MANRS

Mutually Agreed Norms for Routing Security

Steven Wallace

ssw@internet2.edu

Why Does Routing Security Matter?

A Routing Overview

The Basics: How Routing Works

There are ~70,000 core networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

Border Gateway Protocol (BGP) is based entirely on trust between networks

- Created before security was a concern
- Assumes all networks are trustworthy
- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Routing Incidents Happen Across the Internet

In 2019 alone, over 10,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are attacks; 3.8% of all Autonomous Systems on the Internet were affected.

Incidents are global in scale, with one operator's routing problems cascading to impact others.

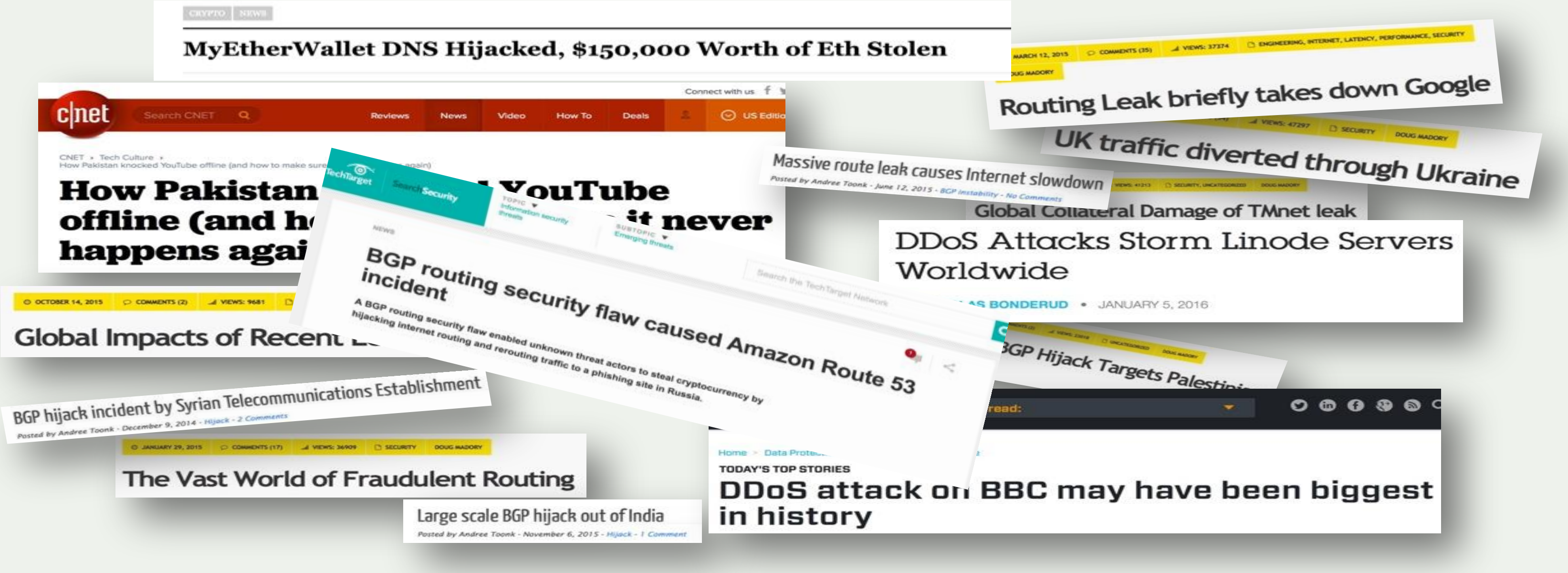
https://www.manrs.org/2019/02/routing-security-getting-better-but-no-reason-to-rest/

Routing Incidents Cause Real World Problems

Insecure routing is one of the most common paths for malicious threats.

Attacks can take anywhere from hours to months to recognize.

Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.



CRYPTO NEWS

MyEtherWallet DNS Hijacked, $150,000 Worth of Eth Stolen

MARCH 12, 2015 · COMMENTS (35) · VIEWS: 37374 · ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY · DOUG MADORY

Routing Leak briefly takes down Google

VIEWS: 47297 · SECURITY · DOUG MADORY

UK traffic diverted through Ukraine

CNET › Tech Culture ›
How Pakistan knocked YouTube offline (and how to make sure ... again)

How Pakistan ... YouTube offline (and h... it never happens agai...

Massive route leak causes Internet slowdown

Posted by Andree Toonk - June 12, 2015 - BGP instability - No Comments

VIEWS: 41213 · SECURITY, UNCATEGORIZED · DOUG MADORY

Global Collateral Damage of TMnet leak

TechTarget SearchSecurity · TOPIC Information security threats · SUBTOPIC Emerging threats

NEWS

BGP routing security flaw caused Amazon Route 53 incident

A BGP routing security flaw enabled unknown threat actors to steal cryptocurrency by hijacking internet routing and rerouting traffic to a phishing site in Russia.

DDoS Attacks Storm Linode Servers Worldwide

...AS BONDERUD • JANUARY 5, 2016

OCTOBER 14, 2015 · COMMENTS (2) · VIEWS: 9681

Global Impacts of Recent L...

...GP Hijack Targets Palestini...

BGP hijack incident by Syrian Telecommunications Establishment

Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments

JANUARY 29, 2015 · COMMENTS (17) · VIEWS: 36909 · SECURITY · DOUG MADORY

The Vast World of Fraudulent Routing

Large scale BGP hijack out of India

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

Home › Data Prote...

TODAY'S TOP STORIES

DDoS attack on BBC may have been biggest in history

What are Routing Incidents?

A Routing Security Overview

The Threats: What's Happening?

Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place; this can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers announces (often due to accidental misconfiguration) to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks.	Source address validation

On March 28th Twitter was hijacked, but few noticed!!!!

RTCOMM-AS (Russian ISP) started originating Twitter’s 104.244.42.0/24 route. Likely an accident, they created a black hole route to disable Twitter for their customers and accidentally leaked it.

Luckily, Twitter has an RPKI ROA for 104.244.42.0/24, and that prevented most networks from accepting RTCOMM-AS’s route to Twitter.

The same thing happened to Google. On February 24th 2008, Pakistan Telecom decided to black hole Google’s traffic locally, but they leaked the route to the Internet and took down Goggle.

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network’s safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS sets a new norm for routing security.

MANRS Actions for Network Operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible, up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data so others can validate

Blue shading = Mandatory Action

Action #1 - Filtering

- Network operator must implement a system whereby they only announce to adjacent networks the AS numbers and IP prefixes they or their customers are legitimately authorised to originate.
- Network operator must check whether the announcements of their customers are correct; specifically, that each customer legitimately holds the AS numbers and IP address space they announce.

Action #1 - Filtering

- To ensure Internet2 accepts routes, the network owner is required to submit a ticket to the Internet2 NOC requesting that the route be accepted.
- Internet2 maintains customer-facing route filters that ensure only authorized routes are accepted.
- There has been a drift over time in terms of what routes are being announced to Internet2 and what are being accepted.
- From time-to-time the billing contact for an IP address or ASN owner might change without ARIN being notified. Invoiced might be neglected, and, ultimately, the number resource is no longer registered. Internet2 is accepting a few ASN in this category today. We're currently working on a policy to address this issue.

Action #2 - Anti-spoofing (recommended, but optional)

- A network operator should implement a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network.
- A network operator must test whether their network is able to send packets with forged source IP addresses using the CAIDA Spoofer Software. This is to alert the network operator as to whether their network might be used to originate Distributed Denial-of-Service (DDoS) attacks, whilst generating publicly accessible information allowing that network to be checked by others.

Action #2 - Anti-spoofing (recommended, but optional)

- Prevented spoof sources addresses (source address validation) mitigates certain types of denial of service attacks.
- Source address validation is most easily done at the campus network level, and becomes increasingly complex as you get closer to the “core” of the Internet. That’s in part why this is a MANRS optional action.
- Unlike other MANRS actions, Internet2 has a very limited ability to detect spoof sources addresses at the backbone level.
- Only 2.4% of Internet2 community networks operate CAIDA Spoofer Software

Action #3 - Coordination

- Network operator must ensure that up-to-date contact information is entered and maintained in the appropriate RIR (or NIR) database and/or in PeeringDB. It is strongly recommended that contact information is made publicly available, but at a minimum must be available to other network operators registered with PeeringDB.

Action #4 - Global Validation

- Network operators must publicly document their intended routing announcements in the appropriate RIR routing registry, RADB or an RADB-mirrored IRR. This includes ASNs and IP prefixes originating on their own networks, as well as the networks for which they provide transit services.
- A network operator may alternatively implement *Action 4: Facilitate routing information on a global scale - RPKI* (defined below) in lieu of a publicly documented routing policy.

Action #4 - Global Validation

A few years ago, Google announced that it would require valid published route policies for all network routes it accepts via peer networks (e.g., Internet2). At the time, most Internet2-connected networks didn’t have comprehensive, accurate published routing policy. Without the policy, traffic from google would need to traverse a organization’s slower Internet Service Provider.

Today we’re in much better shape, but there’s still room for improvement. Hurricane Electric has the most strict requirement for published routing policies, and they continue to reject 20% of Internet2’s routes.

Action #4 - Global Validation

RPKI is emerging as an important tool to improve global validation. Remember the Twitter outage, it was mitigated using RPKI. Over 30% of the routes in the public Internet are protected by RPKI, however only 6% of Internet2 routes use RPKI.

To use RPKI, a network needs to be covered by an ARIN registration services agreement. Over 50% of Internet2 routes are Legacy networks, assigned before ARIN existed.

ARIN also provides an authenticated IRR service for routes under agreement.

Internet2 Route Reports

These are organized by Internet2 Connector. The reports are updated weekly.

they can be found here:

https://github.internet2.edu/ssw/IRR-report/tree/master/Connectors