Applied Networking Research Workshop 2020

Inferring the Deployment of Inbound Source Address Validation Using DNS Resolvers

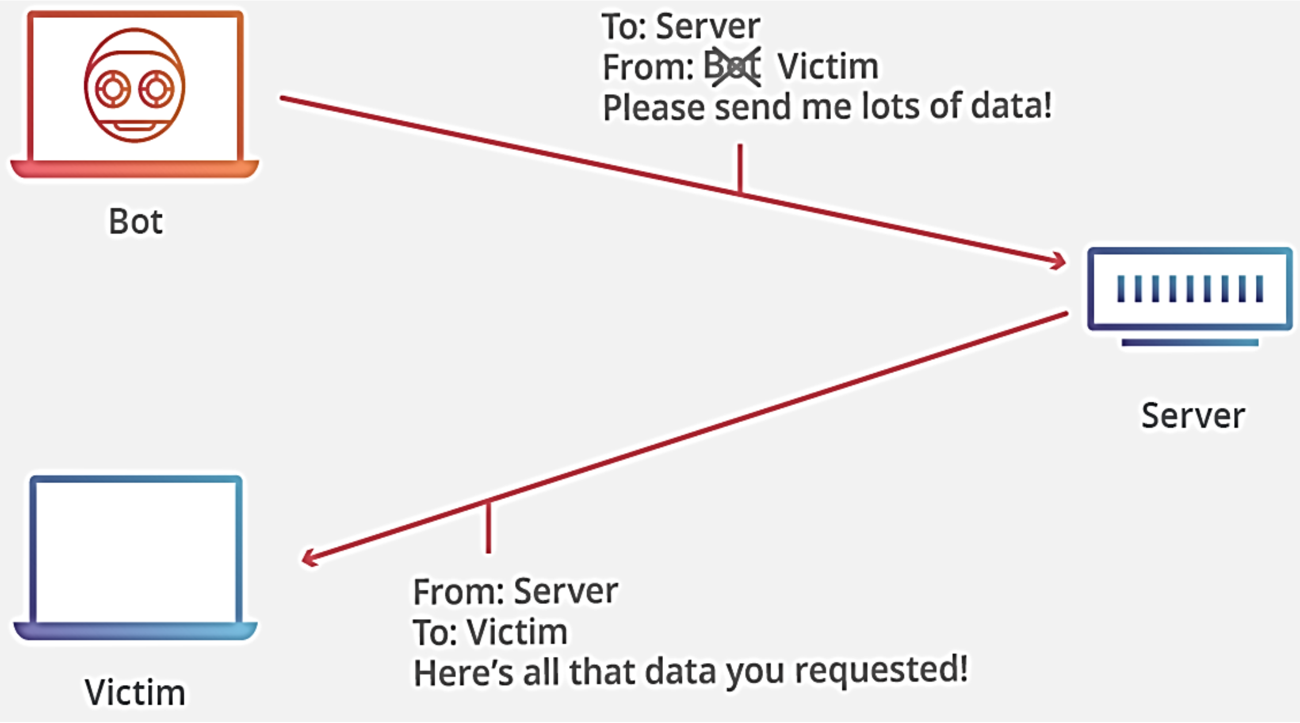
Maciej Korczyński*, Yevheniya Nosyk*, Qasim Lone§,
Marcin Skwarek*, Baptiste Jonglez*, and Andrzej Duda*

*Université Grenoble Alpes, CNRS, Grenoble INP, LIG
§Delft University of Technology

yevheniya.nosyk@etu.univ-grenoble-alpes.fr
maciej.korczynski@univ-grenoble-alpes.fr

What is IP address spoofing?

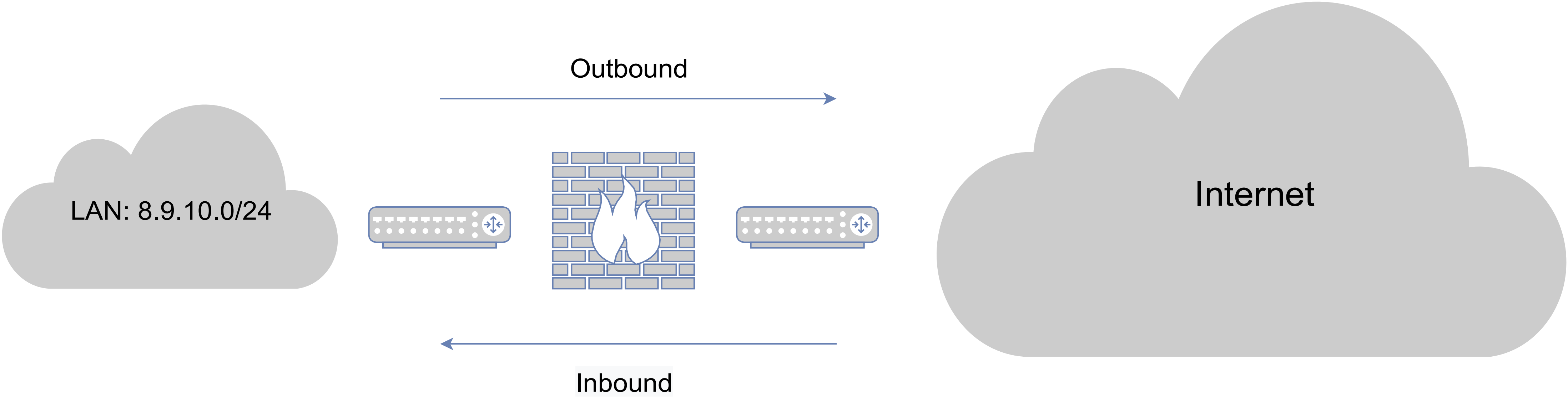
- Modification of the source IP address of the packet
- Anonymity of the sender
- Cause of DDoS attacks
- GitHub DDoS attack of 28.02.2018



https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

Source Address Validation

- Defined in BCP-38 (RFC 2827) in 2000
- Spoofed packets to be dropped at the network edge
- Two directions: inbound and outbound



What is the state of deployment of Source Address Validation by network providers?

Existing work on SAV compliance

- The Spoofer [1]
- Forwarders-based method [2,3]
- Traceroute loops [4]
- Passive detection [5,6,7]

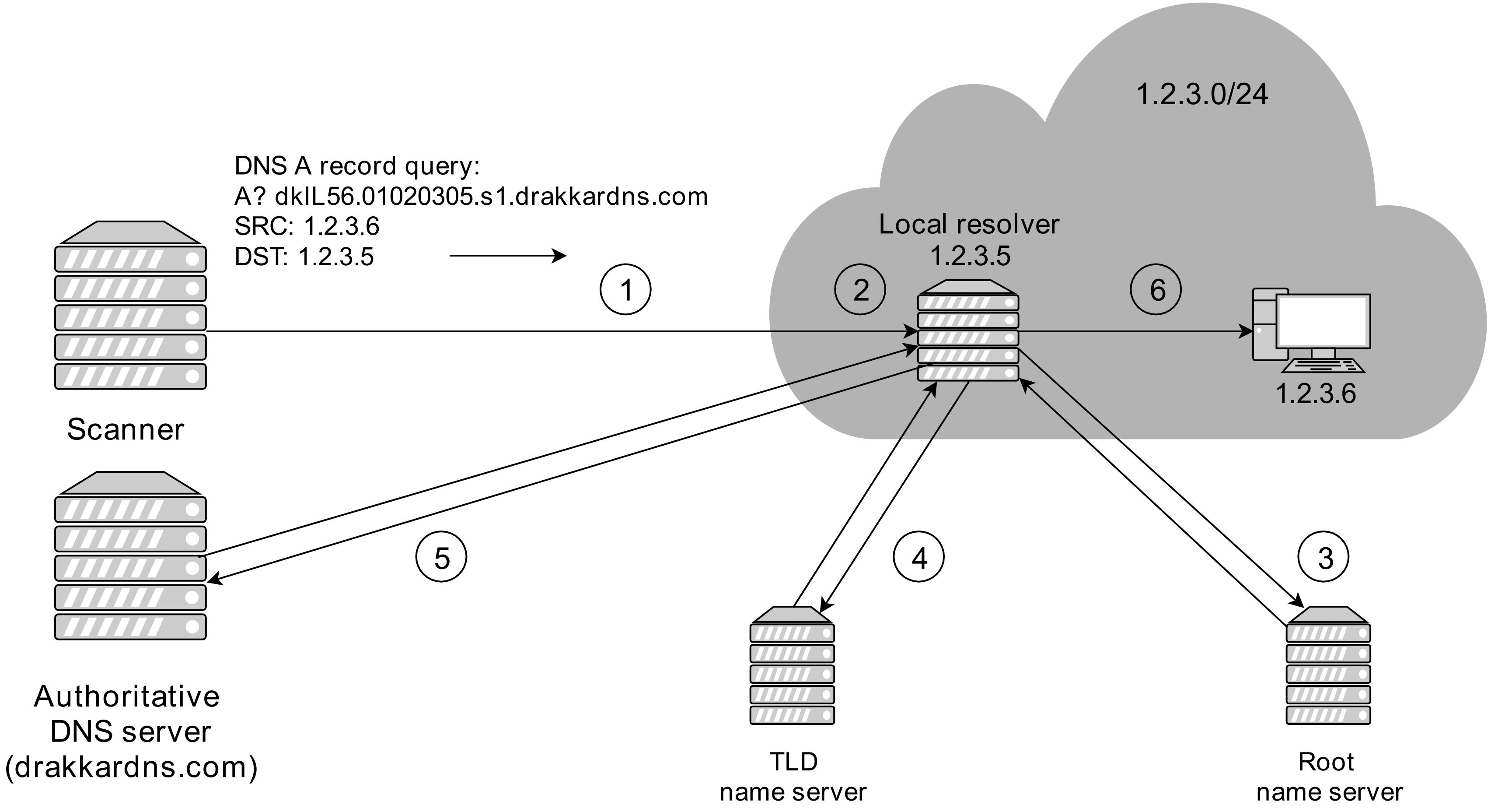
[1] https://www.caida.org/projects/spoofer
[2] Mauch, J.: Spoofing ASNs, http://seclists.org/nanog/2013/Aug/132
[3] Kührer, M., Hupperich, T., Bushart, J., Rossow, C., Holz, T.: Going Wild: Large-Scale Classication of Open DNS Resolvers. In: IMC, ACM (2015)
[4] Lone, Q., Luckie, M., Korczyński, M., van Eeten, M.: Using Loops Observed in Traceroute to Infer the Ability to Spoof. In: PAM (2017)
[5] Lichtblau, F., Streibelt, F., Krüger, T., Richter, P., Feldmann, A.: Detection, Classification, and Analysis of Inter-domain Traffic with Spoofed Source IP Addresses. In: IMC, ACM (2017)
[6] Müller, L.F., Luckie, M.J., Huffaker, B., kc claffy, Barcellos, M.P.: Challenges in Inferring Spoofed Traffic at IXPs. In: CoNEXT, ACM (2019)
[7] Jasper Eumann, Raphael Hiesgen, Thomas C. Schmidt, Matthias Wählisch. arXiv:1911.05164 [cs.NI] (2019)

What do we propose and why?

- Measuring *inbound* SAV compliance. Why *inbound*? Because:
    - NXNSAttack [1]
    - Windows DNS Server Remote Code Execution Vulnerability (SigRead) [2]
    - Zone poisoning [3]
- Completely remote
- Covering the whole routable IPv4 space
- Not relying on misconfigurations

[1] Lior Shafir, Yehuda Afek, Anat Bremler-Barr. NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities. In: USENIX Security (2020)
[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350
[3] Zone Poisoning: The How and Where of Non-Secure DNS Dynamic Updates. Maciej Korczynski, Michal Krol, and Michel van Eeten. In: IMC (2016)

Methodology



Methodology

- The proposed method detects the *absence* of inbound SAV.
- How to detect its *presence*?
  - Follow each spoofed packet with a non-spoofed one!

- Overcomes major limitations of existing work
- Follows ethical scanning principles

Results

- Scan performed in December 2019
- 5,651,672,542 spoofed and non-spoofed packets sent

- 6,946,782 vulnerable resolvers:
  - 4,589,251 closed
  - 2,357,531 open

- Vulnerable resolvers come from:
  - 32,673 autonomous systems (49.34%)
  - 197,641 BGP prefixes (23.61%)
  - 959,666 /24 IPv4 networks (8.62%)

Presence vs. Absence of SAV

- Significantly more networks do not deploy inbound SAV than deploy it
- Many filter partially:
  - 38,47% of autonomous systems
  - 22,37% of BGP prefixes
  - 12,30% of /24 IPv4 networks
- Why?
  - Packet losses
    - Rescanned a sample of 1000 /24 partially vulnerable networks
    - 50% immediately became consistent (all vulnerable to spoofing)
  - Done on purpose
    - Confirmed by network operators

Outbound vs. Inbound Filtering

- Inbound SAV – protects the network itself
- Outbound SAV – protects *other* networks

- Assumption: inbound filtering is more deployed than outbound

Outbound vs. Inbound Filtering

- Comparison with the Spoofer data

- 559 common /24 networks:
  - 95 do not filter in either direction
  - 151 filter in both directions
  - 298 filter only outbound traffic
  - 15 filter only inbound traffic

- Inbound filtering is less deployed than outbound

Conclusions

- Novel method to infer inbound SAV deployment [1,2]
- Internet-wide measurement study
- Over 49% of ASes and 23% of the longest matching BGP prefixes are vulnerable to inbound IP spoofing
- Notification campaign in the near future
- Follow-up study [3]
  - 25,47 % of IPv6 autonomous systems are vulnerable to inbound spoofing
  - SAV is less deployed in IPv6 than IPv4

[1] Korczyński M., Nosyk Y., Lone Q., Skwarek M., Jonglez B., Duda A. Don't Forget to Lock the Front Door! Inferring the Deployment of Source Address Validation of Inbound Traffic. In: Passive and Active Measurement Conference (2020).
[2] Korczyński M., Nosyk Y., Lone Q., Skwarek M., Jonglez B., Duda A. Inferring the Deployment of Inbound Source Address Validation Using DNS Resolvers. In: ANRW (2020).
[3] Korczyński M., Nosyk Y., Lone Q., Skwarek M., Jonglez B., Duda A. The Closed Resolver Project: Measuring the Deployment of Source Address Validation of Inbound Traffic. arXiv:2006.05277 [cs.NI] (2020)

Acknowledgements

- This work has been carried out in the framework of the PrevDDoS project funded by the IDEX Université Grenoble Alpes and supported by the Grenoble Alpes Cybersecurity Institute.

- Thanks to network operators: Roland M. van Rijswijk-Deij (University of Twente), Willem Toorop (NLnet Labs), Baptiste Jonglez (Tetaneutral.net), Niels Raijer (Fusix Networks)

Are you vulnerable to inbound spoofing?
Contact us!

closedresolver.com

maciej.korczynski@univ-grenoble-alpes.fr
yevheniya.nosyk@etu.univ-grenoble-alpes.fr

Questions?

maciej.korczynski@univ-grenoble-alpes.fr
yevheniya.nosyk@etu.univ-grenoble-alpes.fr