Visualizing, Analyzing and Filtering Zeek Events

using a graphical frontend and OpenGL

Nick Skelsey
ZeekWeek 2019
Seattle, WA
11 October, 2019
AGENDA

1. Motivation
2. State of the art
3. Monopticon
4. Related research
CONNECTIVITY ISSUES: do not suffer in silence

- ping google.com
- ping 8.8.8.8
- ip a
- ping 192.168.1.0
- dhcp -4 iface_name

*check cable*
*check unpaid bills*
*check news for regional disaster*
1. Graphics can have high information density.
2. No certifications required.
3. Develop intuition.
A GPLv3 application built with C++, zeek and Mangum for POSIX systems.
Bettercap ARP Spoofing

> set arp.spoof.internal true;
> set arp.spoof.targets 192.168.1.20,192.168.1.30;
> set arp.spoof.full_duplex on;
> arp.spoof on;
1. Limit scope: Ethernet and IPv4
2. Must be modular: Represent the OSI stack as a stack
3. Must be passive: offline packet analysis
4. Must be quick: native or web assembly
5. Should be extensible: zeek and bash scripts
DESIGN

[Diagram showing a network model with components such as 'zeek', 'custom zeek script', 'network model', 'epochs', 'zeek-broker', '66 Hz epoch stream', and a graphics process with 'poll and draw at 60 fps', 'rendere pipe; draw calls', and 'GPU'].

---

(BV TECH)
IEEE 802.1* defines ethernet

38:30:f9:61:97:6f
THE GRAPHICS PIPELINE
OBJECT SELECTION
const int elems_per_ring[8] {1, 4, 8, 16, 32, 64, 256, 10000};
const float ring_radii[8] {0.0f, 4.0f, 8.0f, 12.0f, 16.0f, 24.0f, 32.0f, 64.0f};
All devices addressable by their MAC.

Frames traverse switches based on:

- Destination address
- The type of address
- The switches (routing) tables
- Structure of the spanning tree
- Optimizations like 802.1aq

zeek package that passively infers the structure of an IPv4 network over Ethernet
INFERRING NETWORK STRUCTURE

VPN to DNS LAN map on 10/6/2019 by tsheesley.com

Link Layer 64:15:0:8/64  10.7.7.0/24  1

10.7.7.0/24  10.7.7.0/24  1  111

192.168.8.0/24  1  111

8.8.8.8/8  147  71
100  108  188
54  223
193  1  223
14  153
64  178  97
247

BV TECH

securenetwork
Your Protection. Our Mission

20
DRAWING A BROADCAST DOMAIN
Port knocking
FUTURE WORK

1. Extensible event monitoring
2. Sane packaging
3. L2 & L3 model to identify network security policy violations.
THANK YOU

Check out:

Monopticon on github or in the AUR

aaalm zeek package

Bibliography:

nskelsey.com/zweek

bytech.it

securenetwork.it