Advanced Topics in IP Networks
Lecture 07

Lecture by Dr. Yuval Shavitt and Dr. Anat Bremler-Barr
Typeset by Steven Karas

2018-11-29
Last edited 20:59:51 2018-11-29

Disclaimer These notes are based on the lectures for the course Advanced Topics in IP Networks, taught by Dr. Anat Bremler-Barr at IDC Herzliyah in the fall semester of 2018/2019. Sections may be based on the lecture slides prepared by Dr. Anat Bremler-Barr.

1 Agenda

Today we will have a guest lecture by Dr. Yuval Shavitt, professor of Electrical Engineering at Tel Aviv University, and CTO of BGProtect. He will present on the topic of IP hijacking.

2 IP Hijacking

Some of the reasons for hijacking IPs:

- Man in the middle
- Impersonation
- White-IP space for staging attacks

An overview of attack methodologies:

- BGP hijack
  - an AS announces a very specific route for a block.
  - an AS announces they are a peer for a block.
- DNS
- Stealth attacks with little to no control plane signature:
  - static BGP route
  - static forwarding entry into an IP block
  - manipulations at exchange points (ettercap, etc)
  - breaking the routers themselves or using an insider

Stealth attacks have little to no signature on the control plane and may persist for a very long time, although they are likely to have limited impact, for example only affecting a very small percentage of the traffic.

2.1 Detection of an attack

Due to the nature of BGP, routes may not necessarily follow the rule of thumb of shortest path to a backbone to the destination exchange point. Extreme examples can be readily found. For example, routes from Japan to California back to South Korea. Sometimes the geography is a sufficient indicator, for example routes from Canada to South Korea that went through China.

Note that because traceroute is based on ICMP and many networks do not expose or pass ICMP traffic, especially to non-customer networks, sometimes other routing signals need to be used, such as UDP beacons or TCP sessions.

2.1.1 BGProtect

Uses a distributed system of monitoring agents to track latency and routing to collect signals. Features are extracted from these signals and the detected route. Example features are IP ownership, AS (BGP), geography, delay, and political relationships. They then use a rule-based analysis engine, with rules based on expert domain knowledge and proprietary databases.

There are two interesting effects of attacks. Traffic has a tendency to go to a somewhat unlikely hop, and will then reappear in a different city with no intervening hops. This can sometimes happen, but is suspicious. The other is that mitigation is typically handled via email to NOC teams around the world.

3 Homework Notes

HW1 has been mostly graded, and feedback has been given, but grades have not been published yet. The next HW will be published soon, and will be done in Python.

The project proposal must be submitted before the end of the course. They will be due one month after the end of the semester. Each project should be a combination of programming and research, for example taking a paper that suggested two options but only implemented/checked one, and to implement the other one.

4 Software Defined Networks

The internet before SDN looked like a list of vendors, as each vendor had different things they supported, and they would often write the protocols themselves. Most of the infrastructure was based on a 3-tier model of specialized hardware, a specialized operating system, and a small set of apps built by the vendors themselves for specific hardware models, with many complex functions baked into the infrastructure.

Generally speaking, even a traditional router can be split into a management plane, a control plane, and a data plane. The approach of SDN is to consolidate the control plane into one place and separate it from the data plane. This gives us the ability to write different applications on top of this centralized control plane, and replace them independently of the network fabric.

Nicira, the original SDN startup was purchased by VMWare for 1.26B USD in 2012. Google published a paper[2] in 2013 describing how they use SDN.

4.1 OpenFlow

OpenFlow is a specific implementation of SDN. Early versions specified the exact fields, actions, and statistics gathered, but with each version this grew and now there is a generic language for defining matches, actions, etc.

Reactive vs Proactive In a reactive environment, the flow table has a single rule: forward all packets to the controller. The controller then installs flow entries in response to incoming packets. This is good for stateful forwarding, such as L2 switching, dynamic firewall, and resource management.

In a proactive environment, the flow table is populated by the controller on switch boot. This is good for stateless forwarding, such as L3 switching, static firewall, etc.

Evolution of the AL Single tables are overly wide and overly long. Instead of doing the cross product of all the rules, we just pipeline everything through multiple tables.

References

[1] Mark Crovella and Balachander Krishnamurthy. *Internet Measurement: Infrastructure, Traffic and Applications*. John Wiley & Sons, Inc., New York, NY, USA, 2006.

[2] Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jon Zolla, Urs Hölzle, Stephen Stuart, and Amin Vahdat. B4: Experience with a globally-deployed software defined wan. *SIGCOMM Comput. Commun. Rev.*, 43(4):3–14, August 2013.

[3] James F. Kurose and Keith Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition, 2002.

[4] George Varghese. *Network Algorithmics,: An Interdisciplinary Approach to Designing Fast Networked Devices (The Morgan Kaufmann Series in Networking)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2004.