



UNIVERSITY
OF TRENTO - Italy




Offensive technologies Fall 2017


BGP or Internet Traffic Across Borders
Fabio Massacci
(Some slides courtesy of Jelena Mirkovic and Jen Rexford)

https://securitylab.disi.unitn.it/doku.php?id=course_on_offensive_technologies

24/10/17 Offensive Technologies - Fabio Massacci 1




UNIVERSITY
OF TRENTO - Italy




Last Slide of Last Lecture

- ***What are the features of Internet?***
 - No need of
 - validating IP source address
 - enforcing amount of resources requested
 - tracking traffic flows
 - Or tracking those controlling traffic flows
 - assigning responsibility for packets or packet streams
 - determining who accessed a machine
 - BUT no need = no way
 - because nobody is going an extra mail if it ain't needed
 - In good and in bad fortune...

24/10/17 Offensive Technologies - Fabio Massacci 2




UNIVERSITY OF TRENTO - Italy




Questions

- **How many (people using) different internet providers are in this room?**
 -
- **How do they talk to each other?**
 - Eg how do I send packets
 - from www.massacci.org
 - to www.timinternet.it
 - The DNS only resolves names to IPs then I have to connect IPs to each other

24/10/17 Offensive Technologies - Fabio Massacci 3



UNIVERSITY OF TRENTO - Italy



How the Internet Really Works

- **AS-level (autonomous system)**
 - Collection of networks under single administrative organization
- **Relationships (usually private info)**
 - Customer/provider (customers pay to providers)
 - Peer-to-peer (peers do not pay each other)
- **Host Several "Domains"**
 - Both within the same mother organization
 - Eg Google & Youtube
 - Or for different administrative entities
 - E.g. Individual customers
- **Possibly share the physical infrastructure**

24/10/17 Offensive Technologies - Fabio Massacci 4




UNIVERSITY OF TRENTO - Italy




Top 10 AS in the World

Nat.	Autonomous System	Number of "Owned" IPs
US	AS26496 GoDaddy.com, LLC	38,836,692
DE	AS8560 1&1 Internet SE	5,570,753
US	AS14618 Amazon.com, Inc.	5,377,432
US	AS15169 Google LLC	4,827,056
BVI	AS40034 Confluence Networks Inc	4,282,990
US	AS46606 Unified Layer	3,889,172
FR	AS16276 OVH SAS	3,442,272
US	AS29873 The Endurance International Group, Inc.	2,711,863
US	AS16509 Amazon.com, Inc.	2,639,930
US	AS13335 Cloudflare, Inc.	2,325,654

24/10/17 Offensive Technologies - Fabio Massacci 5




UNIVERSITY OF TRENTO - Italy




Endurance – WHOIS Record

- **ASHandle: AS29873**
- **OrgID: EIG-12**
- **ASName: BIZLAND-SD**
- **ASNumber: 29873**
- **RegDate: 2003-05-23**
- **Updated: 2012-03-02**
- **Source: ARIN**
- **OrgID: EIG-12**
- **OrgName: The Endurance International Group, Inc.**
- **CanAllocate:**
- **Street: 10 Corporate Drive**
- **Street: Suite 300**
- **City: Burlington**
- **State/Prov: MA Country: US**
- **PostalCode: 01803**
- **RegDate: 2005-02-07**
- **Updated: 2017-01-28**
- **OrgTechHandle:**
- **EIGAR-ARIN**
- **OrgAdminHandle: EIGAR-ARIN**
- **OrgAbuseHandle: EIGAB-ARIN**
- **OrgNOCHandle: ENO91-ARIN**
- **Source: ARIN**

24/10/17 Offensive Technologies - Fabio Massacci 6



UNIVERSITY OF TRENTO - Italy



Endurance, Top 10 Domains

IP Address	Domain	Domains on this IP Address
207.148.248.143	balisculpture.com	880,868
66.96.149.1	athenstk.com	274,150
66.96.149.32	americanbedrock.com	265,434
207.148.248.145	grocerymadness.com	113,350
65.254.227.224	britmerican.com	109,836
65.254.227.240	conniegilbert.com	102,858
66.96.149.22	hawaiiibrad.com	29,796
66.96.149.31	bourbonwine.com	27,161
66.96.149.30	gmfurs.com	23,305
207.148.248.144	besttrafficbuilder.com	22,064

24/10/17 Offensive Technologies - Fabio Massacci 7



UNIVERSITY OF TRENTO - Italy






Endurance, Some IP ranges

IP Range	Owner	IP Addresses
143.95.160.0/23	Athenix Inc.	512
206.125.208.0/20	The Endurance International Group, Inc.	4,096
207.148.224.0/24	The Endurance International Group, Inc.	256
38.113.1.0/24	PSINet, Inc.	256
50.201.183.0/24	Comcast Cable Communications, LLC	256
64.150.160.0/23	iPower, Inc.	512
66.242.16.0/20	The Endurance International Group, Inc.	4,096
66.249.0.0/19	The Endurance International Group, Inc.	8,192
66.96.128.0/18	The Endurance International Group, Inc.	16,384
67.223.224.0/19	The Endurance International Group, Inc.	8,192

24/10/17 Offensive Technologies - Fabio Massacci 8

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Example: American Bedrock

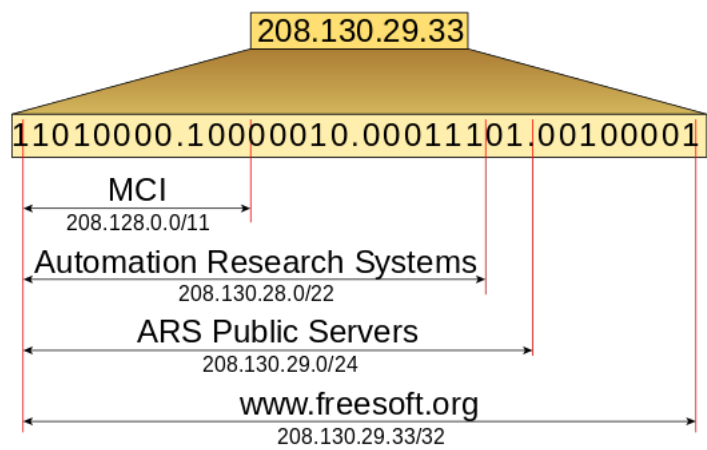
- **Endurance Range (66.96.128.0/18)**
- **0100.0010 . 0110.0000 . 1000.0000 . 0000.0000**
- **66 . 96 . 128 . 0 / 18**
- **18 bits** 
- **American Bedrock Domain (66.96.149.0)**
- **0100.0010 . 0110.0000 . 1001.0101 . 0010.0000**
- **66 . 96 . 149 . 0**
- **18+ bits**  

24/10/17 Offensive Technologies - Fabio Massacci 9

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Graphically

208.130.29.33



- **By Fred the Oysteri (Wikipedia)**

24/10/17 Offensive Technologies - Fabio Massacci 10

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Top 10 ASes in Italy

AS	Autonomous System	"Owned" IPs
AS3269	Telecom Italia S.p.a.	19,468,814
AS1267	Wind Telecomunicazioni SpA	6,110,720
AS30722	Vodafone Italia S.p.A.	5,051,648
AS12874	Fastweb SpA	3,577,600
AS137	Consortium GARR	2,769,408
AS24608	WINDTRE s.p.a	2,171,136
AS16232	TELECOM ITALIA SPA	1,777,664
AS8612	Tiscali Italia S.P.A.	1,432,320
AS20959	Telecom Italia S.p.A.	1,310,720
AS8968	BT Italia S.p.A.	891,392

UNITN's IPs are here


24/10/17 Offensive Technologies - Fabio Massacci 11

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


How do ASes know where to send?

- **Border Gateway Protocol**
- **Routers from neighbor ASes exchange periodic updates using TCP sessions**
 - BGP speakers send a 19-bytes keep-alive message every 60sec
 - If TCP session dies (e.g., RST) or HELLO messages are absent assume all routes announced by neighbor are not valid anymore
 - Withdraw your announcements of those routes
 - Creates a rippling effect in the Internet
- **Full Mesh → each router must be configured as peer to every other router.**
 - Scaling problems → the number of connections scales quadratically
- **Alternatives consider the hierarchical nature of ASes**
 - Route Reflectors
 - BGP confederations

24/10/17 Offensive Technologies - Fabio Massacci 12




UNIVERSITY
OF TRENTO - Italy




Announcing Routes

- ***Each AS announces routes it knows including entire AS path to the destination***
 - All routes announced to customers and providers
 - Customer routes announced to peers
- ***Each AS can choose which routes to adopt***
 - Short routes
 - Specific routes (longest matching prefix)
 - Preference given to
 1. customer routes
 2. peers,
 3. Providers

24/10/17 Offensive Technologies - Fabio Massacci 13



UNIVERSITY
OF TRENTO - Italy



BGP prefix (sub)hijacking

- ***An AS announces itself***
 - As origin of a prefix it doesn't own
 - As being close to the origin of a prefix
- ***Attracts the prefix's traffic***
 - Can drop it (blackholing)
 - Can reroute it to prefix (interception)

24/10/17 Offensive Technologies - Fabio Massacci 14

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Prefix Hijacking

- **Originating someone else's prefix**
 - What fraction of the Internet believes it?

The diagram shows a network of seven Autonomous Systems (ASes) represented as clouds, numbered 1 through 7. AS 1 is at the bottom left, AS 2 is above it, AS 3 is to the right of AS 2, AS 4 is to the right of AS 3, AS 7 is below AS 4, AS 5 is to the right of AS 7, and AS 6 is to the right of AS 5. A red arrow points from AS 1 to AS 2, and another red arrow points from AS 2 to AS 3. A green arrow points from AS 3 to AS 4, and another green arrow points from AS 4 to AS 7. A green arrow points from AS 7 to AS 5, and another green arrow points from AS 5 to AS 6. A green arrow points from AS 6 to AS 1, forming a loop. A red arrow points from AS 1 to AS 3. A green arrow points from AS 6 to AS 1. The prefix 12.34.0.0/16 is shown in red text near AS 1 and in green text near AS 6.

24/10/17 12.34.0.0/16 15
Offensive Technologies - Fabio Massacci

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Sub-Prefix Hijacking

- **Originating a more-specific prefix**
 - Every AS picks the bogus route for that prefix
 - Traffic follows the longest matching prefix

The diagram shows the same network of seven Autonomous Systems (ASes) as in the previous slide. A red arrow points from AS 1 to AS 2, and another red arrow points from AS 2 to AS 3. A green arrow points from AS 3 to AS 4, and another green arrow points from AS 4 to AS 7. A green arrow points from AS 7 to AS 5, and another green arrow points from AS 5 to AS 6. A green arrow points from AS 6 to AS 1, forming a loop. A red arrow points from AS 1 to AS 3. A green arrow points from AS 6 to AS 1. The prefix 12.34.158.0/24 is shown in red text near AS 1 and in green text near AS 6.

24/10/17 12.34.158.0/24 16
Offensive Technologies - Fabio Massacci

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

What is really happening

- **From 7's Perspective → BOTH routes co-exist**
 - Send to 12.34.100.5? → Matches 6 and nothing else → send it to 6
 - Send to 12.34.158.1? → Matches 1 & 6 but 1's prefix is longer → 1 more specific → send to 1
 - This is very, very resilient!


24/10/17 Offensive Technologies - Fabio Massacci 17

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Why is hijacking hard to handle?


- **Malicious routes do not propagate to source**
 - Source cannot observe the problem easily
- **Even if source can observe problem, fix is hard**
 - No automatic fix – source's announcements count as much as anyone else's once they leave the source
 - Must go through human channels
- **Interception attacks are very hard to detect**
- **Source of attacks is not just maliciousness – often it is misconfiguration**

24/10/17 Offensive Technologies - Fabio Massacci 18




UNIVERSITY OF TRENTO - Italy

Beyond The Network America, Inc. (now PCCW Global, Inc.)




AS number:	3491
AS name:	BTN-ASN
Org name:	Beyond The Network America, Inc.
AS rank:	17
Country:	US
Customer cone size:	3,572
AS transit degree:	547
	Providers 2
	Peers 197
	Customers 461
	Siblings 1
Type:	Transit/Access

24/10/17
Offensive Technologies - Fabio Massacci
19



UNIVERSITY OF TRENTO - Italy


AS3491 Partnership (from Caida)




The relationship table below displays the neighbors of AS 3491, and each neighbor's inferred relationship type with AS 3491. Table shows 20 of 660 neighbor ASes, sorted by relationship type and AS rank, with simple details. update view

AS rank	AS	AS name	neighbor AS type(s)	Org name	type	known locations (hide cities)
1	3356	LEVEL3	TsAc	Level 3 Communications, Inc.	↑ provider	Seattle, San Jose, Los Angeles, Dallas, Atlanta, Miami, Washington, D.C., New York City, Uberlandia, Paris, Frankfurt Am Main
50	4826	VOCUS-BACK...	TsAc	Vocus Connect International Backbone	↑ provider	Mascot
2	174	COGENT-174	TsAc	Cogent Communications	*** peer	Seattle, San Jose, Los Angeles, Dallas, Chicago, Miami, Hamilton, Hoofddorp, Kuala Lumpur
4	2914	NTT-COMMUN...	TsAc	NTT America, Inc.	*** peer	Seattle, Santa Clara, San Jose, Los Angeles, Dallas, Houston, Chicago, Atlanta, Miami, Sterling, New York City, Dongguan, Beijing, Shanghai, Osaka, Tokyo, London, Paris, Hoofddorp, Frankfurt Am Main, Milano, Vilnius, New Delhi, Changi, Tseung Kwan O, Melbourne
5	3257	GTT-BACKBONE	TsAc	Tinet Spa	*** peer	Seattle, San Jose, Los Angeles, Dallas, Chicago, Miami, Washington, D.C., New York City, Massasauga, London, Hoofddorp, Marseille, Frankfurt Am Main, Milano, New Delhi, Changi, Dongguan, Chek Lap Kok, Seoul, Tokyo
6	6762	SEABONE-NET	TsAc	TELECOM ITALIA SPARKLE S.p.A.	*** peer	Los Angeles, Miami, Ashburn, London, Frankfurt Am Main, Changi, Dongguan, Chek Lap Kok
7	6453	AS6453	TsAc	TATA COMMUNICATIONS (AMERICA) INC	*** peer	Guangzhou, Dongguan, Dallas, London, Paris, Frankfurt Am Main, Changi, Tokyo, Mascot
8	6939	HURRICANE	TsAc	Hurricane Electric, Inc.	*** peer	Seattle, San Jose, Los Angeles, Dallas, Chicago, Atlanta, Miami, Ashburn, London, Hoofddorp, Frankfurt Am Main, Changi, Chek Lap Kok, Tokyo
9	2828	XO-AS15	TsAc	XO Communications	*** peer	San Jose, Los Angeles, Dallas, Chicago, Miami, New York City, Uberlandia, Sobral, London, Beijing, Tokyo

24/10/17
Offensive Technologies - Fabio Massacci
20



UNIVERSITY OF TRENTO - Italy




Whois Record

- **ASHandle:** AS3491
- **OrgID:** BNA-42
- **ASName:** BTN-ASN ASNumber: 3491
- **RegDate:** 1994-03-21
- **Updated:** 2012-03-02
- **Source:** ARIN
- **OrgID:** BNA-42
- **OrgName:** PCCW Global, Inc.
- **CanAllocate:**
- **Street:** 450 Springpark PL
- **Street:** Suite 1000
- **City:** Herndon
- **State/Prov:** VA
- **Country:** US
- **PostalCode:** 20170
- **RegDate:** 2004-05-25
- **Updated:** 2017-07-11
- **OrgAdminHandle:** PGIE-ARIN
- **OrgAbuseHandle:** PAD13-ARIN
- **OrgTechHandle:** RW437-ARIN
- **OrgTechHandle:** PUN6-ARIN
- **OrgNOCHandle:** PUN6-ARIN
- **OrgTechHandle:** BALON-ARIN
- **Source:** ARIN


24/10/17

Offensive Technologies - Fabio Massacci

21



UNIVERSITY OF TRENTO - Italy



AS3491 Now

Trascina verso il basso per visualizzare la cronologia

[Français](#) | [Español](#) | [日本語](#) | [简体](#) | [PARTNERS](#) | [CUSTOMER SUPPORT](#) | [CONTACT US](#) | [SEARCH](#)

[HOME](#)
[ABOUT](#)
[ENTERPRISE](#)
[SERVICE PROVIDER](#)
[GLOBAL COVERAGE](#)
[INDUSTRY SECTORS](#)
[NEWS & VIEWS](#)
[CONSULT](#)
[CAREERS](#)

Enterprise Services

- [Network](#)
- [International Managed Bandwidth](#)
- [Global Internet Access](#)
- [VPN Services](#)
- [Global Ethernet](#)
- [Content Delivery Network](#)

Global Internet Access

PCCW Global / Enterprise / Network / Global Internet Access

PCCW Global's high capacity and fully diversified global backbone and peering infrastructure makes it one of the premier IP network providers in the world. It is a one-stop shop for reliable and cost effective connectivity, enabling enterprises to access mission-critical applications over the Internet.

Trusted the World Over

PCCW Global offers global and regional enterprises 3 terabit, single AS global IPv4/IPv6 backbone (AS3491) so that they can deliver voice, video and applications over IP. We have a proven track record of quality and that allows us to carry more than 1.5 terabits of customer traffic globally.

One of the Largest IP Gateways to China

AS3491 is consistently ranked in the top 10 for global peering.

24/10/17

Offensive Technologies - Fabio Massacci

22

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

2/24/2008, YouTube Outage

- **YouTube (AS 36561)**
 - Web site www.youtube.com
 - Address block 208.65.152.0/22
- **Pakistan Telecom (AS 17557)**
 - Receives government order to block access to YouTube
 - Starts announcing 208.65.153.0/24 to provider (AS 3491)
 - All packets directed to YouTube get dropped on the floor
- **Mistakes were made**
 - AS 17557: announcing to everyone, not just customers
 - AS 3491: not filtering routes announced by AS 17557 (will come back to this later)
- **Lasted 100 minutes for some, 2 hours for others**

24/10/17 Offensive Technologies - Fabio Massacci 23


UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

YouTube Outage in Pictures


The diagram illustrates the network topology during the YouTube outage. It shows several Autonomous Systems (ASes) represented as clouds: AS 17557, AS 3491, AS 4, AS 7, AS 15169, and AS 36561. Red arrows indicate the path of the leaked route 208.65.153.0/24, starting from AS 17557 and being announced to AS 3491, AS 4, and AS 7. Green arrows show the intended path for traffic to YouTube (AS 36561) via AS 15169. The diagram highlights how the leaked route from AS 17557 caused traffic to be misrouted and dropped.

- **YouTube (AS 36561)**
- **Beyond the Network America/PCCW (AS 3491)**
- **Pakistan Telecom (AS 17557)**

24/10/17 Offensive Technologies - Fabio Massacci 24




UNIVERSITY OF TRENTO - Italy




Timeline (UTC Time)

- **18:47:45**
 - First evidence of hijacked /24 route propagating in Asia
- **18:48:00**
 - Several big trans-Pacific providers carrying the route
- **18:49:30**
 - Bogus route fully propagated
- **20:07:25**
 - YouTube starts advertising the /24 to attract traffic back
- **20:08:30**
 - Many (but not all) providers are using the valid route
- **See:**
 - <http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/>

24/10/17 Offensive Technologies - Fabio Massacci 25




UNIVERSITY OF TRENTO - Italy




Timeline (UTC Time)

- **20:18:43**
 - YouTube starts announcing two more-specific /25 routes
- **20:19:37**
 - Some more providers start using the /25 routes
- **20:50:59**
 - AS 17557 starts prepending (“3491 17557 17557”)
 - Prepending makes routes longer, less desirable
- **20:59:39**
 - AS 3491 disconnects AS 17557
- **21:00:00**
 - All is well, videos of cats flushing toilets are available

24/10/17 Offensive Technologies - Fabio Massacci 26




UNIVERSITY
OF TRENTO - Italy




Lessons From the Example

- ***BGP is very efficient → very vulnerable***
 - Local actions → global consequences
 - Propagating information is easy → propagating misinformation too
 - Telling information from mis-information is hard → need authentication
- ***Recovering from the problem required vigilance***
 - Monitoring to detect and diagnose the problem
 - Immediate action to (try to) attract the traffic back
- ***Preventing these problems requires cooperation***
 - Require all ASes to perform defensive filtering
 - Automatically detect and stop bogus route
 - Require proof of ownership of the address block
- ***All “preventive” solutions require cooperative action by “by-standers” rather than victims***
 - Might work if solution also prevents mistakes besides mischiefs
 - Mistakes are more frequent and nobody wants to have faulty business partners

24/10/17 Offensive Technologies - Fabio Massacci 27




UNIVERSITY
OF TRENTO - Italy




Solutions

- ***Protective filtering***
 - Know your neighbors
- ***Anomaly detection***
 - Suspect the unexpected
- ***Checking against registries***
 - Establish ground truth for prefix origination
 - May not be up to date
- ***Signing and verifying***
 - Prevent bogus AS PATHs
- ***Data-plane verification***
 - Ensure the path is actually followed

28/10/17 Offensive Technologies - Fabio Massacci




UNIVERSITY
OF TRENTO - Italy




Defensive Filtering

- **Filter announcements**
 - from customers but not for customer prefixes
- **Filter announcements**
 - from customers that have a large AS on the path
- **Keep history of prefix origins and prefer bindings that are long-lived**
 - Could do the same for adjacencies in AS paths
 - BUT violates the basic idea of routing – resiliency
 - Doesn't work on closeness attacks

24/10/17 Offensive Technologies - Fabio Massacci 29



UNIVERSITY
OF TRENTO - Italy



Attacking BGP Sessions

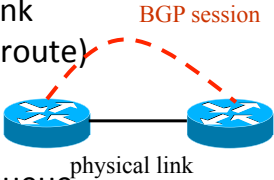
- **BGP session runs over TCP**
 - TCP connection between neighboring routers
 - BGP messages sent over TCP connection
 - Makes BGP vulnerable to attacks on TCP
- **Main kinds of attacks**
 - Against confidentiality: eavesdropping
 - Against integrity: tampering
 - Against performance: denial-of-service
- **Main defenses**
 - Message authentication or encryption
 - Limiting access to physical path between routers
 - Defensive filtering to block unexpected packets

24/10/17 Offensive Technologies - Fabio Massacci 30

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Denial-of-Service Attacks, Part 1

- **Overload the link between the routers**
 - To cause packet loss and delay
 - ... disrupting the performance of the BGP session
- **Relatively easy to do**
 - Can send traffic between end hosts
 - As long as the packets traverse the link
 - (which you can figure out from traceroute)
- **Easy to defend**
 - Give higher priority to BGP packets
 - E.g., by putting packets in separate queue



physical link


24/10/17 Offensive Technologies - Fabio Massacci 31

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


Denial-of-Service Attacks, Part 2

- **Third party sends bogus TCP packets**
 - FIN/RST to close the session
 - SYN flooding to overload the router
- **Leads to disruptions in BGP**
 - Session reset, causing transient routing changes
 - Route-flapping, changing routes back and forth
- **Hard to launch**
 - Spoofing TCP packets the right way is hard
 - Difficult to send FIN/RST with the right TCP header
 - Packet filters may block the SYN flooding
 - Filter packets to BGP port from unexpected source
 - ... or destined to router from unexpected source
 - Turn on SYN cookies

24/10/17 Offensive Technologies - Fabio Massacci 32




UNIVERSITY OF TRENTO - Italy




Exploiting the IP TTL Field

- **BGP speakers are usually one hop apart**
 - To thwart an attacker, can check that the packets carrying the BGP message have not traveled far
- **IP Time-to-Live (TTL) field**
 - Decrement once per hop
 - Avoids packets staying in network forever
- **Generalized TTL Security Mechanism (RFC 3682)**
 - Send BGP packets with initial TTL of 255
 - Receiving BGP speaker checks that TTL is 254
 - ... and flags and/or discards the packet others
- **Hard for third-party to inject packets remotely**

24/10/17 Offensive Technologies - Fabio Massacci 33




UNIVERSITY OF TRENTO - Italy




Authenticate Adverts

- **Resource public-key infrastructure (RPKI)**
- **Used for origin validation in routes**
 - Cannot validate path
- **The organization that sells you an IP range also issues you a certificate that you hold this range (no identity information)**
 - Binds your address range to your public key
- **When you advertise routes you include a ROA (Route Origin Authorization), showing which ASes can advertise this route**
 - Signed with your private key
- **More Info**
 - <https://www.ietf.org/proceedings/interim-2014-sidr-01/slides/slides-interim-2014-sidr-1-0.pdf>
 - Slides 3-10

24/10/17 Offensive Technologies - Fabio Massacci 34




UNIVERSITY OF TRENTO - Italy




BGPSEC

- ***Sign everything you announce***
 - Origin and AS_PATH
- ***Use your private key to sign (same key as in RPKI):***
 - Prefix
 - AS_PATH
 - Your AS number, neighbor's AS number
- ***Check everything when you get announcements***
- ***Generate signed announcements only toward neighbors that support BGPSEC***

24/10/17 Offensive Technologies - Fabio Massacci 35



UNIVERSITY OF TRENTO - Italy



BGPSEC – Open problems

- ***Replay is possible***
 - Added timers to route announcements
 - Short timers increase overhead, long timers leave you open to attack longer
- ***Validating route announcements is expensive computationally***
 - Much more than processing BGP updates
 - Really large signatures
 - 15 x overhead of regular BGP
 - Really problematic at convergence time
 - Disable optimizations such as “update packing”
- ***BIGGEST PROBLEM:***
 - If each router uses a separate public key BGPSEC enables others to learn about internal ISP topology
 - Might be used for commercial advantage
 - let me offer your customers a better (e.g. direct) connection

24/10/17 Offensive Technologies - Fabio Massacci 36