



Security of Routing Protocols

Tamás Holczer

Laboratory of Cryptography and System Security

Department of Networked Systems and Services

holczer@CrySyS.hu

Outline

- Revision
- Attacker goals and models
- Security of Interior Gateway Protocols
- Security of the BGP
- Case studies

REVISION

Revision

■ Routing

- Running one or more routing algorithms ("processes") to exchange information about the network
- Building and maintaining a Routing Information Base (RIB) during said exchange
- Selecting the *best* path to each network, based on the RIB entries
- Creating and updating the Forwarding Information Base (FIB)

■ Forwarding

- Determining the *best* path for each packet, based on the FIB entries
- Sending the packet to the next hop for the best path

Revision

- Autonomous System (AS)
 - *"An AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy."* – RFC 1930
 - Simplified: a group of networks (prefixes) that are managed together under a single, clearly defined routing policy
- Routing protocol
 - A set of rules that define how and what kind of information is exchanged between routers to build and maintain the RIB

AS Example: BME

```
aut-num:        AS2547
as-name:        BMENET-AS
org:            ORG-BME1-RIPE
descr:          Budapest University of Technology and Economics
import:         from AS1955 accept ANY
export:         to AS1955 announce AS2547
admin-c:        JB19170-RIPE
tech-c:         IOS2-RIPE
tech-c:         GOYA-RIPE
tech-c:         THU-RIPE
status:         LEGACY
mnt-by:         AS2547-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2019-10-16T11:58:50Z
```

AS2547: BME

AS1955: NIIF / KIFÜ

[AS2547 BME](#)

ks

[Home](#)
[Report](#)
[Report](#)
[Report](#)
[Routes](#)

AS Info



Graph v4

Prefixes v4

Peers v4

Whois

IRR

Prefix		Description	
152.66.0.0/16	✓	BME	
152.66.127.0/24	✓	BME	

Updated 25 Apr 2022 13:32 PST © 2022 Hurricane Electric

Revision

- Interior Gateway Protocol – used inside ASes
 - Distance vector
 - » RIP, RIPv2, RIPng, IGRP, EIGRP
 - Link-state
 - » OSPF, OSPFv3, IS-IS
- Exterior Gateway Protocol – used among ASes
 - Path vector
 - » Border Gateway Protocol (BGP)

ATTACKER GOALS & MODELS

Attacker Goals

- Traffic redirection
 - To the attacker (for man-in-the-middle attacks)
 - To black holes (null-routing)

- Denial of service
 - Null-routing
 - Crashing the router
 - Crashing the routing process

Attacker Goals

- Insertion of rogue prefixes
 - Useful for hiding traffic origins
- Intelligence gathering
 - The IP addresses of other routers on the network may be learned
 - » To be attacked
 - » To be used as spoofed source addresses (where applicable)

Attacker Models

- Attacker is not a member of the network
 - Attacking from home...
 - Not much chance of success, unless the network is badly misconfigured
- Attacker is a regular member of the network (e.g. a laptop user)
 - Passive behaviour: attacker may learn the network topology
 - Active behaviour: he may be able to successfully pose as a router and participate in routing message exchanges
 - » All of the previously discussed goals may be reached this way
- Attacker can also alter routing traffic between routers
 - Active behaviour: by inserting, modifying, or dropping messages: all previous goals

SECURITY OF INTERIOR GATEWAY PROTOCOLS

IGP Security – Routing Information Protocol (RIP)

- RIP (RIPv1) (1988, RFC 1058)
 - No authentication
 - Uses UDP (port 520) for transport, no sequence numbering
 - Allows unsolicited advertisements
 - » Very easy to falsify routes (CVE-1999-0111)
- RIPv2 (1993, RFC 1388)
 - Mandatory support for cleartext authentication
 - » Password can be sniffed if the attacker has access to the routing traffic
 - Optional support for keyed MD5 authentication (RFC 2082)
 - » The key is *reasonably difficult* to recover
 - » Prevents tampering with messages
- RIPng (next generation) (1997, RFC 2080)
 - Similar to RIPv2, but supports IPv6

IGP Security – Routing Information Protocol (RIP)

The image shows a Wireshark capture of a RIPv1 response packet. The packet list shows three packets, all of which are RIPv1 responses from 10.0.1.1 to 255.255.255.255. The packet details pane shows the structure of the first packet, which is a Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits). The Ethernet II header shows Src: c2:01:24:b5:00:00 (c2:01:24:b5:00:00) and Dst: Broadcast (ff:ff:ff:ff:ff:ff). The Internet Protocol Version 4 header shows Src: 10.0.1.2 and Dst: 255.255.255.255. The User Datagram Protocol header shows Src Port: 520 and Dst Port: 520. The Routing Information Protocol section shows Command: Response (2), Version: RIPv1 (1), and a list of IP addresses and metrics: IP Address: 10.0.3.0, Metric: 1; IP Address: 10.0.4.0, Metric: 2; IP Address: 192.168.2.0, Metric: 1; and IP Address: 192.168.4.0, Metric: 2. The packet bytes pane shows the raw data of the packet, with the IP address 192.168.4.0 highlighted in blue.

RIPv1.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.1.2	255.255.255.255	RIPv1	126	Response
2	8.995892	10.0.1.1	255.255.255.255	RIPv1	126	Response
3	26.725532	10.0.1.2	255.255.255.255	RIPv1	126	Response

> Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)

> Ethernet II, Src: c2:01:24:b5:00:00 (c2:01:24:b5:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 10.0.1.2, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 520, Dst Port: 520

▼ Routing Information Protocol

- Command: Response (2)
- Version: RIPv1 (1)
- > IP Address: 10.0.3.0, Metric: 1
- > IP Address: 10.0.4.0, Metric: 2
- > IP Address: 192.168.2.0, Metric: 1
- ▼ IP Address: 192.168.4.0, Metric: 2
 - Address Family: IP (2)
 - IP Address: 192.168.4.0
 - Metric: 2

0010 00 70 00 00 00 02 11 ac bc 0a 00 01 02 ff ff .p.....

0020 ff ff 02 08 02 08 00 5c 4b c4 02 01 00 00 02 \ K.....

0030 00 00 0a 00 03 00 00 00 00 00 00 00 00 00

0040 00 01 00 02 00 00 0a 00 04 00 00 00 00 00

0050 00 00 00 00 00 02 00 02 00 00 c0 a8 02 00 00

0060 00 00 00 00 00 00 00 00 01 00 02 00 00 c0 a8

IP Address (rip.ip), 4 byte(s) | Packets: 6 • Displayed: 6 (100.0%) | Profile: Default

IGP Security – Routing Information Protocol (RIP)

Arduino Routing Protocol RIPv1 Spoofer / Network Jammer - Ethernet Shield Tutorial

By andyman5002 in Technology > Arduino  3,357  39  3



Source: <https://www.instructables.com/id/Arduino-Routing-Protocol-RIPv1-Spoofers-Network-Jammer/>

IGP Security – Routing Information Protocol (RIP)

Arduino Routing Protocol RIPv1 Spoofer / Network Jammer - Ethernet Shield Tutorial

By andyman5002 in Technology > Arduino  3,357  39  3

```
void loop()
{
    Udp.beginPacket(broadcast,remotePort);

    memset(packetBuffer, 0, packetSize);
    packetBuffer[0] = 0x02; // RIP command of response
    packetBuffer[1] = 0x01; // RIP v1
    packetBuffer[2] = 0x00; // bytes of padding
    packetBuffer[3] = 0x00;
    packetBuffer[4] = 0x00;
    packetBuffer[5] = 0x02;
    packetBuffer[8] = 0xC0; // first octet of network to spoof C0 = 192
    packetBuffer[23] = 0x00; // metric for the route

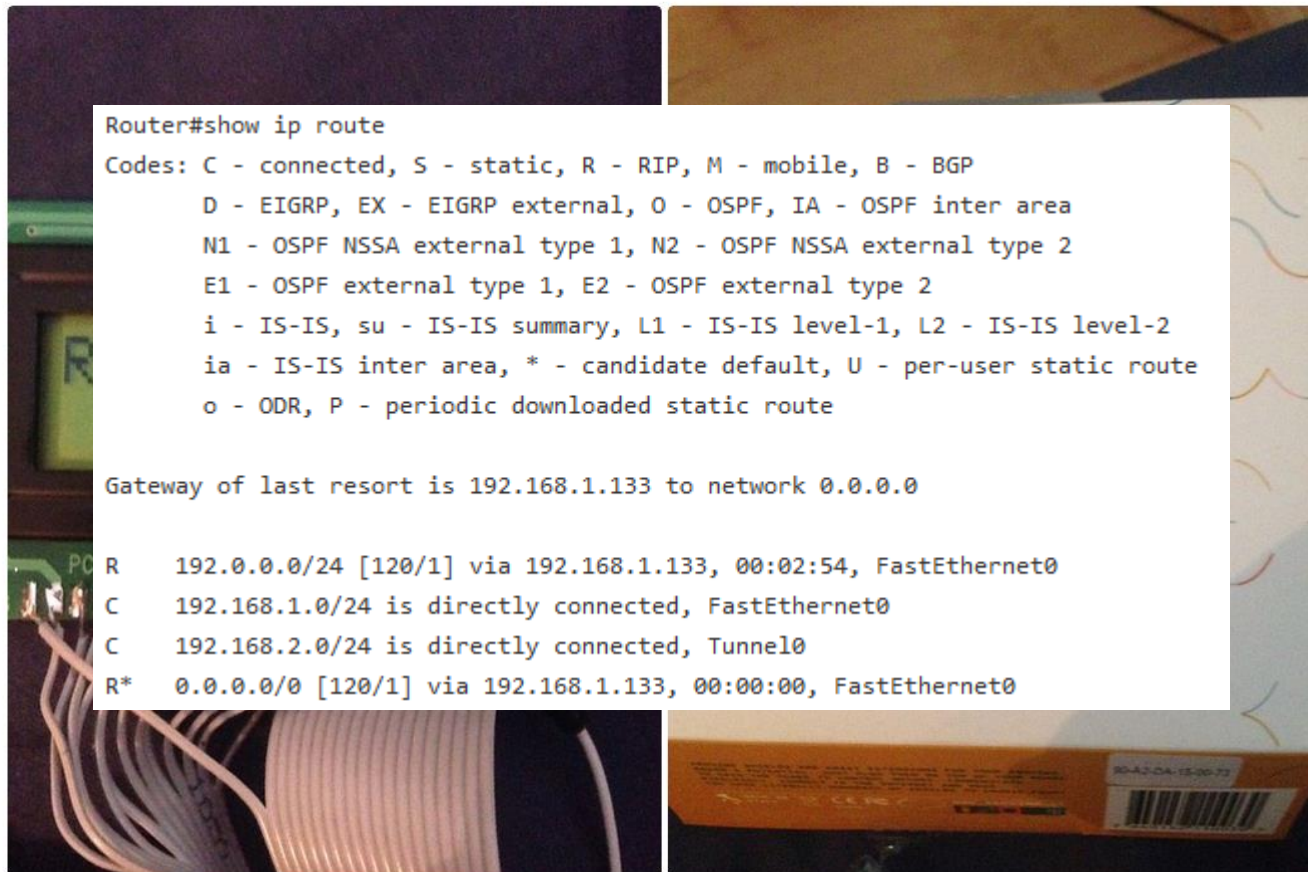
    Udp.write(packetBuffer,packetSize);
    Udp.endPacket();
}
```

Source: <https://www.instructables.com/id/Arduino-Routing-Protocol-RIPv1-Spoofers-Network-Jam/>

IGP Security – Routing Information Protocol (RIP)

Arduino Routing Protocol RIPv1 Spoofer / Network Jammer - Ethernet Shield Tutorial

By andyman5002 in Technology > Arduino  3,357  39  3



Source: <https://www.instructables.com/id/Arduino-Routing-Protocol-RIPv1-Spoofers-Network-Jammer/>

IGP Security – Routing Information Protocol (RIP)

- RIP (RIPv1) (1988, RFC 1058)
 - No authentication
 - Uses UDP (port 520) for transport, no sequence numbering
 - Allows unsolicited advertisements
 - » Very easy to falsify routes (CVE-1999-0111)
- RIPv2 (1993, RFC 1388)
 - Mandatory support for cleartext authentication
 - » Password can be sniffed if the attacker has access to the routing traffic
 - Optional support for keyed MD5 authentication (RFC 2082)
 - » The key is *reasonably difficult* to recover
 - » Prevents tampering with messages
- RIPng (next generation) (1997, RFC 2080)
 - Similar to RIPv2, but supports IPv6

IGP Security – Interior Gateway Routing Protocol

- IGRP (1988, Cisco)
 - From a security point of view, it's the same as RIPv1
 - Obsolete, unsupported

- Enhanced IGRP (EIGRP) (1993, proprietary until 2013, RFC 7868)
 - Optional authentication
 - » Plaintext password
 - » MD5 (later SHA-2) authentication
 - Routers must form an adjacency before route information is exchanged
 - » It is more difficult to spoof routes

IGP Security – Open Shortest Path First, IS-IS

- OSPF (1998, RFC 2328)
 - Authentication options
 - » Null (no authentication)
 - » Clear text
 - » Keyed MD5
 - Routers must form an adjacency before route information is exchanged
 - » It is more difficult to spoof routes
- OSPFv3 (1999, RFC 5340)
 - Supports IPv6
 - Authentication options were removed
 - » Relies on IPSec's AH/ESP for message integrity/confidentiality
- Intermediate System to Intermediate System (1990, RFC 1142)
 - Similar to OSPF from a security point of view

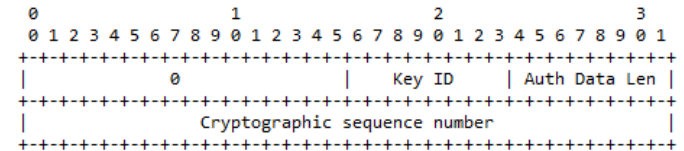


Figure 18: Usage of the Authentication field in the OSPF packet header when Cryptographic Authentication is employed

IGP Security – Best Practices

- Use only routing protocols that support message authentication
 - The default option is always *no authentication* – you have to set it up!
 - Pick the best authentication method that is supported by all of your devices (it should be at least *keyed MD5*, though)
 - This prevents spoofing or tampering with messages as long as the key is not known to the attacker
- Use static neighbours with protocols that support it
 - When neighbours are statically configured, protocols switch to unicast traffic instead of multicast
 - » Makes information gathering more difficult
 - Routers will only form adjacencies with their static neighbours
 - » Makes it reasonably difficult to add rogue routers

IGP Security – Best Practices

- Set client-facing interfaces as *passive* interfaces
 - Passive interface: an interface to which no routing process related messages should be sent
 - » But incoming messages *may* still be processed
 - This prevents adjacencies from being formed on those interfaces (where applicable)
 - » Attacker cannot add a rogue router to the network, even if no auth. is used
 - Default approach
 - » Blocklist (`passive-interface...`)
 - » Allowlist (`passive-interface default` & `no passive-interface ...`)

IGP Security – Food for Thought

- Routing processes are implemented in software...
- Usually in low-level languages such as C or C++...
- Software may contain bugs...
- These typically run with high privileges...

IGP Security – A Case Study – CVE-2005-4436

- *Extended Interior Gateway Routing Protocol (EIGRP) 1.2, as implemented in Cisco IOS after 12.3(2), 12.3(3)B, and 12.3(2)T and other products, allows remote attackers to cause a denial of service by sending a "spoofed neighbor announcement" with (1) mismatched k values or (2) "goodbye message" Type-Length-Value (TLV).*
- *DoS attack*

CVSS Score	7.8
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

Source: <https://www.cvedetails.com/cve/CVE-2005-4436/>

IGP Security – A Case Study – CVE-2017-6770

- *Open Shortest Path First (OSPF) protocol implementations may improperly determine Link State Advertisement (LSA) recency for LSAs with MaxSequenceNumber. According to RFC 2328 section 13.1, for two instances of the same LSA, recency is determined by first comparing sequence numbers, then checksums, and finally MaxAge. In a case where the sequence numbers are the same, the LSA with the larger checksum is considered more recent, and will not be flushed from the Link State Database (LSDB). Since the RFC does not explicitly state that the values of links carried by a LSA must be the same when prematurely aging a self-originating LSA with MaxSequenceNumber, it is possible in vulnerable OSPF implementations for an attacker to craft a LSA with MaxSequenceNumber and invalid links that will result in a larger checksum and thus a 'newer' LSA that will not be flushed from the LSDB. **Propagation of the crafted LSA can result in the erasure or alteration of the routing tables of routers within the routing domain, creating a denial of service condition or the re-routing of traffic on the network.** CVE-2017-3224 has been reserved for Quagga and downstream implementations (SUSE, openSUSE, and Red Hat packages).*
- *Delete/add routes*

Source: <https://www.cvedetails.com/cve/CVE-2017-6770/>

IGP Security – OSPF on CVE

Search Results

There are **52** CVE Records that match your search.

Name	Description
CVE-2022-22169	An Improper Initialization vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an attacker who sends specific packets in certain orders and at specific timings to force OSPFv3 to unexpectedly enter graceful-restart (GR helper mode) even though there is not any Grace-LSA received in OSPFv3 causing a Denial of Service (DoS). Unexpectedly entering GR helper mode might cause the OSPFv3 neighbor adjacency formed on this interface to be stuck in the "INIT" state which can be observed by issuing the following command: user@device> show ospf3 neighbor ID Interface State xx.xx.xx.xx ae100.0 Init <<<<<<<<< An indicator of compromise can be seen in log files when traceoptions for OSPFv3 are enabled before the issue occurs. These logfile messages are as follows: OSPF restart signaling: Received hello with LR bit set from nbr ip=xx::xx id=xx.xx.xx.xx. Set oob-resync capability 1. OSPF Restart Signaling: Start helper mode for nbr ip xx::xx id xx.xx.xx.xx OSPF restart signaling: abort helper mode for nbr ip=xx::xx id=xx.xx.xx.xx OSPF neighbor xx::xx (realm ipv6-unicast <interface.unit> area xx.xx.xx.xx) state changed from Full to Init due to 1WayRcvd (event reason: neighbor is in one-way mode) (nbr helped: 0) This issue affects: Juniper Networks Junos OS. 15.1 versions prior to 15.1R7-S11; 18.3 versions prior to 18.3R3-S6; 18.4 versions prior to 18.4R2-S9, 18.4R3-S10; 19.1 versions prior to 19.1R2-S3, 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S4; 19.3 versions prior to 19.3R2-S7, 19.3R3-S4; 19.4 versions prior to 19.4R3-S6; 20.1 versions prior to 20.1R3-S1; 20.2 versions prior to 20.2R3-S3; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R1-S1, 21.2R2. This issue does not affect any version of Juniper Networks Junos OS 12.3. This issue affects Juniper Networks Junos OS Evolved all versions prior to 21.2R2-EVO.
CVE-2020-5881	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when the BIG-IP Virtual Edition (VE) is configured with VLAN groups and there are devices configured with OSPF connected to it, the Network Device Abstraction Layer (NDAL) Interfaces can lock up and in turn disrupting the communication between the mcpd and tmm processes.
CVE-2020-3528	A vulnerability in the OSPF Version 2 (OSPFv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete input validation when the affected software processes certain OSPFv2 packets

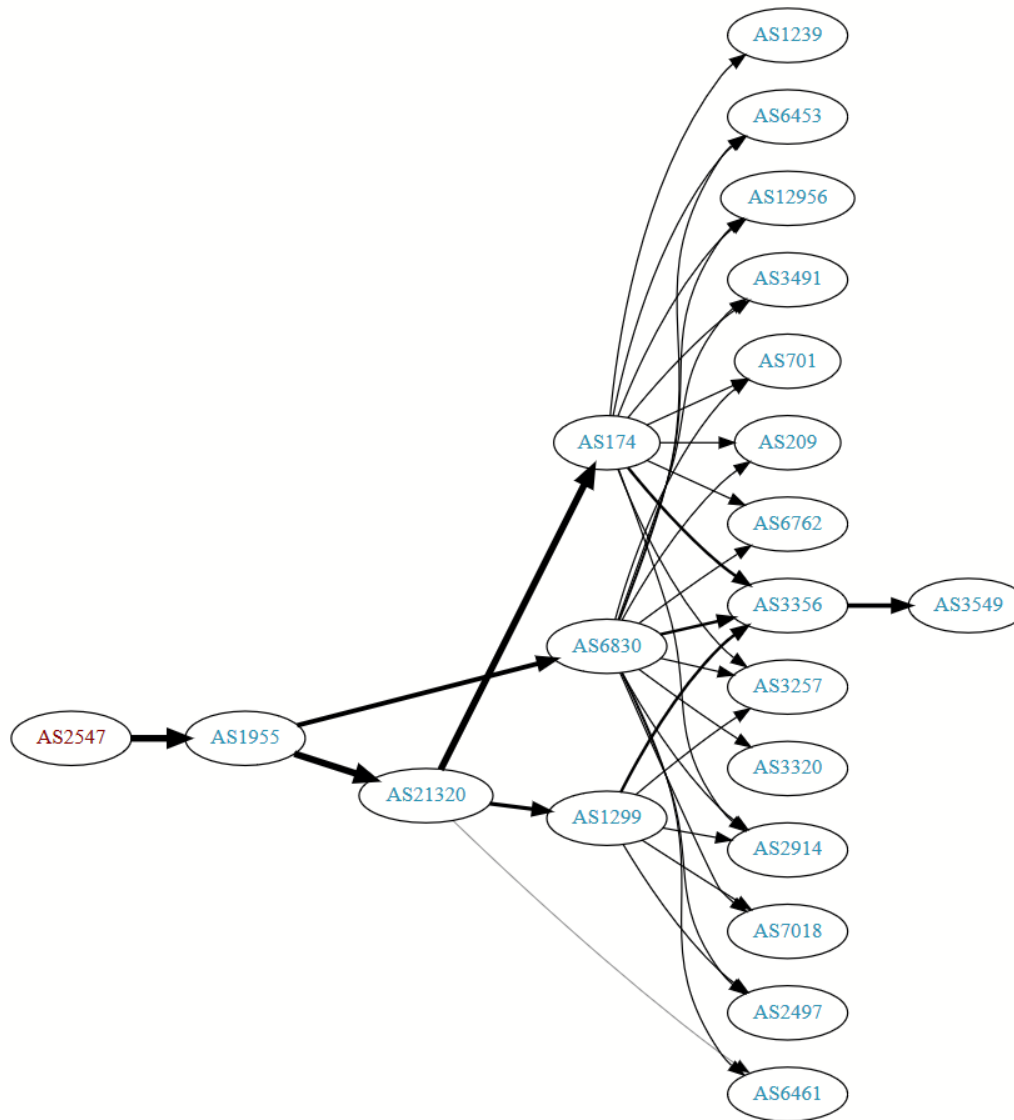
SECURITY OF THE BORDER GATEWAY PROTOCOL

Revision of BGP

- Autonomous Systems announce their AS numbers and prefixes to their neighbours (along with other things not discussed here)
 - E.g. 10 | 198.52.100.0/24
 - Neighbours must be configured manually (no automatic discovery)
- Announcement reason: own network, transit, peering
- Neighbours propagate this information, prepending their own AS numbers to announcements
 - E.g. 20 10 | 198.52.100.0/24
- There may be multiple paths to a prefix
 - Shortest path *may* be chosen (behaviour can be customized and can depend on several other factors)
- A more specific path is always preferred over a less specific one
- BGP uses TCP (port 179) for transport

Revision of BGP

- Autonomous
to their ne
– E.g. 10
– Neighb
- Neighbou
AS numbe
– E.g. 201
- There ma
– Shortes
depend
- A more sp
- BGP uses



and prefixes
discussed here)

discovery)
their own

ed and can

specific one

Revision of BGP

- Autonomous Systems announce their AS numbers and prefixes to their neighbours (along with other things not discussed here)
 - E.g. 10 | 198.52.100.0/24
 - Neighbours must be configured manually (no automatic discovery)
- Neighbours propagate this information, prepending their own AS numbers to announcements
 - E.g. 20 10 | 198.52.100.0/24
- There may be multiple paths to a prefix
 - Shortest path *may* be chosen (behaviour can be customized and can depend on several other factors)
- A more specific path is always preferred over a less specific one
- BGP uses TCP (port 179) for transport

BGP Security

- BGP supports message authentication
 - Keyed MD5 should be supported in general
 - Vendors may offer alternative options (e.g. HMAC-SHA1)
 - This only prevents messages from being modified in transit
- Adding a rogue router is reasonably difficult
 - The other party needs to be configured manually for the new neighbour
- Spoofing a BGP session is also reasonably difficult
 - The attacker would have to complete the three-way TCP handshake
 - Even if that worked, he would have to know the key (if auth. is used)

BGP Security

- The contents of the messages (i.e. the announced prefixes) are rarely validated
 - An attacker having access to a compromised router may announce arbitrary prefixes
 - The attacker may deaggregate a prefix and announce it by parts
 - Since a deaggregated prefix is more specific, it will be preferred over the legitimate announcement
 - » This can be leveraged for a man-in-the-middle attack
- Prefixes smaller than /24s are usually ignored (limited memory)
 - Announcing prefixes in /24s makes them harder to hijack since the attacker would have to deaggregate them into two /25s (or smaller parts)
 - This behaviour can be exploited for defense (e.g. if an attacker hijacks a /23, I can announce it as two /24s, which he can't further announce as four /25s ...)

CASE STUDIES

BGP Case Study – Pakistan Telecom

- 2008-02-24, a trailer of an anti-Islamic film makes it to YouTube
- The Pakistani government orders blocking of YouTube
 - YouTube's prefix is 208.65.152.0/22 at that time
- At 18:47, Pakistan Telecom (PT from now on) starts announcing a route for 208.65.153.0/24 to PCCW (PT's provider)
 - It is unclear why they only picked this subnet, but later evidence suggests that youtube.com was only being served from IP addresses from this range
 - » PT might have thought that this was all of YouTube's addresses
 - This was meant to be a null-route to be propagated downstream
 - Seems like the guy who set this up forgot to set the upstream filter
- From PCCW, the route gets propagated to the internet
 - PCCW did not check whether PT had the right to announce this prefix

BGP Case Study – Pakistan Telecom

- Since the /24 is more specific than the /22, everyone attempting to reach YouTube attempts to do so via PT
 - Remember, youtube.com was only being served from servers from the /24
 - Traffic is null-routed -> YouTube appears to be down
- At 20:07, YouTube starts announcing the /24
 - There are now two ASes announcing the same prefix, the usual rules apply (shorter paths are preferred)
 - » Those who are closer to PT will still try to reach YouTube via PT
- At 20:07, YouTube starts announcing the /24 as two /25s as well
 - Small prefixes were not typically dropped in 2008, so this worked

BGP Case Study – Pakistan Telecom

- 20:51, PCCW changes route advertisements to include PT's AS number multiple times
 - This makes it seem a longer path -> will be chosen less often
- 21:01, the unauthorized announcements are no longer propagated by PCCW
- The route hijacking (towards the internet) was probably not intended
- Visualization: <https://www.youtube.com/watch?v=IzLPKuAOe50>

BGP Case Study – Data Siphoning

KIM ZETTER SECURITY 12.05.13 06:30 AM

SOMEONE'S BEEN SIPHONING DATA THROUGH A HUGE SECURITY HOLE IN THE INTERNET

Earlier this year, researchers say, someone mysteriously hijacked internet traffic headed to government agencies, corporate offices and other recipients in the U.S. and elsewhere and redirected it to Belarus and Iceland, before sending it on its way to its legitimate destinations. They did so repeatedly over several months. But luckily someone did notice.

The attackers initiated the hijacks at least 38 times, grabbing traffic from about 1,500 individual IP blocks – sometimes for minutes, other times for days – and they did it in such a way that, researchers say, it couldn't have been a mistake.

Analysts at Renesys, a network monitoring firm, said that over several months earlier this year someone diverted the traffic using the same vulnerability in the so-called Border Gateway Protocol, or BGP, that the two security researchers demonstrated in 2008. The BGP attack, a version of the classic man-in-the-middle exploit, allows hijackers to fool other routers into re-directing data to a system they control. When they finally send it to its correct destination, neither the sender nor recipient is aware that their data has made an unscheduled stop.

Source: <https://www.wired.com/2013/12/bgp-hijacking-belarus-iceland/>

BGP Case Study – DDoS Against GitHub

- 2018-02-28, 17:21: a huge DDoS attack hits GitHub
 - ~1,3 Tbps, the largest DDoS in history so far
- GitHub is unavailable until 17:26
 - Intermittent downtimes between 17:26 and 17:30
 - Less than 10 minutes!
- GitHub called for help from Akamai Prolexic
 - Prolexic used BGP route hijacking to route all GitHub traffic to them
 - They are big enough to withstand such an attack
 - They filtered bad traffic, then forwarded good traffic to GitHub via an alternative route
- A benign use of route hijacking!

BGP Case Study – MyEtherWallet Hijacking

6,789 views | Apr 24, 2018, 02:10pm

A \$152,000 Cryptocurrency Theft Just Exploited A Huge 'Blind Spot' In Internet Security



Thomas Brewster Forbes Staff

Security

I cover crime, privacy and security in digital and physical forms.



Ether has been the target of repeated hacks. Now one has abused a core part of internet infrastructure. (Photo by Jaap Arriens/NurPhoto via Getty Images)

Source: <https://www.forbes.com/sites/thomasbrewster/2018/04/24/a-160000-ether-theft-just-exploited-a-massive-blind-spot-in-internet-security/>

The Register
Biting the hand that feeds IT



DATA CENTRE

SOFTWARE

SECURITY

DEVOPS

BUSINESS

PERSONAL TECH

SCIENCE

EMERGE

Security

AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet

Audacious BGP seizure of Route 53 IP addys followed by crypto-cyber-heist

By Shaun Nichols in San Francisco 24 Apr 2018 at 19:04

42



Updated Crooks today hijacked internet connections to Amazon Web Services systems to ultimately steal a chunk of alt-coins from online cryptocurrency website MyEtherWallet.com.

Source: https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

BGP Case Study – Google (Again)

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

THE ACCIDENTAL LEAK —

Google goes down after major BGP mishap routes traffic through China

Google says it doesn't believe leak was malicious despite suspicious appearances.

DAN GOODIN - 11/13/2018, 8:25 AM



byjshardow

Enlarge

The leak started at 21:13 UTC when **MainOne Cable Company**, a small ISP in Lagos, Nigeria, suddenly updated tables in the Internet's global routing system to improperly declare that its **autonomous system 37282** was the proper path to reach **212 IP prefixes belonging to Google**. Within minutes, China Telecom improperly accepted the route and announced it worldwide. The move by China Telecom, aka AS4809, in turn caused Russia-based **Transtelecom**, aka AS20485, and other large service providers to also follow the route.

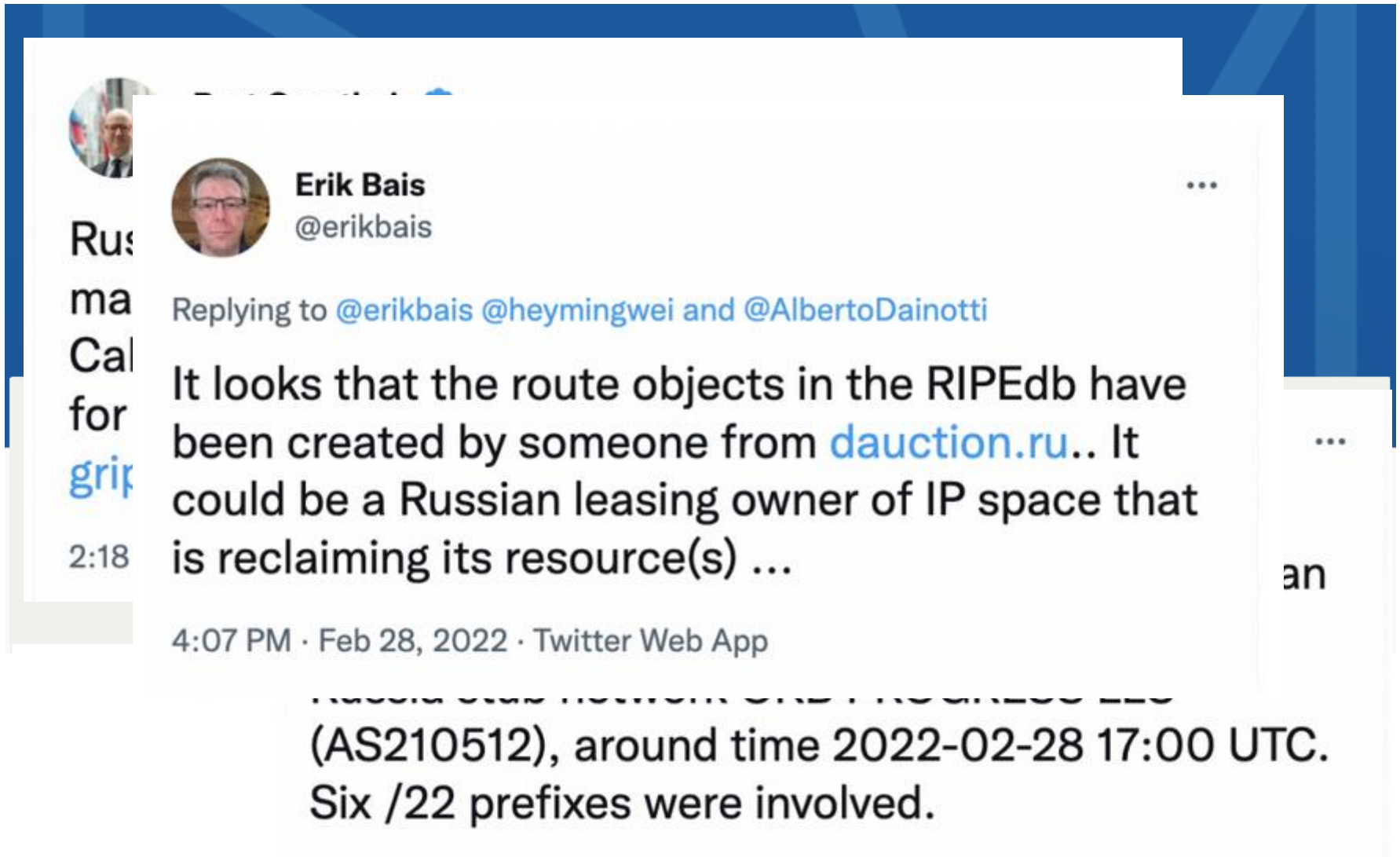


FURTHER READING

Strange snafu misroutes domestic US Internet traffic through China Telecom


Source: <https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/>

BGP Case Study – Ukraine 2022?



The image is a screenshot of a Twitter thread. The top tweet is from Erik Bais (@erikbais), replying to @erikbais, @heymingwei, and @AlbertoDainotti. The tweet text reads: "It looks that the route objects in the RIPEdb have been created by someone from dauction.ru.. It could be a Russian leasing owner of IP space that is reclaiming its resource(s) ...". The tweet is timestamped "4:07 PM · Feb 28, 2022 · Twitter Web App". Below this, a second tweet is partially visible, mentioning "(AS210512), around time 2022-02-28 17:00 UTC. Six /22 prefixes were involved."

Rus
ma
Cal
for
grip
2:18

 **Erik Bais**
@erikbais

Replying to @erikbais @heymingwei and @AlbertoDainotti

It looks that the route objects in the RIPEdb have been created by someone from dauction.ru.. It could be a Russian leasing owner of IP space that is reclaiming its resource(s) ...

4:07 PM · Feb 28, 2022 · Twitter Web App

...
an

...
(AS210512), around time 2022-02-28 17:00 UTC.
Six /22 prefixes were involved.

BGP Case Study – CVE

Insecure by nature, but vulnerabilities are common as well...

Search Results

There are **153** CVE Records that match your search.

Name	Description
CVE-2022-23046	PhpIPAM v1.4.4 allows an authenticated admin user to inject SQL sentences in the "subnet" parameter while searching a subnet via app/admin/routing/edit-bgp-mapping-search.php
CVE-2022-22197	An Operation on a Resource after Expiration or Release vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker with an established BGP session to cause a Denial of Service (DoS). This issue occurs when proxy-generate route-target filtering is enabled, and certain proxy-route add and delete events are happening. This issue affects: Juniper Networks Junos OS All versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R1-S2, 20.3R2. Juniper Networks Junos OS Evolved All versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R3-EVO; 20.3 versions prior to 20.3R2-EVO.
CVE-2022-22193	An Improper Handling of Unexpected Data Type vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). Continued execution of this command might cause a sustained Denial of Service condition. If BGP rib sharding is configured and a certain CLI command is executed the rpd process can crash. During the rpd crash and restart, the routing protocols might be impacted and traffic disruption might be seen due to the loss of routing information. This issue affects: Juniper Networks Junos OS 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R2. Juniper Networks Junos OS Evolved 20.4 versions prior to 20.4R3-EVO; 21.1 versions prior to 21.1R3-EVO; 21.2 versions prior to 21.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 20.3R1. Juniper Networks Junos OS Evolved versions prior to 20.3R1-EVO.
CVE-2022-22166	An Improper Validation of Specified Quantity in Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks

SECURITY OF THE BORDER GATEWAY PROTOCOL (CONT'D)

BGP Security – Defending Against Attacks

- Route monitoring
 - Route Views
 - » Project by the University of Oregon
 - » Lets you view routing information from different parts of the world
 - Looking Glass
 - » ISPs may let you check what paths they see to a given prefix
 - » For example: <https://us.ntt.net/support/looking-glass/>
 - There are companies that offer services for continuously analysing announcements and alerting you when anomalies are detected
 - This is reactive, not preventive (i.e. when you see it, it's already too late)

BGP Security – Defending Against Attacks – Looking Glass

Router:

-- select a router --

- Osaka - JP
- Seoul - KR
- Singapore - SG
- Taipei - TW
- Tokyo - JP

Europe

- Amsterdam - NL
- Barcelona - ES
- Berlin - DE
- Brussels - BE
- Bucharest - RO
- Budapest - HU**
- Düsseldorf - DE
- Frankfurt - DE
- London - GB
- Luxembourg City - LU
- Madrid - ES
- Marseille - FR
- Milan - IT
- Paris - FR

Router:

Budapest - HU

Query:

BGP

IP Address:

- ☐ Your current IP Address: [REDACTED]
- ☒ Specify an IP Address (IPv4 or IPv6)

Only IP addresses are allowed parameters for BGP Queries. FQDN can not be used.

Submit

Reset

BGP Security – Defending Against Attacks – Looking Glass

Query Results:

Router: Budapest - HU

Command: show bgp ipv4 unicast 152.66.208.14

BGP routing table entry for 152.66.0.0/16

Versions:

Process	bRIB/RIB	SendTblVer
Speaker	174386164	174386164

Last Modified: Feb 16 09:24:34.150 for 3w4d

Paths: (25 available, best #19)

Advertised to update-groups (with more than one peer):

0.5 0.7

Advertised to peers (in unique update groups):

83.217.233.14

Path #1: Received by speaker 0

Not advertised to any peer

174 21320 1955 2547

154.54.9.41 (metric 25932) from

Origin IGP, metric 429496729

Received Path ID 0, Local Path

Community: 2914:390 2914:100

Path #2: Received by speaker 0

Not advertised to any peer

174 21320 1955 2547

154.54.11.237 (metric 24848) from (129.250.0.20)

Origin IGP, metric 4294967294, localpref 100, valid, confed-internal

Received Path ID 0, Local Path ID 0, version 0

Community: 2914:390 2914:1011 2914:2000 2914:3000 65504:174

Path #3: Received by speaker 0

Path #19: Received by speaker 0

Advertised to update-groups (with more than one peer):

0.5 0.7

Advertised to peers (in unique update groups):

83.217.233.14

174 21320 1955 2547

130.117.14.129 (metric 8038) from (129.250.0.166)

Origin IGP, metric 4294967294, localpref 100, valid, confed-internal, best, group-best

Received Path ID 0, Local Path ID 0, version 174386164

Community: 2914:395 2914:1201 2914:2202 2914:3200 65504:174

BGP Security – Defending Against Attacks

- Filtering incoming announcements
 - ASes may publish their prefixes in Internet Route Registries
 - Neighbours may set up filters to ignore announcements for unlisted prefixes
 - Challenges
 - » This list has to be kept up-to-date
 - » Not suitable for ASes with often-changing lists of prefixes
 - » < 50% adoption in 2009

BGP Security – Defending Against Attacks

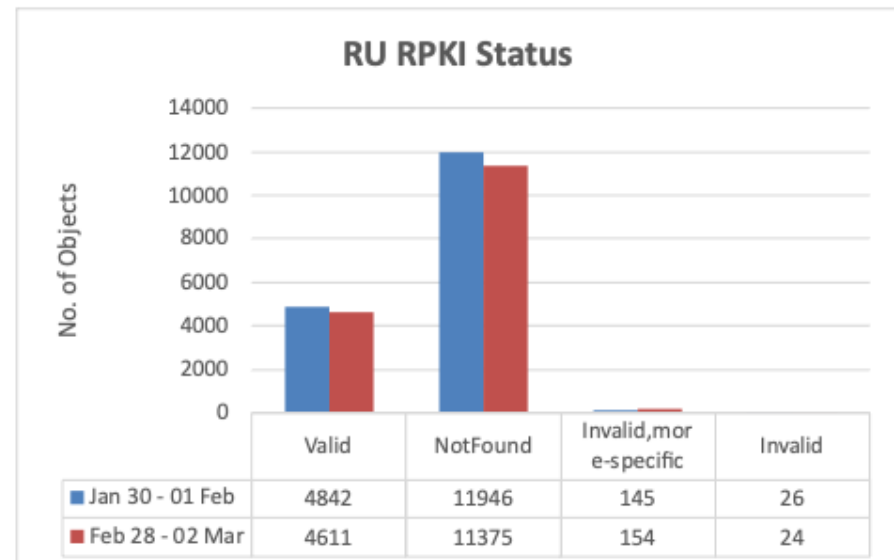
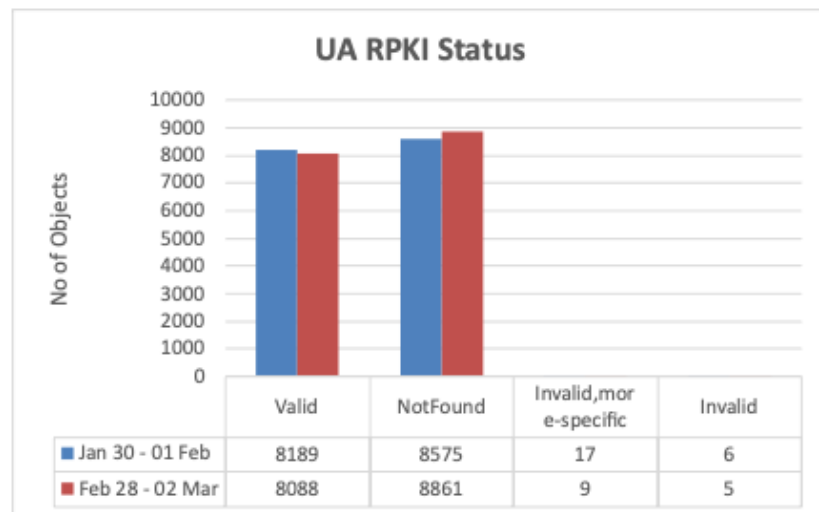
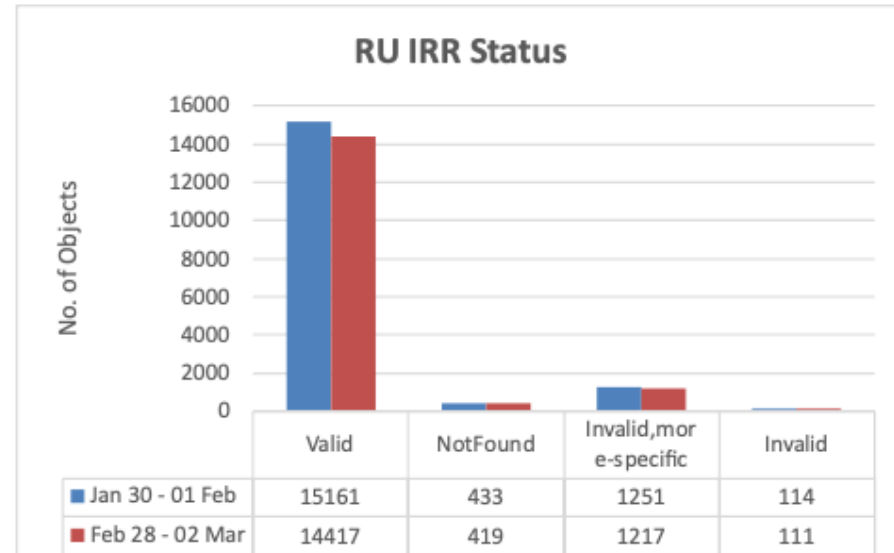
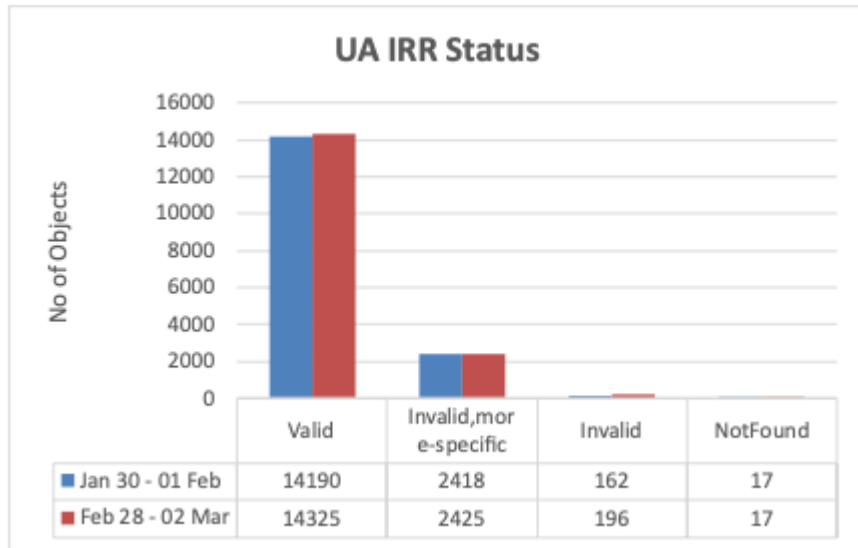
- Secure BGP (S-BGP) – 2000(!)
 - Builds on PKI
 - » Address Attestations – prefix owner authorizes an AS to originate it
 - » Route Attestations – AS authorizes a neighbour to advertise prefixes
 - Employs IPSec between routers
 - Was not really adopted

- Secure Origin BGP (soBGP) – 2003
 - Builds on PKI, but without central authorities (i.e. Web-of-Trust model)
 - » A peer announcing a prefix should have at least one valid path to it
 - Less resource-intensive
 - Also was not adopted

BGP Security – Defending Against Attacks

- Resource Public Key Infrastructure (RPKI) – 2012
 - Relies on PKI
 - RIRs can sign ASN+IP pairs
 - » Route Origin Authorization (ROA)
 - ROA distribution and validation logic is decoupled from the routers
 - There is no path validation, only origin validation
 - Backed by some big providers (e.g. CloudFlare)
 - Supported by major networking vendors (e.g. Cisco, Juniper)
 - May be the future?
 - » ~9% adoption in Sep 2018 (worldwide), ~16% in Europe
 - » ~17% adoption in Sep 2020 (worldwide), ~40% in Europe

BGP Security – IRR and RPKI adoption during a war



MISCELLANEOUS

Control Questions

- When attacking routing protocols, what goals may an attacker have?
- Considering routing protocols, what are the two typical attacker models?
- Talking about routing protocols, name an action that a passive attacker may perform, and two that an active attacker may take.
- From a security point of view, what was the problem with early routing protocols such as RIPv1 and IGRP?
- What typical authentication methods are supported by modern IGP routing protocols?
- What is a passive interface, why are they important for security?
- Why is it considered reasonably difficult to spoof a BGP session?
- If you were to hijack 198.52.100.0/24, would you announce it as is, or would you deaggregate it first? Why?
- What kind of countermeasures are there against BGP hijacking?
- Name a scenario where BGP route hijacking is beneficial for the owner of the prefix.

Further Reading, Sources

- Chris Russel: Security of IP Routing Protocols
- Security Sage's Guide to Hardening the Network Infrastructure
- Secure Border Gateway Protocol (S-BGP) - IEEE Journals & Magazine
- Dyn.com: Pakistan hijacks YouTube
 - <https://dyn.com/blog/pakistan-hijacks-youtube-1/>
- RIPE NCC: YouTube Hijacking: A RIPE NCC RIS case study
 - <https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>
- GitHub Engineering: February 28th DDoS Incident Report
 - <https://githubengineering.com/ddos-incident-report/>

THANK YOU FOR YOUR ATTENTION!