Computer Networks

Routing and Its Woes

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

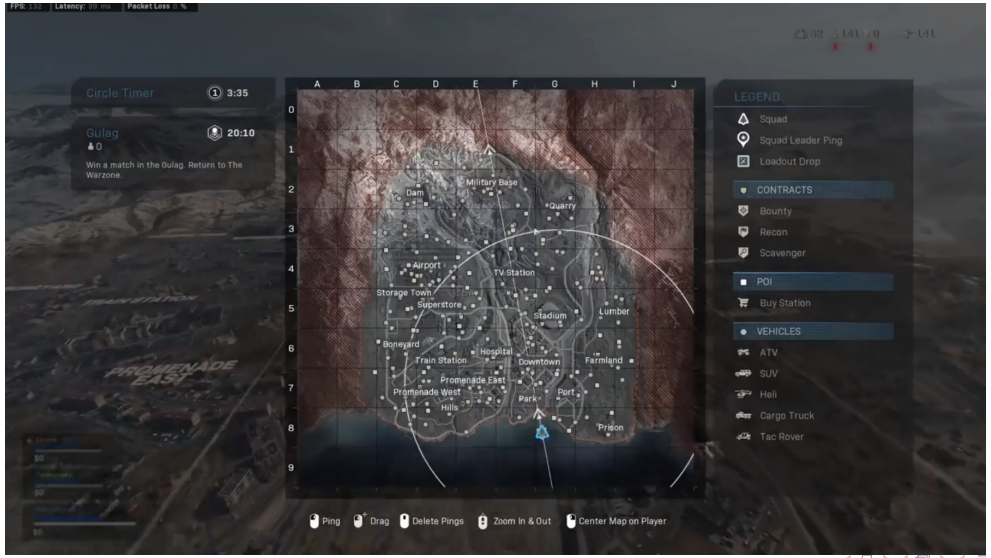
Computer Networks
Routing and Its Woes
Irfan Kanat
Department of Digitization
Copenhagen Business School
February 21, 2022

We will talk about how routing can be exploited for fun and profit.

Can you think of a misuse of routing algorithms?

In June 2019, European internet traffic was routed through China (also in 2010).
This can allow interception of data, or MITM attacks.
Similar attacks happened in the past as well.
They rely on manipulating BGP.

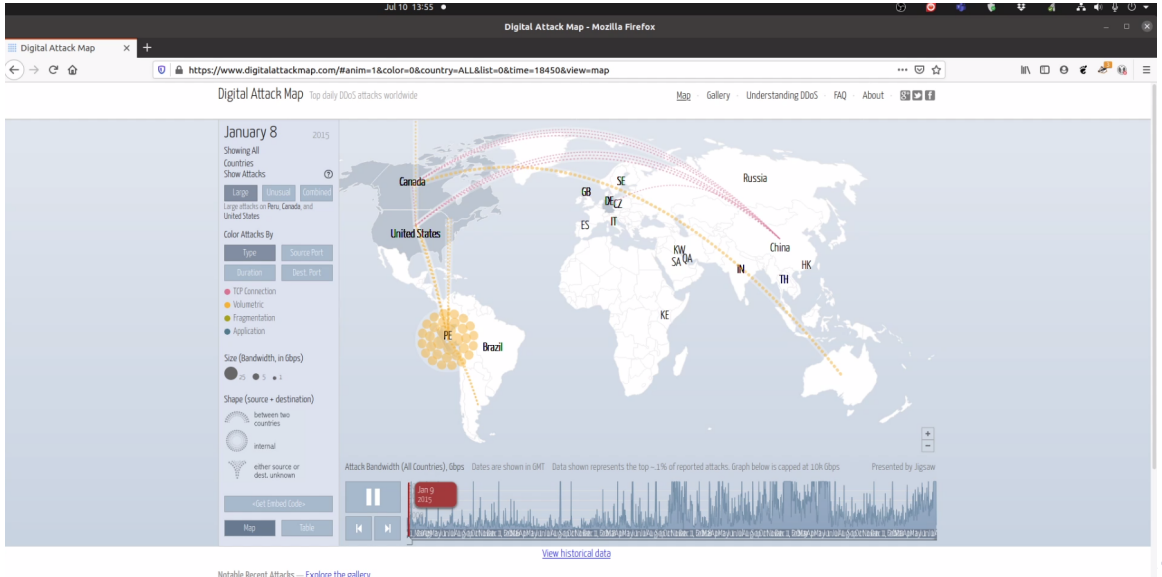
Lag and Package Loss

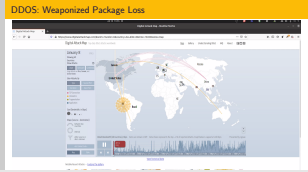


Lag and Package Loss

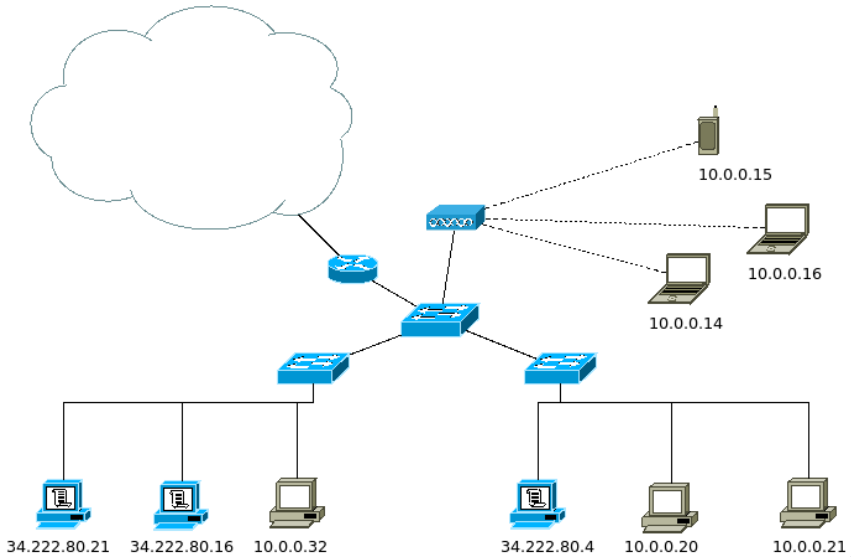
Lag and Package Loss

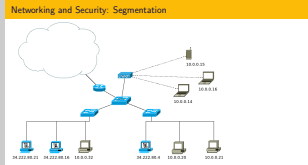
DDOS: Weaponized Package Loss





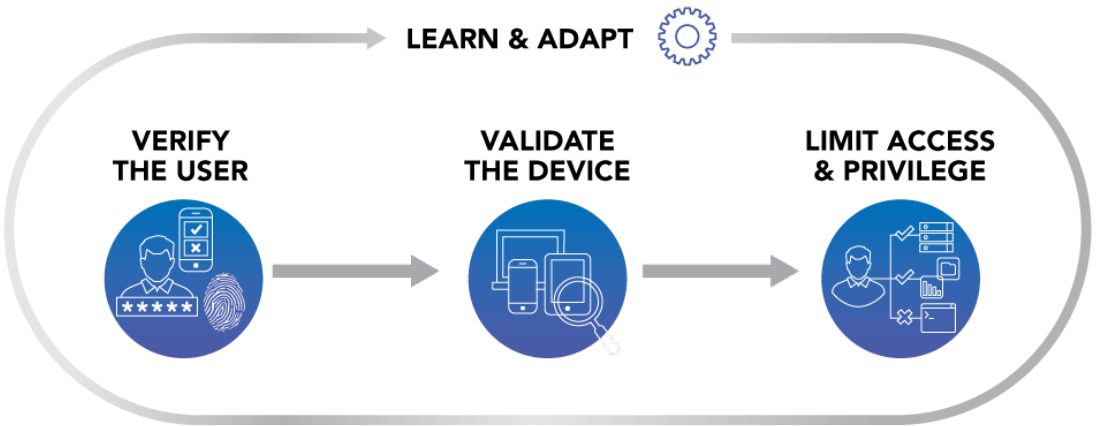
Networking and Security: Segmentation

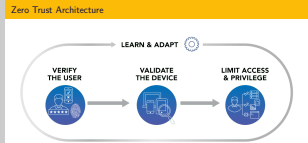




Segmentation: it kept coming up in cases we read (target esp.)
The idea is, you can have multiple virtual networks on the same hardware. So you put your customer facing machines on one network, and your back office oprations in another, and perhaps mission critical systems on yet another network. What this means is they all get their own IP prefix and treat each other as nodes in different networks.

Zero Trust Architecture





This is a more recent trend.
No trust is granted based on network location.
All devices and users authenticated
Data released on a need to know basis
Focus is on protecting resources and not network segments.
This is in contrast to prior approaches that focused on network segments.
NIST draft 800-207

Intrusion Detection on Networks

Unusual behavior on your network

Heuristics

Known signatures

Intrusion Detection on Networks
Unusual behavior on your network
Heuristics
Known signatures

A few examples:
A client is rapidly sending packages to a large number of ip's and ports (proably nmap scan)
A server with minimal functionality generally does not initiate exchanges. Meaning TCP syn packets do not generally originate from servers. If you see your server reaching out.
Or generating traffic on ports it is not supposed to generate traffic on...
Then you know that there is something wrong.

Attacks often have certain characteristics. These attack specific characteristics are called signatures. These signatures are often shared through intel sharing schemes. If your network demonstrates behavior that matches the signature IDS will pick up.

NIDS Solutions

Appliances

Software

NIDS Solutions
Appliances
Software

IDS can be provided by appliances (like Watchguard), or by software solution (like SNORT). Appliances are used for larger networks where latency can be an issue.
The network based intrusion detection is often coupled with end point ids. That is not within our scope today.