PEIMA: Using Power Laws to address Denial of Service Attacks

REDEZEM

Who Am I?

- Stefan Prandl
- PhD student, Curtin University
- That's in Perth, Australia
- Networks and Network Security
- Also work with ES2 as a security consultant
- Been breaking stuff since a young age

Contents

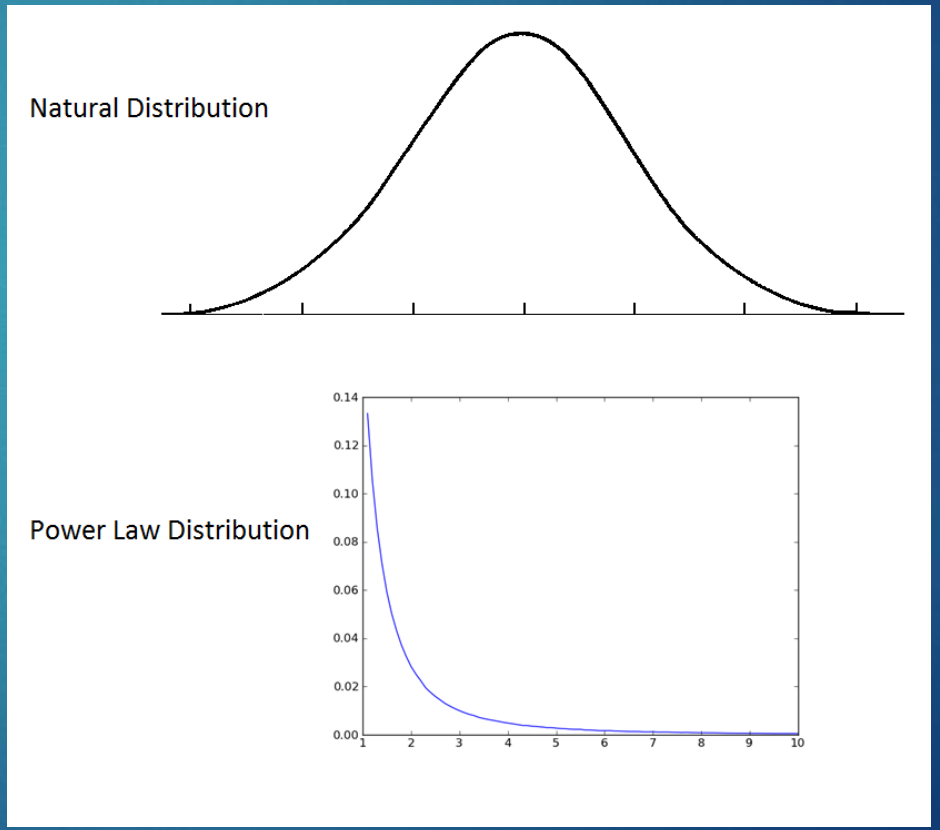
- The stuff you've just seen
- Introduction to Power Laws
- What we've been doing; DDoS Defence
- What else you can do:
  - IDS
  - Diagnostics
  - User ID-ing
- Then we'll look at this tool thing I've thrown together
- Demo of what you can do

Introduction to Power Laws

Or more honestly, power law probability distributions

That's a mouthful though

- Natural processes, they're statistical
- Things descriptive of natural processes follow power laws
- When they don't, something's wrong
- Not all natural processes are natural!
- Eg., Financial transactions
- You can use power laws to detect fraud.

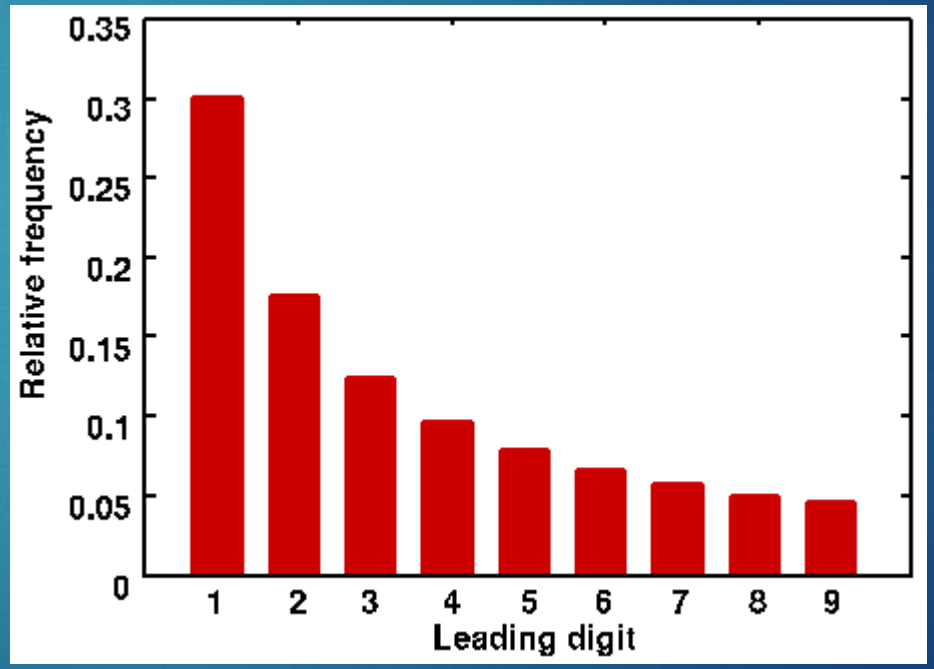


Why does that matter?

- Somehow network traffic is "natural"
- Good lord the machines are alive!
- So power laws must apply
- If they don't, something is wrong
- Some power laws can be hard coded
- Extremely fast and low cost anomaly detection!

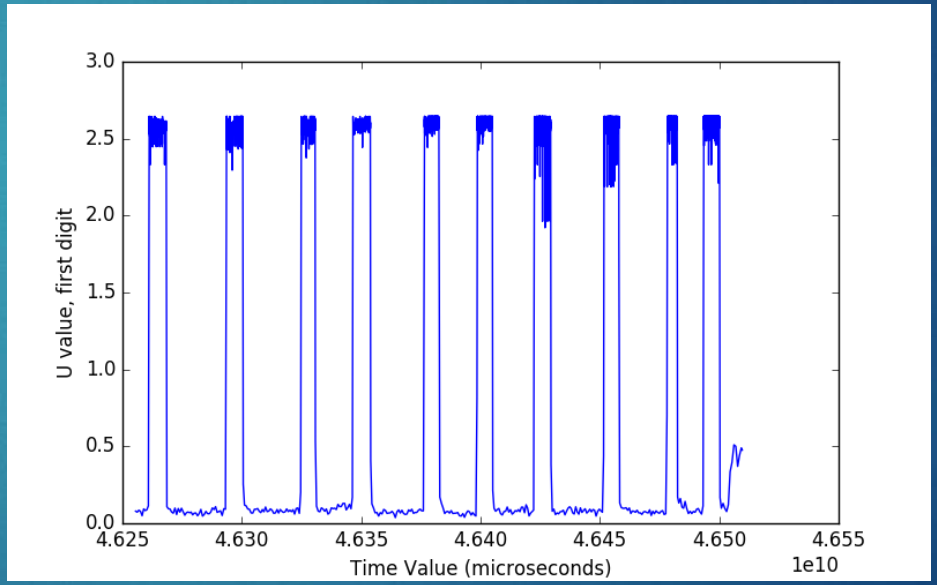
Benford's Law

- Simple and awesome power law
- If it's a number…
- Generated by a process…
- Process is natural…
- We know what the probability of the first digit is!
- Never changes, you can hard code it.
- Such speed. Wow.



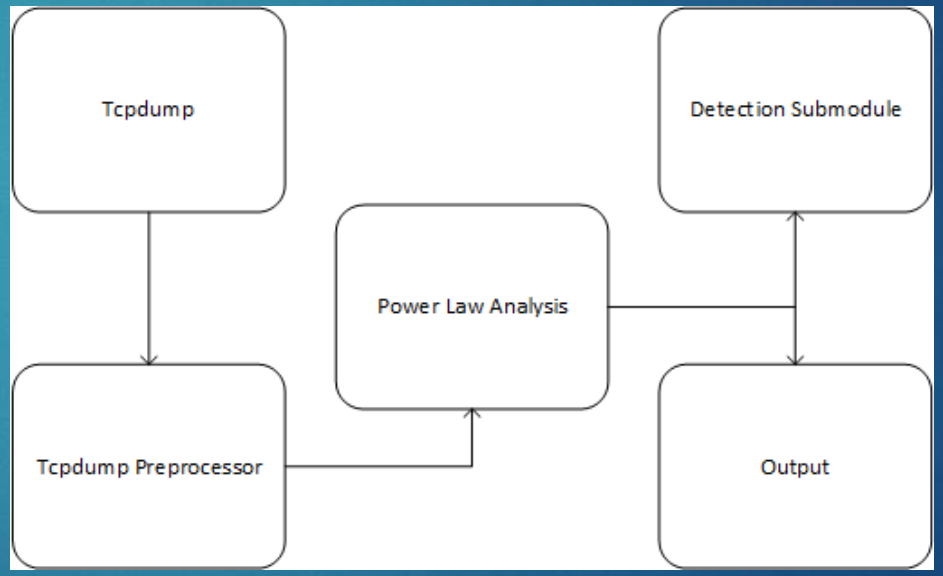
What we've been doing: DDoS Defence

- The more artificial the packet, the worse the anomaly
- Flood DDoS (Amplification, tcp, udp, http, etc attack) are very loud
- Can be clearly seen in gestalt connection data
- Practically instantaneous
- Real time in 100Mbit/1000Mbit scenarios (probably much more)
- No training at all



How we do it

- Detection processes Tcpdump data
- Extracts features
- Power law analysis tells us "Goodness"
- Print out to csv with timestamp
- Or throw an alarm and do something
- Iptables maybe.

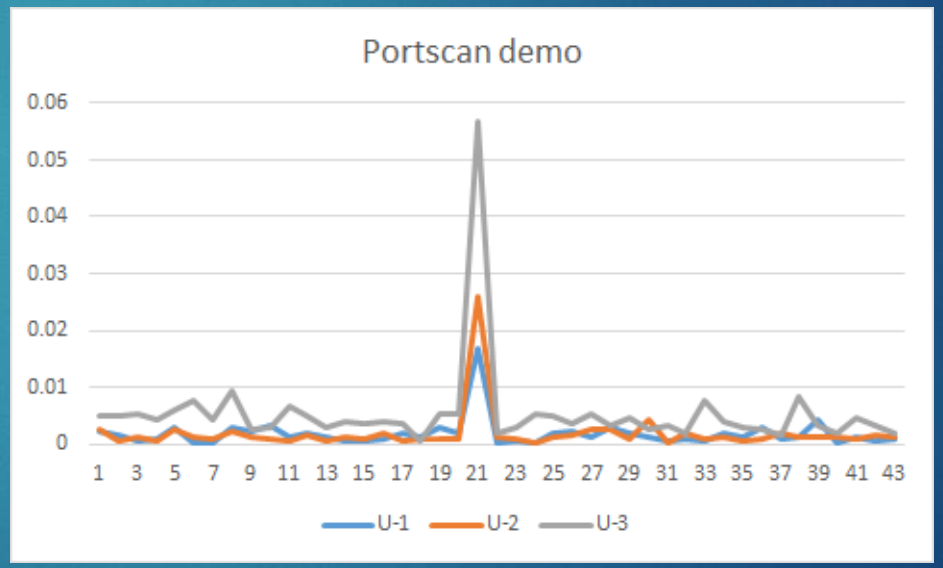


What you can do with that

- Watch for DDoS attacks
- Probably won't save your network
- Can determine if someone is using your pc
- "DDoS zombie!" instead of "WTF is this"
- Determine between attack types too

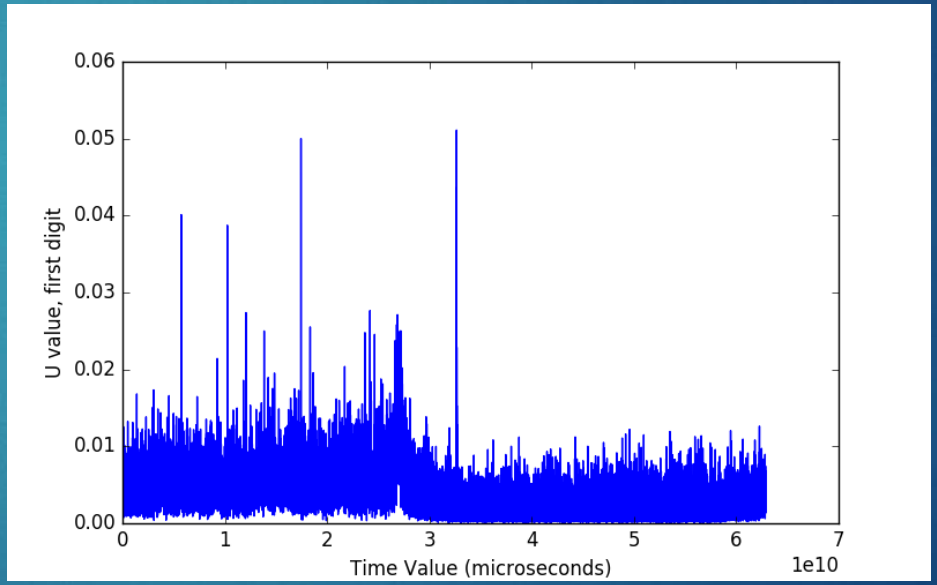
What else you can do: IDS

- DoS isn't the only kind of disturbance on a network
- Obviously we don't know what all of them are
- Strap learning agent to output
- Tell it to make decisions
- Should (at the very least) detect active recon, even at slow speeds



What else you can do: Diagnostics

- Changes in traffic across a network change “power law profile”
- Are all the changes where you expect?
- Is someone doing something to your systems when they’re not around?



What else you can do: User ID-ing

- Natural systems aren't just networks!
- User interaction with computer is too
- You can profile their keystrokes
- Profile *your* keystrokes
- Have your own laptop/pc as a honeypot.

What else you can do: Probably Lots More

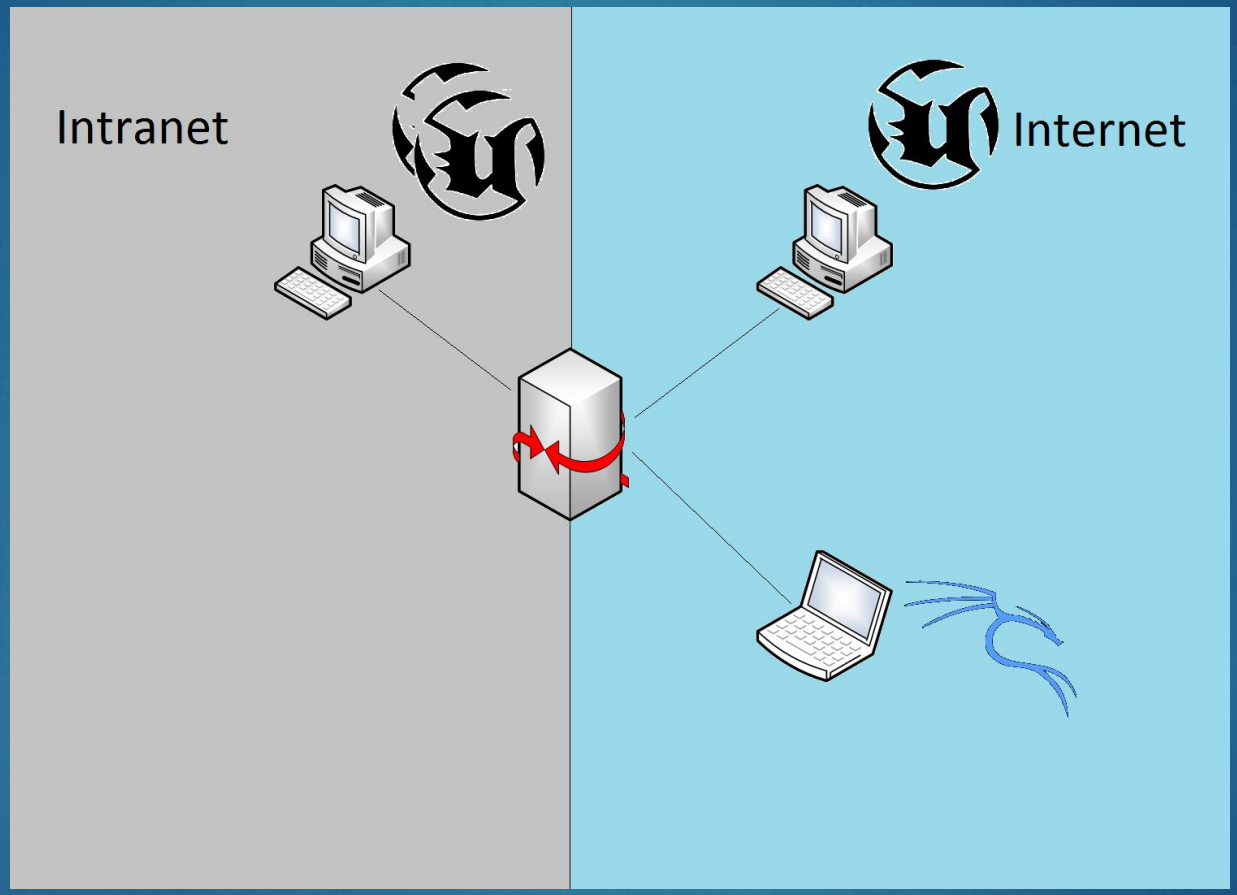
- Very early days for power law based analysis
- Possible that all kinds of computer metrics are power law compliant
- Experiment!
- It's cheap, fast, and simple, so why not?

And now, a tool that you can go experiment with

GET IT AT HTTPS://BITBUCKET.ORG/REDEZEM/PEIMAULTRALITE

And now, a magic trick

BROUGHT TO YOU BY THE POSSIBILITIES OF POWER LAW ANALYSIS


Intranet
Internet

Thanks To…

Also contact me: redezem@gmail.com

- Thanks to my supervisory team
  - Curtin University
    - Assoc. Prof Mihai Lazarescu
    - Dr Sonny Pham
    - Dr Sie Teng Soh
  - Oklahoma State University
    - Professor Subhash Kak
- And big thanks to my engineering team that built the demo
  - Luke Healy
  - Josh Yeo
  - Jordan Truswell