CPU Ping Reporter Presentation

Vladimir Beaugé

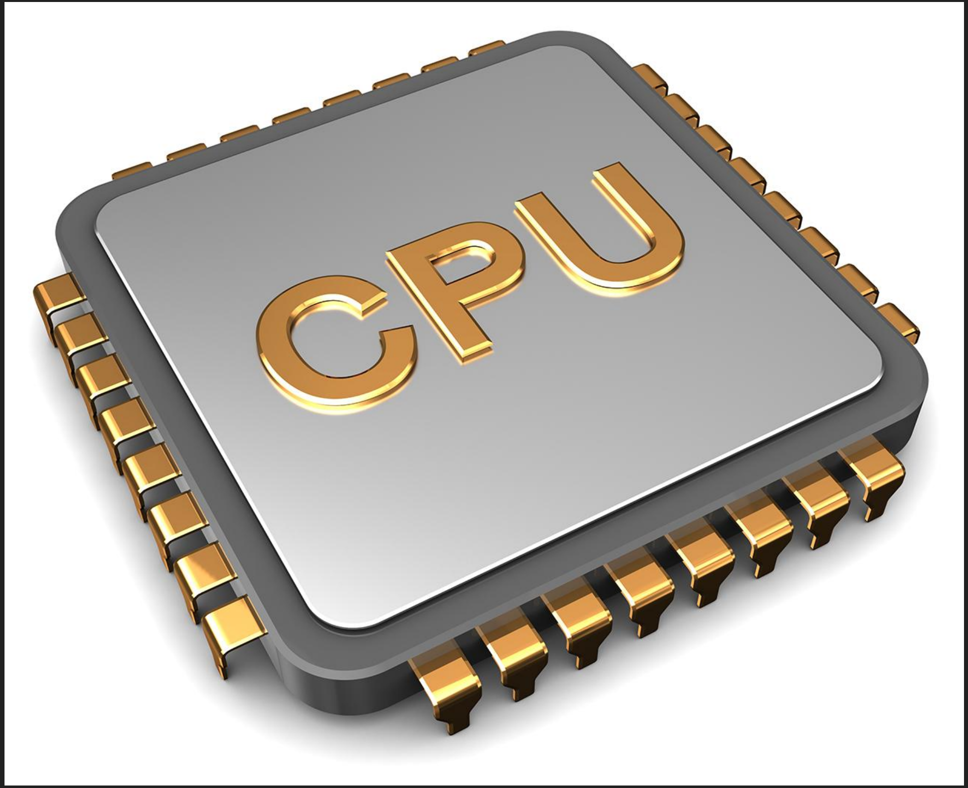
1816

Potsdam

THE STATE UNIVERSITY OF NEW YORK

Project Outline: Scientific Method

- Observation
- Research
- Hypothesis
- Experiments
- Collect Data
- Analysis
- Conclusions



Observation

- New Question: How Do Pings Affect a CPU?

- Original Question: How Many Pings does it take to shut down a server?

Research

- Ping
- DOS vs DDOS
- Ping of Death (PoD)
  - Attack Description
  - Methods of Mitigation
- Ping Flood (ICMP Flood)
    - Attack Description
    - Methods of Mitigation

Hypothesis

If I simulate ping attacks on a machine **then** the CPU of the attacker or victim increase at most 30%.

Experiment Materials

- Hardware
  - Digital Ocean Droplet
    - Cores : 1
    - CPU Freq: 1797.917
    - BogoMips: 3595.83
  - Old Toshiba Laptop
    - Cores : 2
    - CPU Freq: 2401
    - BogoMips: 4788.12
- Software
  - Mpstat, hping3

Code

```
step1....sh
#!/bin/bash


#show cpu usage after getting pinged
mpstat 30 100000 >> git-repo/Ping-Reporter/Exp2/data-<attack xor victim>/data-<set>-<exp>.xlsx



step2....sh
#!/bin/bash


hping3 -1 --flood --rand-source -f <victim IP>
hping3 -1 -d <size> --flood --rand-source -f <victim IP>
```

mpstat

CPU Utilization Parameters

- %usr
- %nice
- %sys
- %iowait
- %irq
- %soft
- %steal
- %guest
- %gnice
- %idle

Specific Parameters

- %soft
  - Show the percentage of time spent by the CPU(s) to service hardware interrupts

Experiment 1

Independent Variables: ping flood over time with variable size

Dependent Variables: CPU usage on “attacker” and “victim”

Controlled Variables: Hardware, time

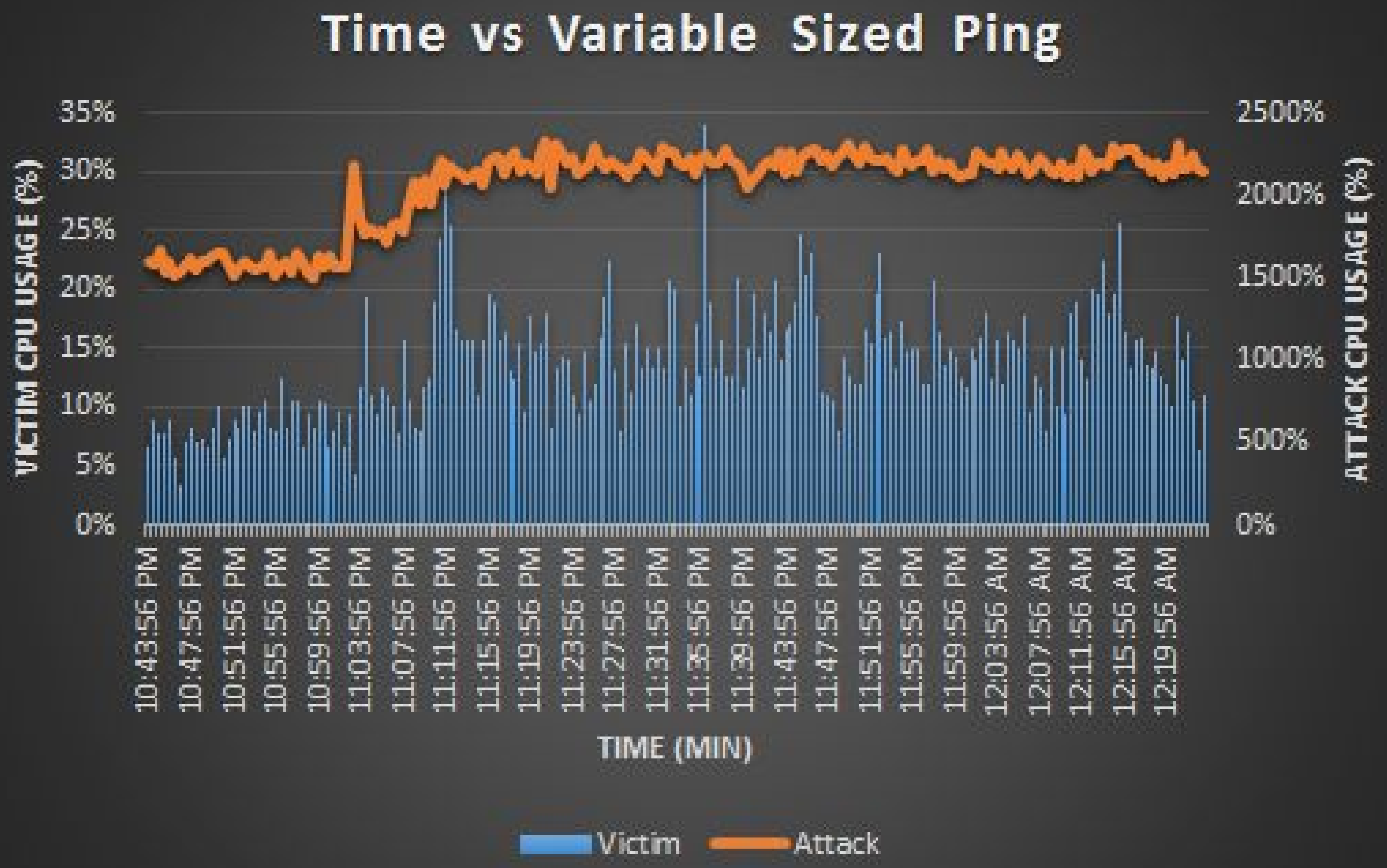
Constant Variable: Location, Network, Software

1. Run mpstat on machines A and B for 20 minutes to collect data on CPU behavior prior

2. Use hping3 on machine A to hit machine B for 1 hour

3. Keep running mpstat for 20 minutes to collect data on CPU behavior

4. Repeat 3 times


Time vs Variable Sized Ping
VICTIM CPU USAGE (%)
35%
30%
25%
20%
15%
10%
5%
0%
ATTACK CPU USAGE (%)
2500%
2000%
1500%
1000%
500%
0%
10:43:56 PM
10:47:56 PM
10:51:56 PM
10:55:56 PM
10:59:56 PM
11:03:56 PM
11:07:56 PM
11:11:56 PM
11:15:56 PM
11:19:56 PM
11:23:56 PM
11:27:56 PM
11:31:56 PM
11:35:56 PM
11:39:56 PM
11:43:56 PM
11:47:56 PM
11:51:56 PM
11:55:56 PM
11:59:56 PM
12:03:56 AM
12:07:56 AM
12:11:56 AM
12:15:56 AM
12:19:56 AM
TIME (MIN)
Victim
Attack

Experiment 2

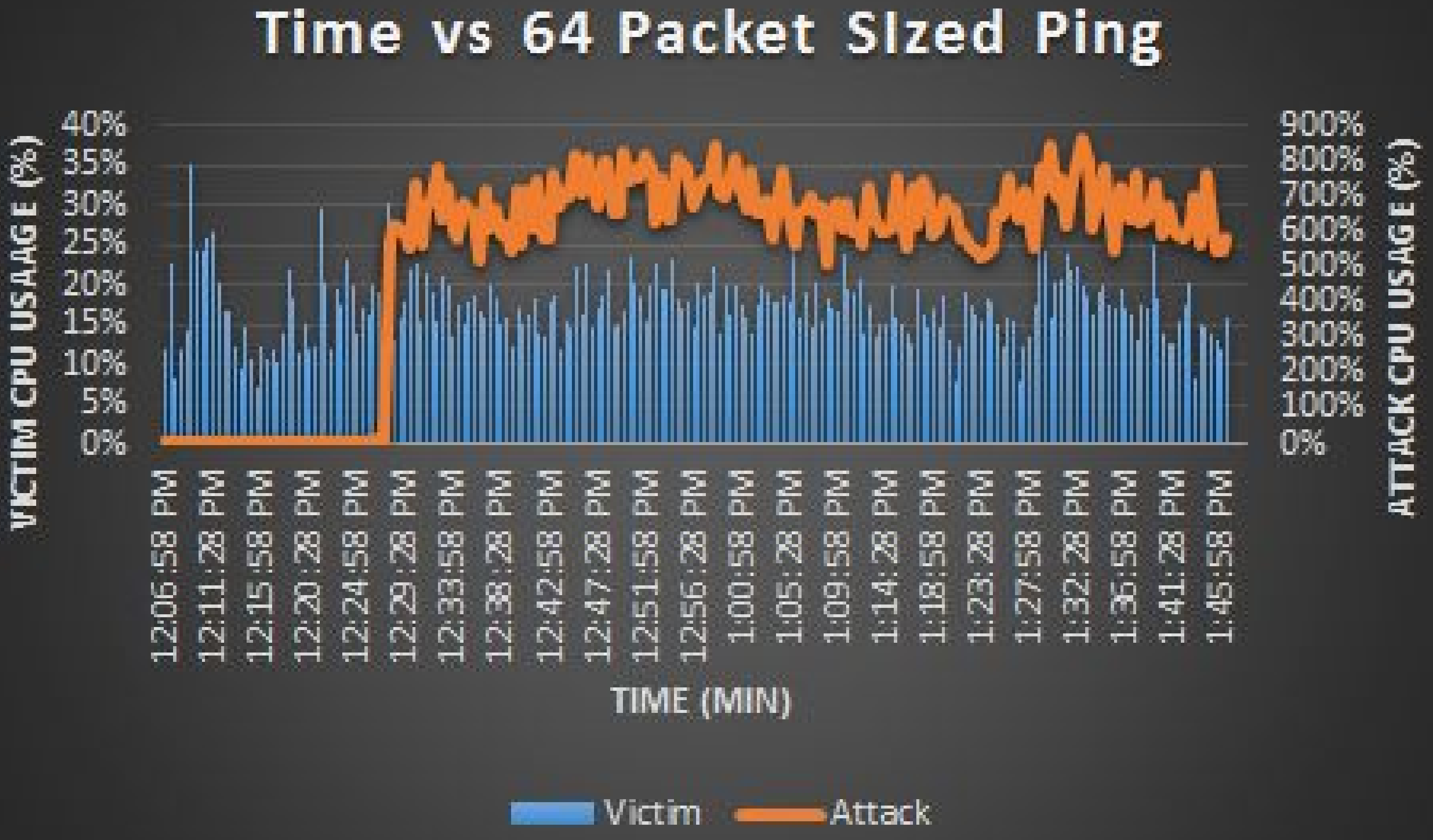
Independent Variables: ping package sizes over time

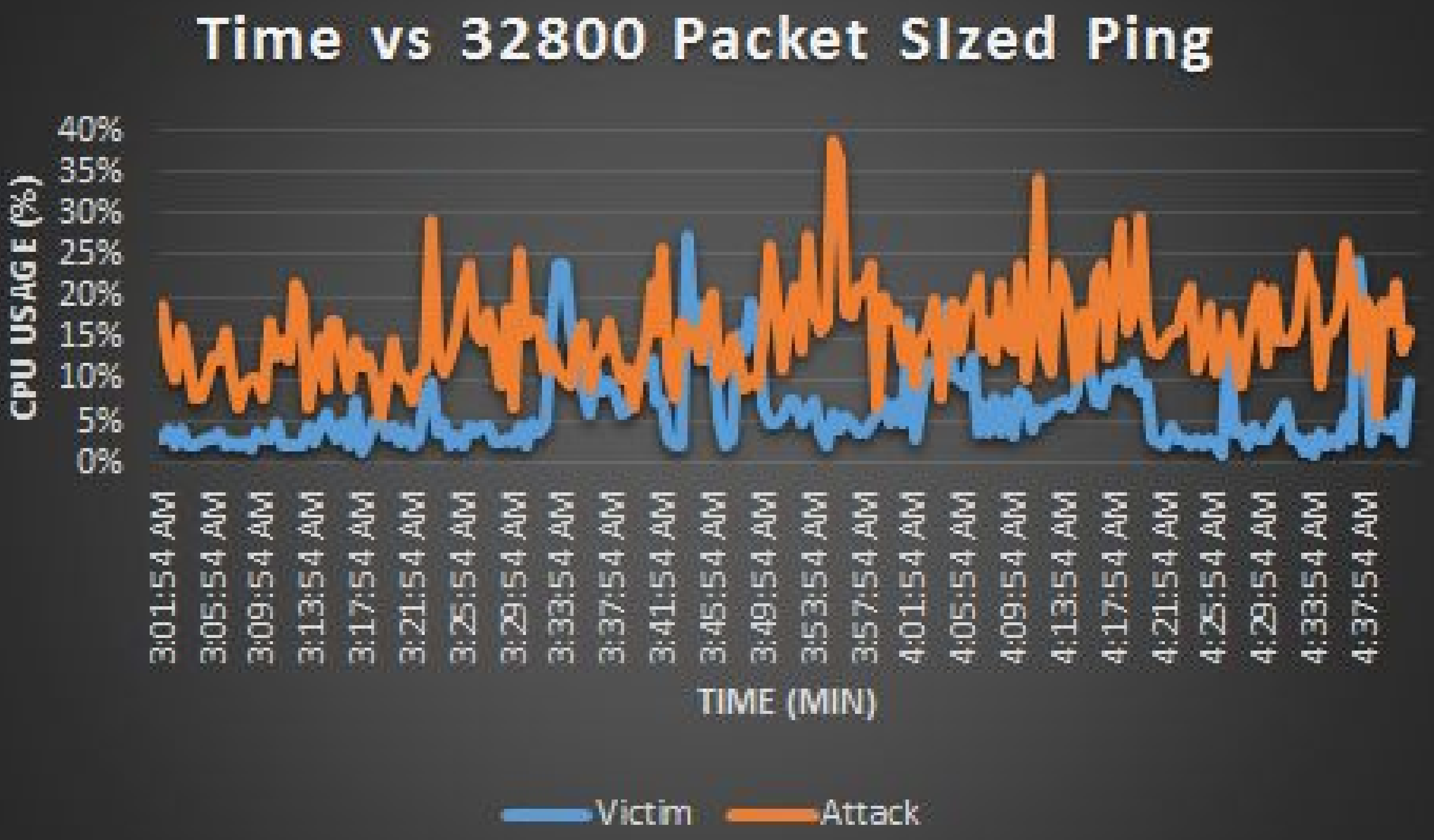
Dependent Variables: CPU usage on “attacker” and “victim”

Controlled Variables: Hardware, time

Constant Variable: Location, Network, Software

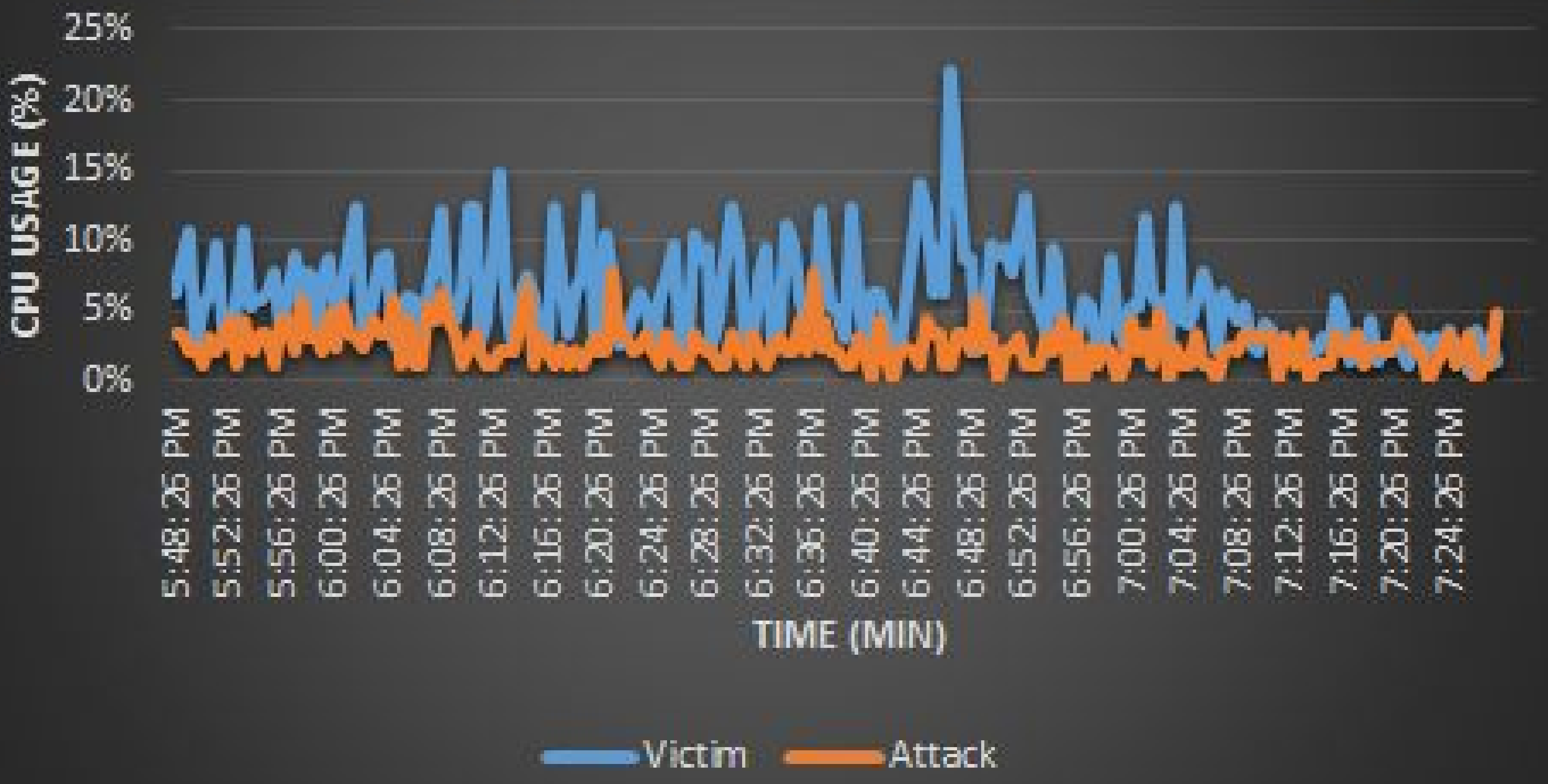
1. Run mpstat on all machines for 20 minutes to collect data on CPU behavior
2. Use hping3 on machine A to hit machine B for 1 hour at packet size 64, 32800, 65536
3. Keep running mpstat for 20 minutes to collect data on CPU behavior
4. Repeat 3 times EACH


Time vs 64 Packet SIzed Ping
VICTIM CPU USAAG E (%)
40%
35%
30%
25%
20%
15%
10%
5%
0%
ATTACK CPU USAG E (%)
900%
800%
700%
600%
500%
400%
300%
200%
100%
0%
12:06:58 PM
12:11:28 PM
12:15:58 PM
12:20:28 PM
12:24:58 PM
12:29:28 PM
12:33:58 PM
12:38:28 PM
12:42:58 PM
12:47:28 PM
12:51:58 PM
12:56:28 PM
1:00:58 PM
1:05:28 PM
1:09:58 PM
1:14:28 PM
1:18:58 PM
1:23:28 PM
1:27:58 PM
1:32:28 PM
1:36:58 PM
1:41:28 PM
1:45:58 PM
TIME (MIN)
Victim
Attack



Time vs 32800 Packet SIzed Ping

Time vs 65536 Packet SIzed Ping



Conclusion

- Restate Hypothesis
- Results
- What I learned
- Places of Error

Ways to Improve

- Include Router info: temp(Before /After), make, model
- Run project multiple times on school network
- Incorporate more tools WireShark, Zenmap, Metasploit etc
- Create online web app to attack and receive data from using autorun
- use cron jobs -_-
- Make a connection between time between pings
- Use faster/updated hardware
- Vary packet types: TCP, SYN, etc

Sources

(Incapsula) https://www.incapsula.com/ddos/attack-glossary/ping-of-death.html

(Tutorials Point) https://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm

(MTU) http://searchnetworking.techtarget.com/definition/maximum-transmission-unit

(More Man) http://www.brocade.com/content/html/en/vrouter5600/40r1/vrouter-40r1-basicrouting/GUID-E5899838-542B-4A56-9A40-F66640BA58B8.html

(IP) https://www.reddit.com/r/sysadmin/comments/2syqts/relaible_ip_to_ping_not_8888_or_4222/

(Hping3 Help) http://0daysecurity.com/articles/hping3_examples.html