड़िए □ो ग्लोबल एड्रेस के लिए होते थे और □न्हें कई AS बॉ□र्र पार करने पड़ते थे।

हालांकि इनमें से हर प्रोटोकॉल स्वाभाविक रूप से □स्ट्रीब्यूटे□ है, लेकिन उनके ऑपरेशन के लिए काफी कोऑर्डि□नेशन की ज़रूरत होती है □ो सेंट्रलाइज़□ कोशिशों पर निर्भर करता है, □ससे कुछ ही साधन संपन्न बिज़नेस का दबदबा हो □ाता है, □ैसे कि कंटेंट □लीवरी नेटवर्क (CDN)[14] ऑपरेटर □नमें Cloudflare, AWS वगैरह शामिल हैं। ये इंटरनेट ट्रांसपोर्ट सुविधा के लिए मुख्य इंफ्रास्ट्रक्चर बन □ाते हैं।

विरोधाभासों

इंटरनेट पर ऐसी कई चीज़ें हैं □ो इसके सिद्धांतों और कामका□ को कन्फ्यू□ंग बनाती हैं:

इंटरनेट सबको बराबर का मौका देता है। लेकिन वेटिकन सिटी को प्रति व्यक्ति 21.4 IPv4 ए□्रेस मिलते हैं, □बकि एक द□न से ज़्यादा एंटिटीज़ को एक भी नहीं मिलता, और दूसरे देशों को इनके बीच की हर संभावना मिलती है[15]. (ध्यान दें: सेशेल्स को 58.4 एलोकेशन मिलना एक □ □ीब बात है, क्योंकि यह ग्लोबल मौकों के लिए लोकल रा□नीतिक माहौल का फायदा उठाने वाले बिज़नेस का नती□ा है।)

इंटरनेट ने एं□-टू-एं□ कनेक्टिविटी का वादा किया था। हालाँकि, इसका मौ□ूदा मुख्य ऑपरेशन मॉ□ल, CDN, लोकल कम्युनिटी में भी इस लक्ष्य को हासिल करने में रुकावट □ालता है।

इंटरनेट ने पब्लिक स्विच□ टेलीफोन नेटवर्क (PSTN) पर टेलीकॉम कंपनियों की मोनोपॉली और सरकारी रेगुलेशन पर सवाल उठाए थे। फिर भी, □ ब इंटरनेट पर मल्टीनेशनल कंपनियों का दबदबा है, □ो □ सल में बि□नेस सेक्टर पर मोनोपॉली कर रही हैं, इस हद तक कि वे □ पनी □म्मेदारियों को नज़र□ंदाज़ कर रही हैं और रेगुलेशन से बच रही हैं। क्या इस तरह का सेंट्रलाइज़ेशन, □स्ट्रीब्यूटे□ इंटरनेट के विज़न के बिल्कुल खिलाफ नहीं है?

साथ ही, लगभग 200 ग्लोबल ज्यूरिसि□क्शन द्वारा इंटरनेट को □ योपॉलिटिकल स्प्लिंटर्नेट[16] में बांटने की संभावना की इंटरनेट कम्युनिटी आलोचना कर रही है, □बकि ASes ने पहले ही इंटरनेट को कम से कम 77K लेयर्स[7] वाला एक □ नियन-नेट बना दिया है। इसके □ लावा, क्योंकि ज़्यादातर ASes चुनिंदा रूप से दुनिया के कुछ हिस्सों को ही सर्विस देते हैं, इसलिए प्या□ के छिलके की हर परत एक आंशिक मछली पकड़ने के □ाल □ैसी दिखती है □ समें छेद होते हैं!

सबसे हैरान करने वाली बात यह है कि इंटरनेट □ पने बॉ□रलेस सिद्धांत का ज़ोरदार बचाव करता है, □बकि इसका □ पना प्राइमरी राउटिंग मैकेनिज्म BGP बन गया है, □हाँ "B" हर ASes के चारों ओर की सीमाओं के लिए है!

कुल मिलाकर, इन प्रोटोकॉल के बहुत ज़्यादा □टिल और □स्ट्रीब्यूटे□ नेचर के कारण, इंटरनेट रोज़ाना की परेशानी से लेकर रैंसमवेयर तक, कई तरह के खतरनाक सिक्योरिटी उल्लंघनों का शिकार हो □ाता है।

शायद इस समय यह बताना सही रहेगा कि IPv6 ने, □ पने बड़े ए□्रेस पूल का फायदा उठाए बिना ही, बीच की ज़रूरतों से विकसित हुए इन IPv4 तरीकों को □ पना लिया। □ ब, IPv6 का महत्व धीरे-धीरे खत्म होता दिख रहा है[17], □बकि IPv4 को बंद करने की तारीख का □ ब कोई ज़िक्र नहीं होता। क्योंकि IPv6, IPv4 के मुकाबले कोई खास फायदे नहीं बताता, इसलिए ज़्यादातर इंटरनेट चर्चाओं में □ ब दोनों के बीच कोई फर्क नहीं किया □ाता।

संदर्भ

1. Cloudflare आउटे□ इतिहास(2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. AWS क्लाउ□ और □टा सेंटर आउटे□ का इतिहास
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. बॉर्□र गेटवे प्रोटोकॉल □ोखिम कम करने की प्रगति पर रिपोर्टिंग; सुरक्षित इंटरनेट रूटिंग
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. बॉर्□र गेटवे प्रोटोकॉल
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. "बॉर्□र गेटवे प्रोटोकॉल रिस्क मिटिगेशन प्रोग्रेस पर रिपोर्टिंग" के मामले में इंटरनेट सोसाइटी, इंटरनेट आर्किटेक्चर बो□, और इंटरनेट कॉर्पोरेशन फॉर □ साइन्ड नेम्स एं□ नंबर्स की टिप्पणियाँ।
   https://datatracker.ietf.org/doc/statement-iab-comments-of-the-internet-society-internet-architecture-board-and-internet-corporation-for-assigned-names-and-numbers-in-the-matter-of-reporting-on-border-gateway-protocol-risk-mitigation-progress/

6. इंटरनेट रूटिंग सुरक्षा को बढ़ाने के लिए रो□मैप
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. स्वायत्त प्रणाली (इंटरनेट)
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. □ोमेन की नामांकन प्रणाली
   https://en.wikipedia.org/wiki/Domain_Name_System

9. □ायनामिक होस्ट कॉन्फ़िगरेशन प्रोटोकॉल
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. एक नियतात्मक इंटरनेट
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. हिल्बर्ट वक्र
    https://en.wikipedia.org/wiki/Hilbert_curve

12. हिल्बर्ट कर्व्स का उपयोग करके IPv4 स्पेस को विज़ु□ लाइज़ करना
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. इंटरनेट □योलोकेशन
https://en.wikipedia.org/wiki/Internet_geolocation

14. सामग्री वितरण नेटवर्क
https://en.wikipedia.org/wiki/Content_delivery_network

15. IPv4 एड्रेस आवंटन के □ नुसार देशों की सूची
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. स्प्लिंटनेट
https://en.wikipedia.org/wiki/Splinternet

17. G□ॉफ हस्टन: इंटरनेट का □ तीत, वर्तमान और भविष्य
(TM: 1:08:18, "IPv6 – Increasingly irrelevant")
https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

पाद लेख

DHCP और DNS इंटरनेट टेक्नोलॉ□ी का सबसे हैरान करने वाला □ोड़ा है □ो इतने सालों से सबके सामने है। यानी, DHCP ज़रूरत के हिसाब से सब्सक्राइबर को □ायनामिक रूप से IP ए□्रेस देकर पर्सनल प्राइवेसी का वादा करता है, लेकिन DNS तुरंत ही इसे पूरी तरह से खत्म कर देता है, □ो रिक्वेस्ट करने पर, सिर्फ़ उस टारगेट की पहचान के आधार पर, किसी पार्टी को □ साइन किया गया लेटेस्ट IP ए□्रेस दिखाता है! ये आम सब्सक्राइबर को इस गलतफहमी में रखते हैं कि वे सुरक्षित हैं, □बकि बहुत सारे IT इं□ीनियरों को रोज़गार मिलता रहता है। यह चीनी कहावत, "भाला बनाम ढाल" (矛盾) का एक परफेक्ट उदाहरण है।

फिर भी, इस स्कीम के आधार पर प्रोटोकॉल की और भी लेयर्स AS, BGP से लेकर CDN बनाने तक बनती गईं, □िससे मल्टी-नेशनल कंपनियों का दबदबा बना, और Cloudflare और AWS □ैसी बड़ी सर्विसेज़ आईं □िन्होंने बेहतर सिक्योरिटी के साथ भरोसेमंद पैकेट ट्रांसपोर्ट देने का वादा किया। हालांकि, इन सर्विसेज़ की मज़बूती □क्सर सवालों के घेरे में रही है। और, □ब इंटरनेट में सेंध लगी, तो कोई भी ज़िम्मेदारी लेने और कमज़ोरी को कम करने के लिए विकल्प ढूंढने को तैयार नहीं था। शायद दोष देना मुश्किल था, क्योंकि पूरा इंटरनेट इतना ज़्यादा फैला हुआ था?

दूसरी ओर, मौ□ूदा इंटरनेट कॉन्फ़िगरेशन हमला करने वाले के लिए एक आदर्श सुविधा है, □ो हमले शुरू करने के लिए किसी भी मनमाने काल्पनिक IP ए□्रेस को एक वैध सामान्य इंटरनेट सब्सक्राइबर मान सकता है, और फिर बाद में उसे छोड़ देता है, □िससे फोरेंसिक ट्रेसिंग के लिए वैध पहचान वाले शायद ही कोई स्थायी रिकॉ□ बचते हैं।