Podcast Transcript

EPISODE #231

The Invisible Roads: Can BGP Hijacking Break Encryption?

Published January 15, 2026 • Runtime: 20:22

https://myweirdprompts.com/episode/bgp-hijacking-internet-security-risks/

EPISODE SYNOPSIS

Most users think of the internet as a direct line, but it’s actually a fragile web of over 90,000 independent networks held together by the Border Gateway Protocol (BGP). In this episode, Herman and Corn dive into the terrifying world of BGP hijacking—a technique where governments or malicious actors "lie" to the internet to reroute traffic through their own servers. Using historical maneuvers as a case study, the duo examines whether high-security apps like Signal can truly protect your data when the underlying roads of the web are compromised. They break down the difference between message content and the "who, when, and where" of metadata, explaining why your encrypted messages might be safe while your identity remains exposed. From the technical hurdles of RPKI adoption to the rise of the "splinternet," this conversation reveals the structural vulnerabilities of our digital world. Is our global communication network built on a foundation of trust that no longer exists? Tune in to find out how the invisible infrastructure of the web defines the future of digital sovereignty and personal privacy.

DANIEL'S PROMPT

Daniel

We've been talking about the internet and how it’s much more than just a place to watch cat videos. The networking side is really interesting, especially with the geopolitical disruptions happening in Iran, which provides a case study in how a government can disrupt the internet. We previously touched on BGP (Border Gateway Protocol) and the potential for man-in-the-middle attacks on a national scale. If BGP routing is altered at a macro-network level, affecting millions of users, do the end-to-end encryption safeguards in apps like Signal still protect the message contents and metadata? Let's discuss BGP as a potential vector for threats in today’s episode.

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. I am Corn, and today we are looking at something that is basically the nervous system of the modern world, but it is a system that almost nobody ever thinks about until it breaks. We are talking about the invisible roads of the internet.

Herman

And I am Herman Poppleberry. Corn, I have been looking forward to this one since breakfast. Our housemate Daniel sent us this prompt because he has been thinking about how the internet is far more than just cables and cat videos. He was specifically curious about the networking side of things and how geopolitical disruptions, like historical case studies in Iran, show how a government can actually manipulate the underlying fabric of the web.

Corn

It is a fascinating and honestly kind of terrifying topic. Daniel's question really gets to the heart of our digital security. He asked about Border Gateway Protocol, or BGP, which we have touched on before, specifically in episode one hundred seventy-three when we talked about achieving the gold standard of uptime. But today we are going deeper into the threat side. If a government or a malicious actor hijacks BGP to reroute traffic for millions of people, do our fancy encrypted apps like Signal actually protect us?

Herman

That is the million dollar question. Or maybe the billion person question, given how many people rely on those safeguards. To understand if the encryption holds up, we first have to understand exactly what BGP is doing. Most people think of the internet as a direct line from point A to point B. You type in a website, and you go there. But in reality, the internet is not a single network. It is a massive collection of **over ninety thousand** independent networks called Autonomous Systems.

Corn

Right, and these Autonomous Systems, or ASes, have to talk to each other to figure out how to get your data where it needs to go. If I am in Jerusalem and I want to send a message to someone in New York, my data has to hop through multiple different networks owned by different companies and governments. BGP is the language they use to say, hey, I have a path to this destination, send your traffic through me.

Herman

Exactly. It is often called the postal service of the internet. But here is the catch, and this is what Daniel was pointing out. BGP was designed in the late nineteen eighties. Back then, the internet was a much smaller, friendlier place. It was built on trust. When a network says, I am the best route to Google, other networks generally just believe it. There was no built-in way to verify that the network was telling the truth.

Corn

And that is where the BGP hijacking comes in. If a government, let us say the Iranian government as a **hypothetical case study based on past technical maneuvers**, decides they want to see what is happening on the network, they can essentially lie to the rest of the internet. They can announce to the global routing table that their servers are the correct destination for a certain block of IP addresses that they do not actually own.

Herman

That is a BGP hijack. And because of how the protocol works, if their announcement looks more specific or more efficient than the real one, the rest of the internet's routers will start sending traffic to them instead of the actual destination. It is like a rogue construction crew putting up detour signs on a highway that lead everyone into a secret warehouse instead of the city center.

Corn

So, let us get to Daniel's core concern. Imagine this happens on a national scale. Millions of users have their traffic diverted through a government-controlled gateway. If I am using an app like Signal, which uses end-to-end encryption, is my message still safe? Or does that detour give the government the keys to the castle?

Herman

This is where we have to distinguish between the content of the message and the metadata of the connection. Let us start with the good news, which is the content. Signal uses the Double Ratchet Algorithm for end-to-end encryption. When you send a message, it is encrypted on your phone and only decrypted on the recipient’s phone. The servers in the middle, even if they are hijacked, only see scrambled gibberish.

Corn

But wait, Herman. If I am being diverted to a malicious server, couldn't that server pretend to be the Signal server? We call that a man-in-the-middle attack. If the hijacked route leads me to a fake server, couldn't that server try to negotiate a new encryption key with my phone?

Herman

That is a great point, and that is exactly what a sophisticated actor would try to do. They would use the BGP hijack to perform a TLS man-in-the-middle attack. TLS, or Transport Layer Security, is the padlock you see in your browser. It is supposed to prove that you are talking to the real website. In a hijack, the attacker tries to intercept that handshake and give you their own certificate instead of the real one.

Corn

But apps like Signal have a defense against that, right? I remember we discussed this briefly back in episode one hundred eighty-four when we did that deep dive into the OSI model.

Herman

They do. It is called certificate pinning. Most modern, high-security apps do not just trust any certificate that a network gives them. They have the specific identity of the real Signal servers hard-coded into the app. If the app sees a certificate that does not match the one it expects, it will simply refuse to connect. It will show a connection error. So, even if a government hijacks the route via BGP, they cannot easily trick the app into handing over the decrypted content because the app will realize something is wrong and shut down the tunnel.

Corn

Okay, so the content of the message is relatively safe from a BGP hijack because the encryption happens before the data even hits the network, and the app is smart enough to recognize a fake destination. That is a relief. But Daniel also mentioned metadata. That feels like a much bigger vulnerability in this scenario.

Herman

It is a massive vulnerability. Even if they cannot read the message, the BGP hijack tells the interceptor everything else. They can see that your IP address is talking to Signal's IP address. They can see exactly when you are sending messages, how often you are sending them, and the size of the data packets.

Corn

And in a geopolitical context, that metadata can be just as dangerous as the content. If a government is looking for dissidents, they do not necessarily need to know what you said. They just need to know that you are talking to a known activist or that you are using an encrypted app at two in the morning during a period of unrest.

Herman

Exactly. Metadata is the context. It is the who, the when, and the where. If you are a government controlling the BGP routes, you can map out the entire social graph of a movement just by watching the traffic flow. You can see which neighborhoods are the most active and which individuals are the hubs of communication. You are essentially seeing the silhouette of the conversation, even if you cannot hear the words.

Corn

That brings up another point Daniel touched on. If the routing is altered at a macro-network level, it can also lead to what we call blackholing. Instead of just watching the traffic, the government could use BGP to just make the traffic disappear.

Herman

Right. By announcing a route to a destination that leads nowhere, they can effectively cut off specific services for the entire country without actually shutting down the whole internet. They can say, oh, we are still online, but mysteriously, nobody can reach Signal or Telegram or any news site. It is a much more surgical way of censoring information than just pulling the plug on the fiber optic cables.

Corn

It is interesting because it feels like a cat-and-mouse game between network engineers and state actors. We have talked about how BGP is based on trust, but surely the internet community has come up with a way to fix this by now? It is twenty twenty-six, we should have a more secure postal service for our data.

Herman

We are trying, Corn! But it is a slow process. The main solution right now is something called RPKI, or Resource Public Key Infrastructure. Think of it like a digital ID card for BGP. It allows a network owner to cryptographically sign an announcement saying, I am the authorized owner of these IP addresses, and this is the only path you should trust.

Corn

So if everyone used RPKI, a BGP hijack would be impossible because the rogue announcement wouldn't have the right signature?

Herman

In theory, yes. But the adoption is the problem. It is not like a software update you can just push out to everyone. From what we can see in the current data, RPKI adoption is growing, but it is still far from universal. Many networks will still accept unsigned routes because they do not want to risk breaking connectivity for their users. It is a classic trade-off between security and availability.

Corn

It is also a geopolitical issue. If a country wants to maintain the ability to disrupt the internet within its borders, it has very little incentive to adopt a technology that makes that disruption harder to pull off.

Herman

Precisely. This is why we see the internet fragmenting into what some people call the splinternet. You have different regions with different levels of security and different levels of government control. In a place like Iran, which Daniel used as his example, the government has spent years building what they call the National Information Network. It is a domestic version of the internet that they can almost entirely decouple from the global BGP table if they want to.

Corn

That is a terrifying thought. A national intranet where the government is the only router that matters. In that scenario, BGP hijacking isn't even a hijack anymore, it is just the standard operating procedure.

Herman

Right. They own the map, so they decide where the roads go. And if you try to use an encrypted app on that network, they might not be able to read your messages, but they can certainly make your life very difficult by identifying you as someone who is trying to hide something.

Corn

So, what can a regular person do? If Daniel is worried about BGP threats and metadata exposure, are there tools that actually help? I know people always talk about VPNs, but if the BGP route is hijacked, doesn't the VPN traffic get diverted too?

Herman

It does. A VPN is essentially just another tunnel. If the hijack is happening at the ISP level, your encrypted VPN tunnel is still taking that detour. However, a good VPN adds another layer of encryption and another layer of certificate validation. It makes it even harder for the interceptor to perform a man-in-the-middle attack. But again, it does not hide the fact that you are using a VPN. The metadata still shows a connection to a VPN server.

Corn

What about Tor? The Onion Router. That is usually the gold standard for hiding metadata because it bounces your traffic through three different nodes all over the world.

Herman

Tor is much more resilient to BGP hijacks because of its distributed nature. For a government to successfully hijack your Tor traffic, they would have to control or hijack the routes to multiple nodes simultaneously, which is much harder to do. But Tor is slow, and many governments actively block Tor entry nodes. It is a constant battle of technical measures and countermeasures.

Corn

It really highlights how fragile the whole system is. We think of the internet as this robust, decentralized web, but it relies on these very old protocols that were never meant to handle the kind of state-level interference we see today. It is like building a skyscraper on a foundation of wooden stilts.

Herman

That is a perfect analogy. We have built this incredible digital civilization on top of a routing protocol that basically works on the honor system. And while we are slowly replacing those wooden stilts with reinforced concrete through things like RPKI and BGPsec, the transition is taking decades.

Corn

I think one of the most interesting things about Daniel’s prompt is how it forces us to look at the physical reality of the internet. We talk about the cloud and virtual spaces, but at the end of the day, it is all about which router is talking to which other router in a physical data center somewhere.

Herman

Exactly. Geopolitics is back in a big way in the networking world. We are seeing countries treat their IP space and their BGP announcements as a matter of national sovereignty. It is not just a technical challenge anymore, it is a diplomatic one.

Corn

You know, it reminds me of when we talked about the ethical side of things in episode one hundred seventy-nine. Even though that was about sloth tourism, the core idea was about how our actions in a digital or global space have real-world consequences for people on the ground. When a government hijacks a BGP route, they aren't just messing with data, they are potentially putting lives at risk.

Herman

They absolutely are. If you are an activist in a high-risk environment, a BGP hijack could be the precursor to a knock on the door. It is a tool of surveillance and control that is almost entirely invisible to the average user. Most people will just think their internet is a bit slow today, or that an app is glitching, without ever realizing that their entire digital footprint is being diverted through a government server.

Corn

So, to summarize for Daniel and for everyone listening, the short answer is that end-to-end encryption in apps like Signal is incredibly robust against the actual theft of your message content. The math is on your side. Even with a BGP hijack, the attacker cannot easily read your texts.

Herman

But, and this is a big but, the metadata is wide open. A BGP hijack is a master key for seeing who is talking to whom. It allows for sophisticated traffic analysis and targeted censorship. While we are making progress with tools like RPKI, we are still living in a world where the routing of the internet can be manipulated by powerful actors.

Corn

It is a sobering thought, but it is why these discussions are so important. We need to understand the vulnerabilities of the tools we rely on every day. It is not about being paranoid, it is about being informed.

Herman

Well said, Corn. I think we have covered a lot of ground today. From the trust-based origins of BGP to the modern-day risks of metadata exposure and the slow march toward a more secure routing table. It is a complex topic, but it is at the very core of how our world functions in twenty twenty-six.

Corn

It really is. And hey, if you are out there listening and you find this kind of deep dive into the guts of the internet as fascinating as we do, we would love to hear from you. We have been doing this for **over 225 episodes** now, and it is the questions from people like Daniel and the feedback from all of you that keep us digging into these rabbit holes.

Herman

Absolutely. And if you have a moment, a quick review on your podcast app or a rating on Spotify really helps the show reach new people. We are a small, independent operation here in Jerusalem, and every bit of support makes a difference.

Corn

Yeah, it genuinely does. You can find us on Spotify and at our website, myweirdprompts.com. We have the full archive there, including those older episodes we mentioned today if you want to go back and brush up on the OSI model or our previous networking discussions.

Herman

Thanks to Daniel for sending in this prompt. It was a great excuse to geek out on some serious infrastructure.

Corn

Definitely. Alright, I think that is a wrap for today. This has been My Weird Prompts.

Herman

Until next time, stay curious and keep an eye on those routing tables.

Corn

See you next week.

Herman

Take care, everyone. [Rest of banter unchanged as low-impact]