black hat®

USA 2017

JULY 22-27, 2017

MANDALAY BAY / LAS VEGAS

#BHUSA / @BLACKHATEVENTS

PEIMA: Harnessing Power Laws to Detect Malicious Activities from Denial of Service to Intrusion Detection Traffic Analysis and Beyond

Stefan Prandl

Who am I?

- Stefan Prandl, PhD Student, Curtin University
- From Perth, Western Australia
- Work on network security threat detection

Curtin University

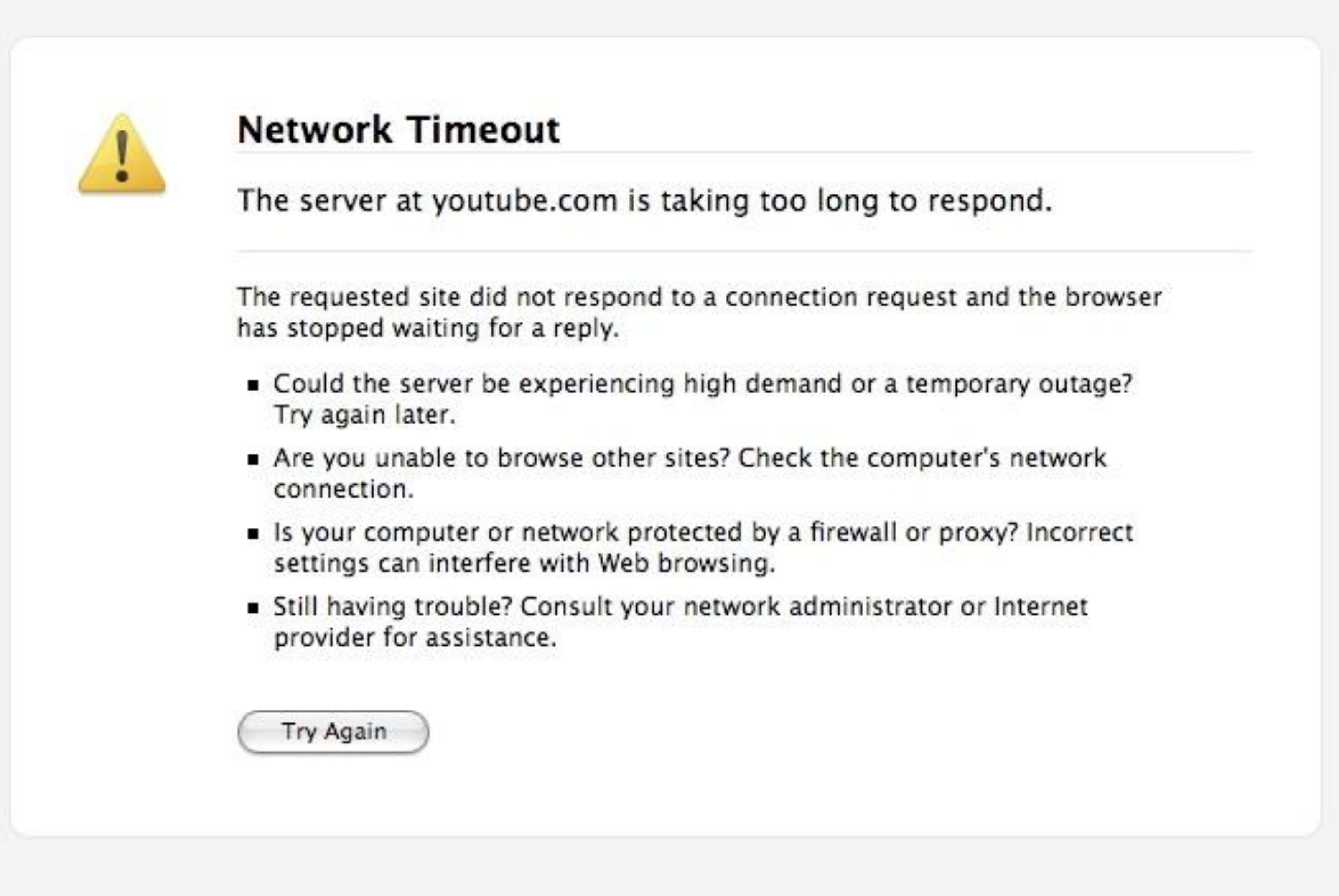
Who am I?

- Stefan Prandl, PhD Student, Curtin University
- From Perth, Western Australia
- Work on network security threat detection
- Stefan.Prandl@curtin.edu.au

Curtin University

Research Team:

- Curtin University:
  - Mihai Lazarescu
  - Duc-Son Pham
  - Sie Teng Soh
- Oklahoma State University:
  - Subhash Kak



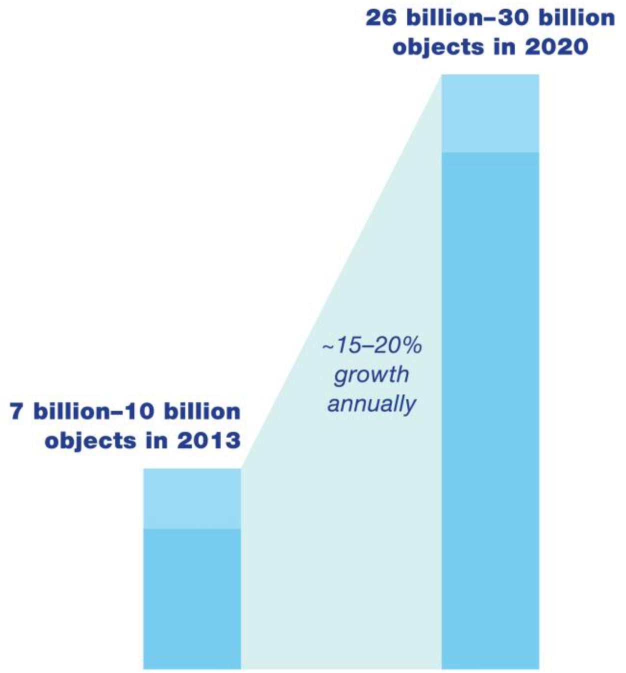
Network Timeout

The server at youtube.com is taking too long to respond.

The requested site did not respond to a connection request and the browser has stopped waiting for a reply.

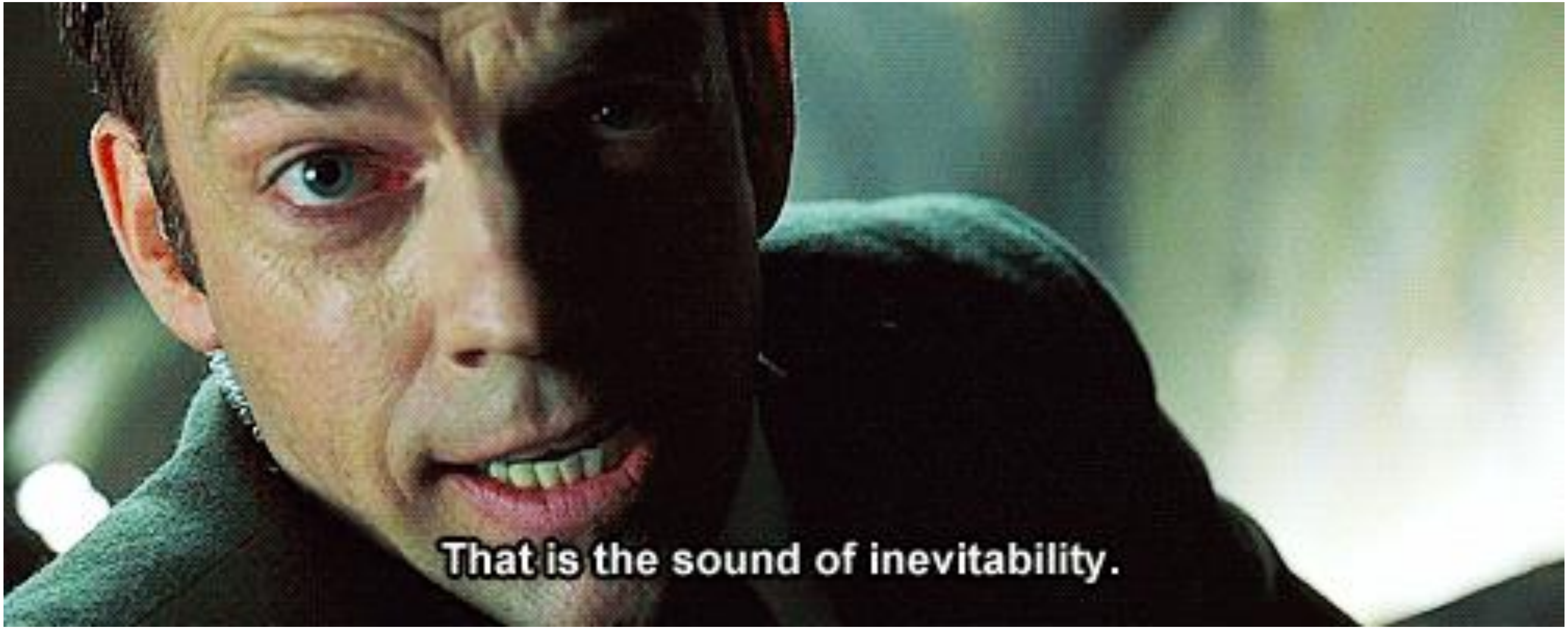
- Could the server be experiencing high demand or a temporary outage? Try again later.
- Are you unable to browse other sites? Check the computer's network connection.
- Is your computer or network protected by a firewall or proxy? Incorrect settings can interfere with Web browsing.
- Still having trouble? Consult your network administrator or Internet provider for assistance.

Some 30 billion objects may be connected to the Internet of Things[1] by 2020.



[1] A networking of physical objects via embedded devices that collect and/or transmit information.

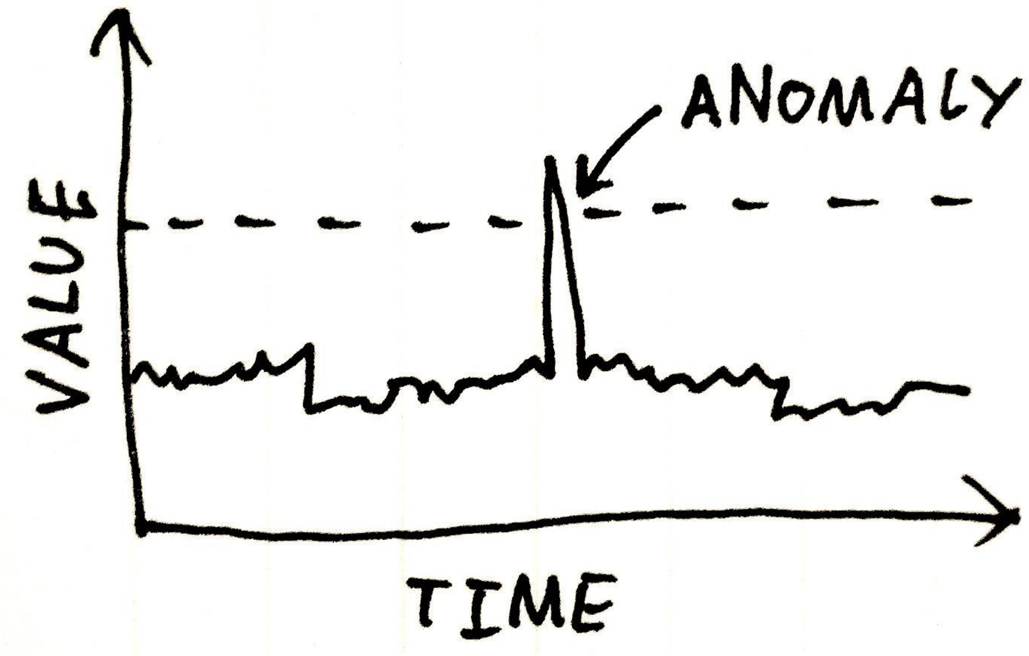
Source: Forecasts derived from ABI Research; expert interviews; Gartner; IDC; McKinsey analysis


That is the sound of inevitability.

What can we do?

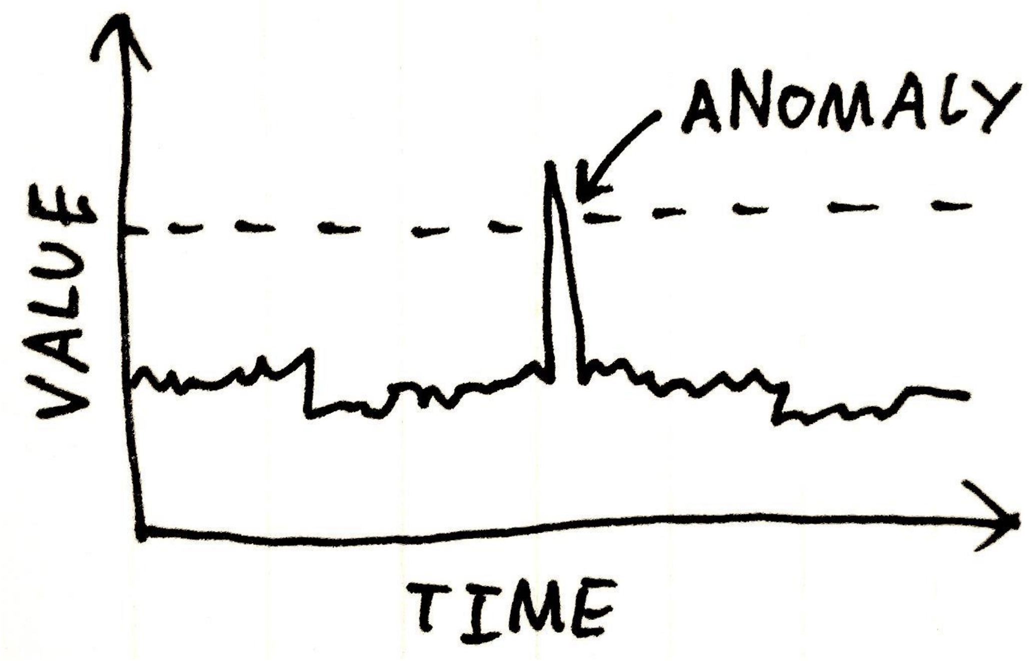
IDS Systems!

Let AI solve our problems for us!



Let AI solve our problems for us!

…. Or not



Introducing PEIMA

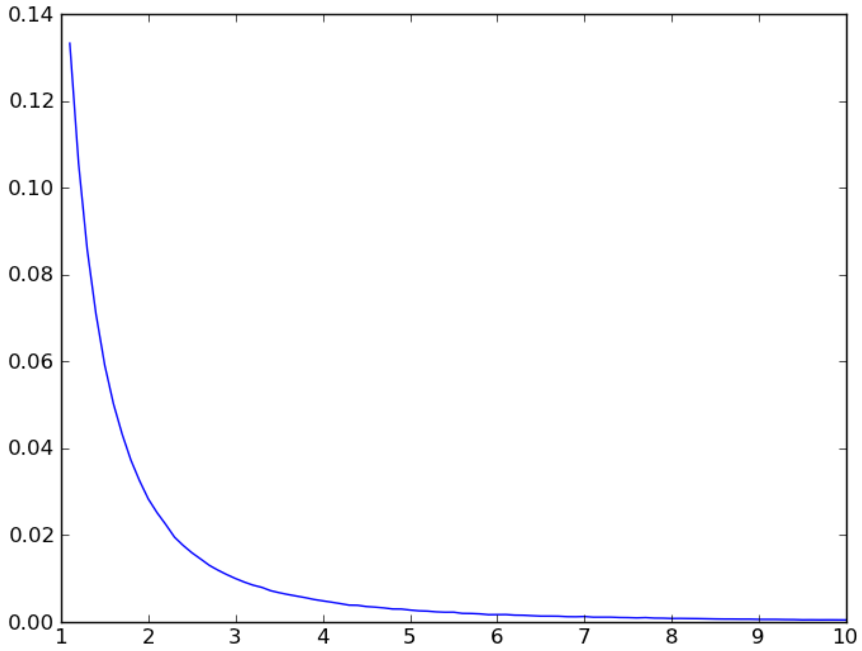
Probability Engine to Identify Malicious Activity

- Detects attacks within microseconds
- Accurate
- Uses only metadata
- No learning

What can it do?

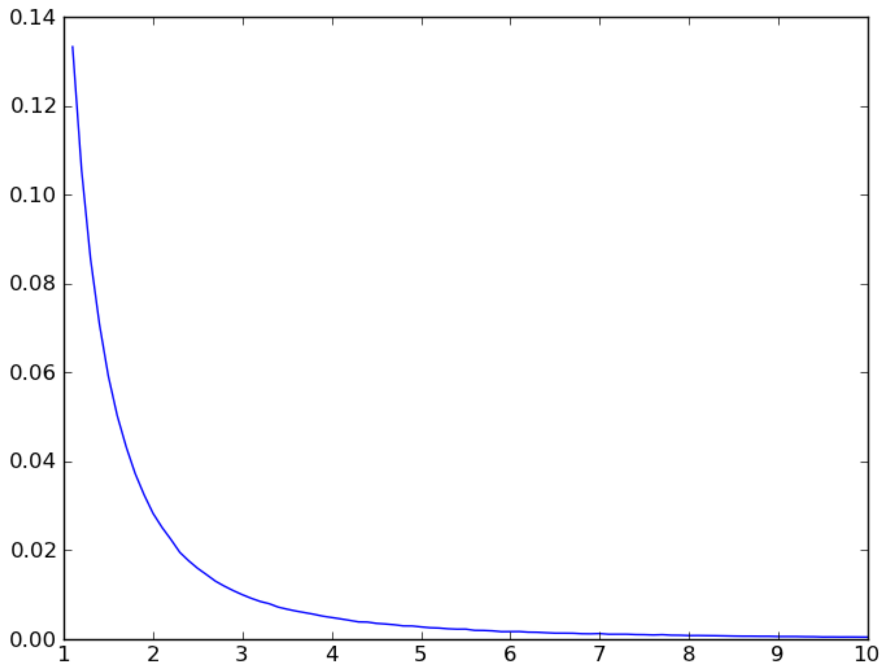
How?

- Uses power law distributions
- Detects the "naturalness" of traffic
- Unnatural traffic is attack traffic!



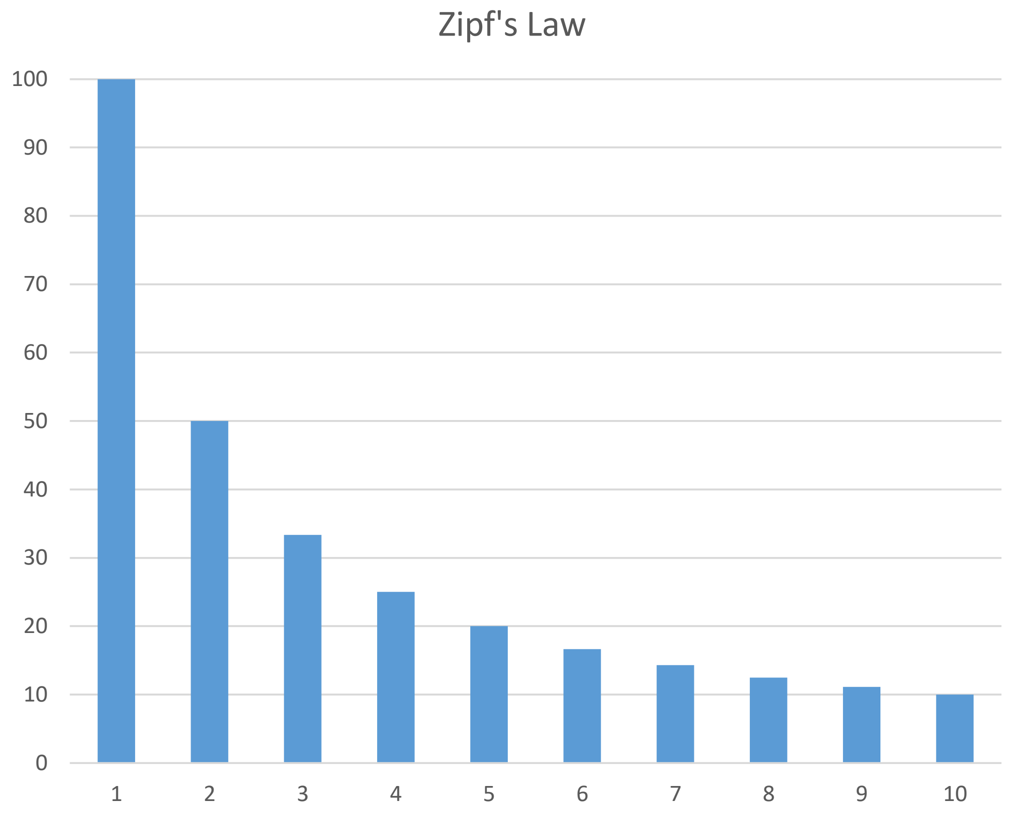
Power Law Probability Distributions

- Continuous power law distribution
- The one on which all others are based
- 80/20 principle
- Not as applicable as other power laws



Pareto Distribution

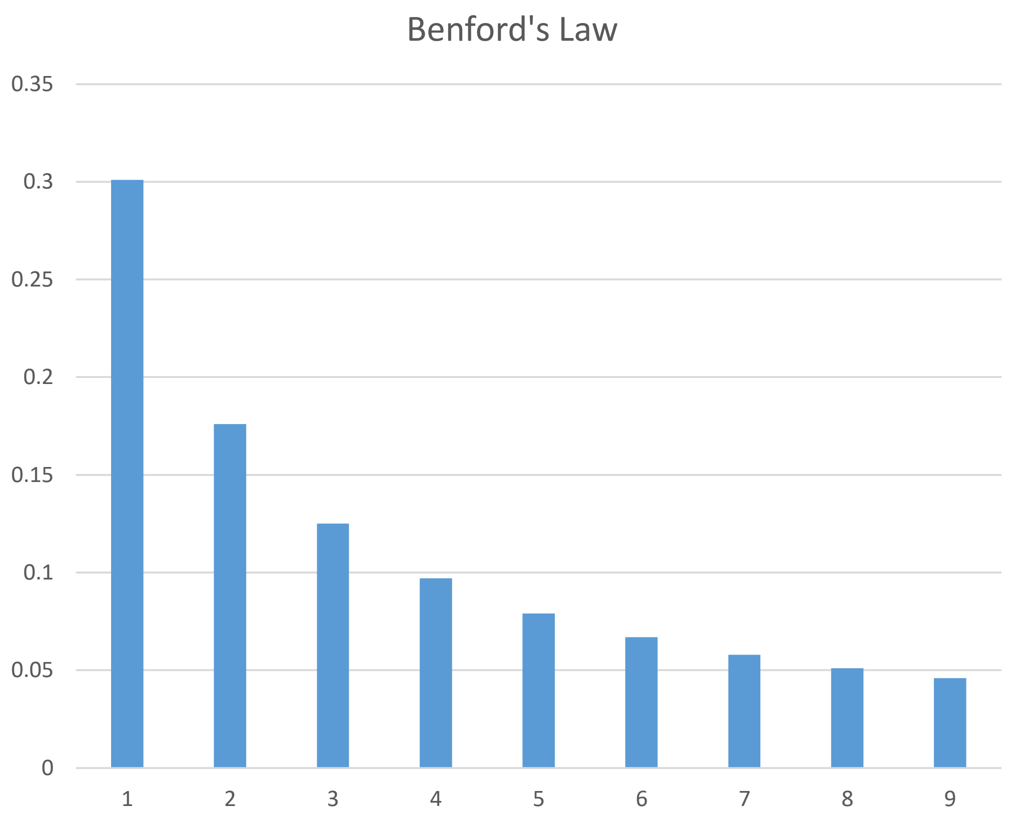
- Relates popularity to frequency
- Exponential decay
- Applies to all sorts of weird situations



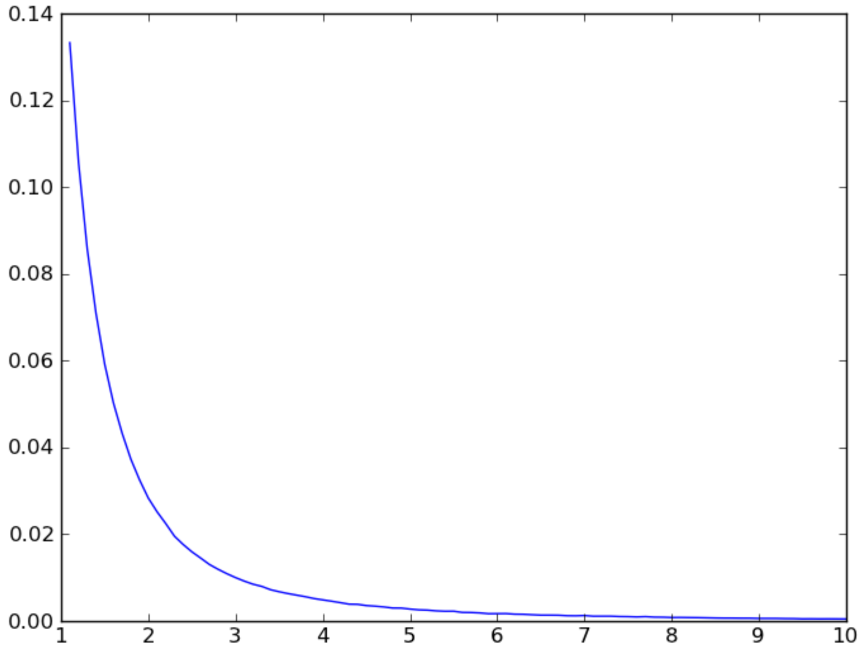
Zipf’s Law

- Is a description of what the first digit of a number will be
- Never have to calculate it, it’s always the same.
- Used in detecting bank fraud for years

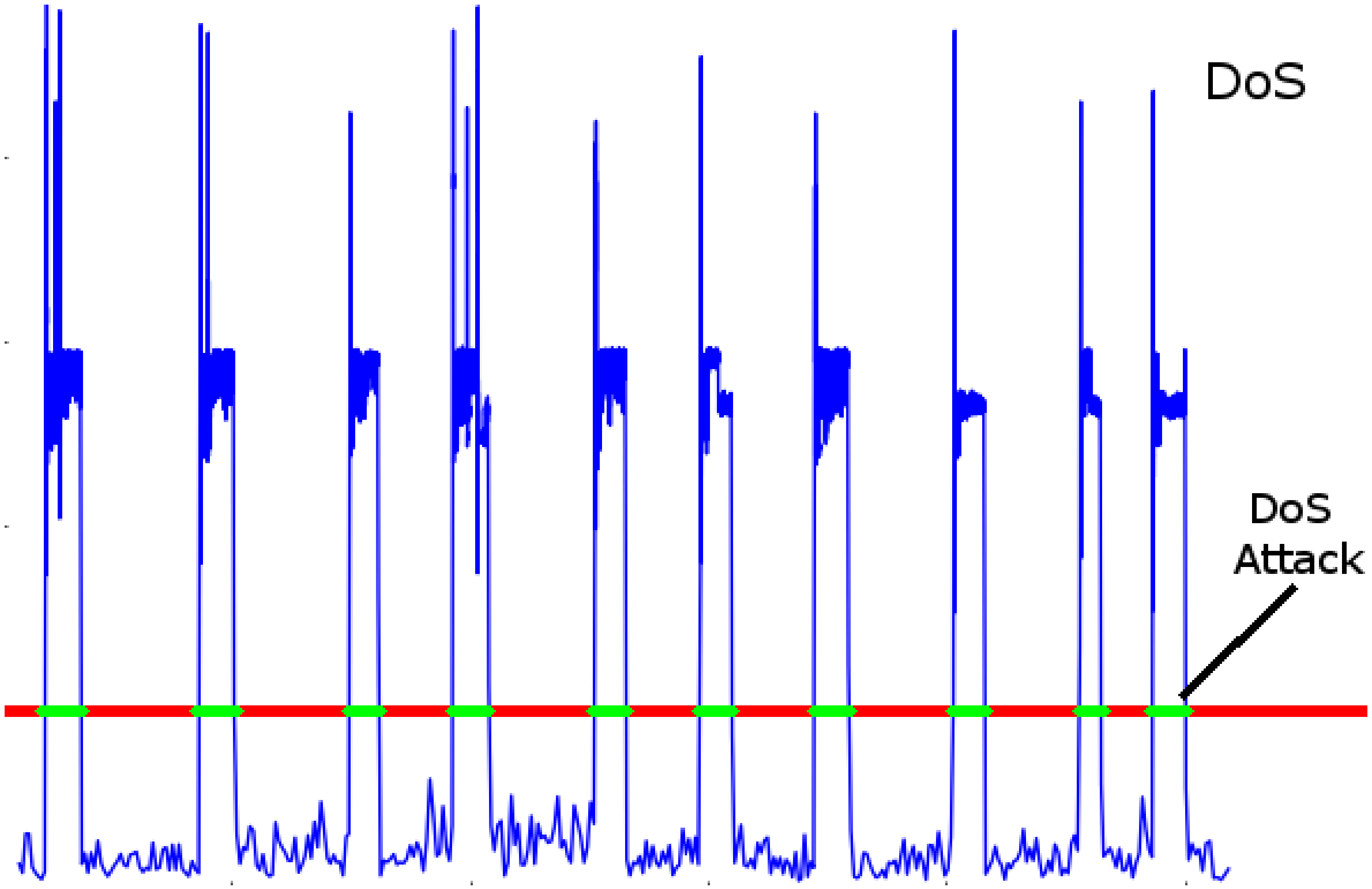
Benford’s Law

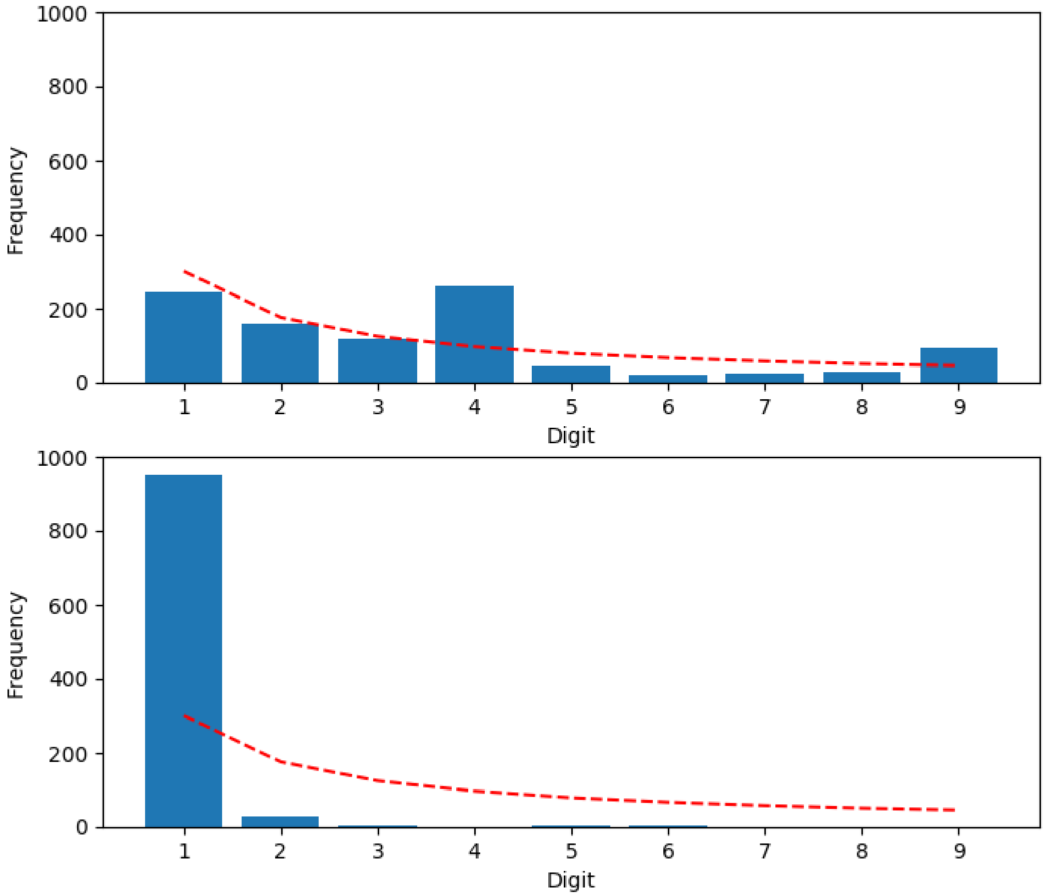


- So we can use power laws to detect “Fraud”, or in this case DoS/DDoS!
- Metadata follows various power laws!
- Just have to check if they match.



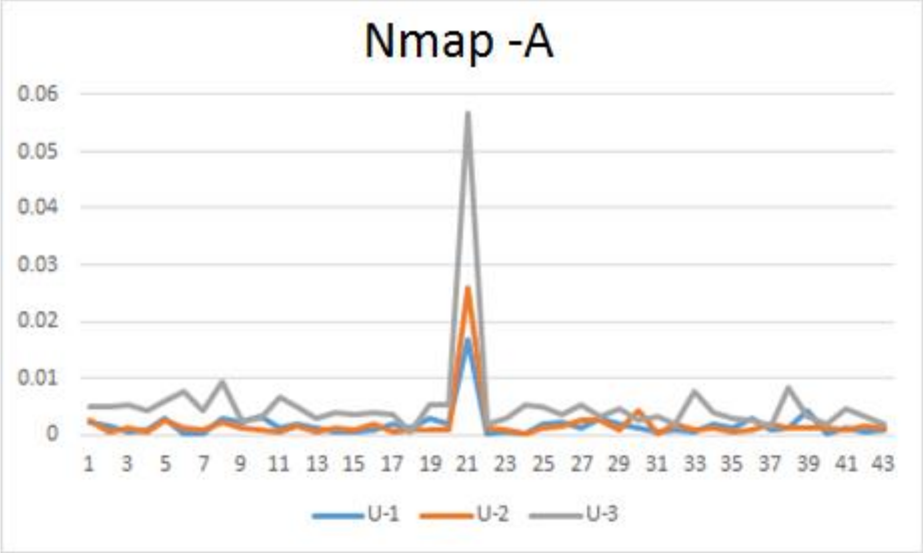
Network traffic is natural!


DoS
DoS Attack


1000
800
600
400
200
0
Frequency
1
2
3
4
5
6
7
8
9
Digit
1000
800
600
400
200
0
Frequency
1
2
3
4
5
6
7
8
9
Digit

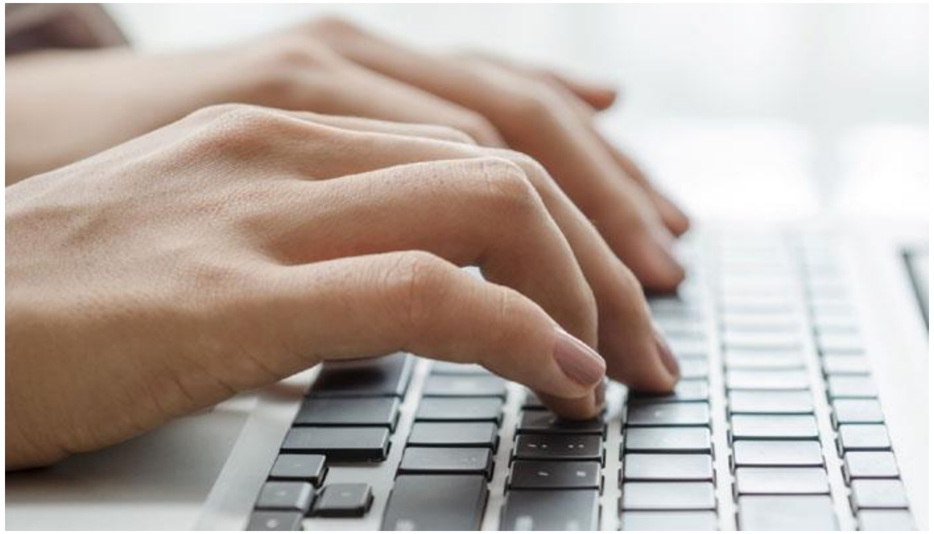
But wait, there’s more!

- Attacks appear to be detectible too
- Any significant activity that changes a network is detectable
- Nmap, brute force, for example



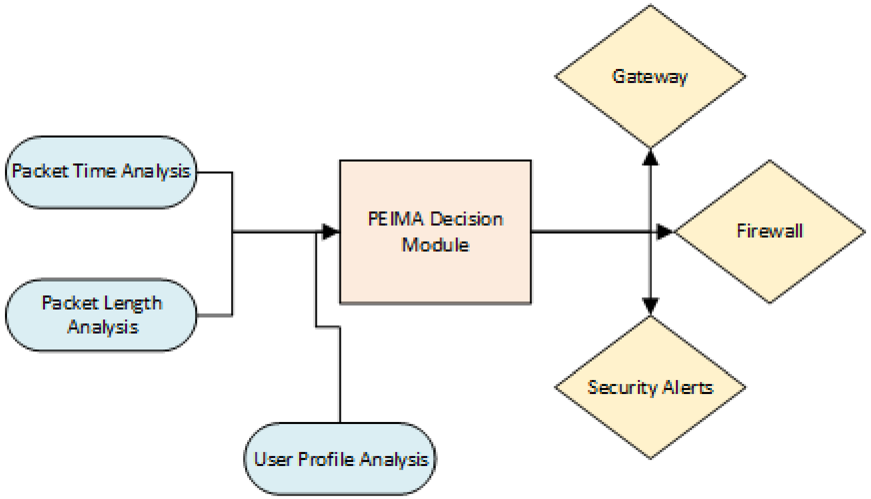
This can be an IDS too!

- Benford’s, Zipf’s laws are sensitive to changes in a system
- Can create unique profiles of users
- Are sensitive to when they change
- Thanks to power laws, are hard to fool too!



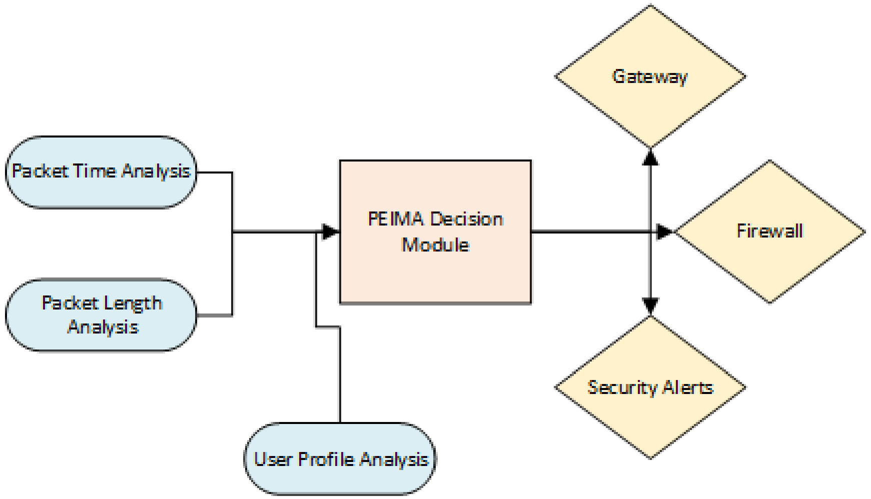
User Profiling

- Is very lightweight
- Can run just as software
- Fully integratable into current systems



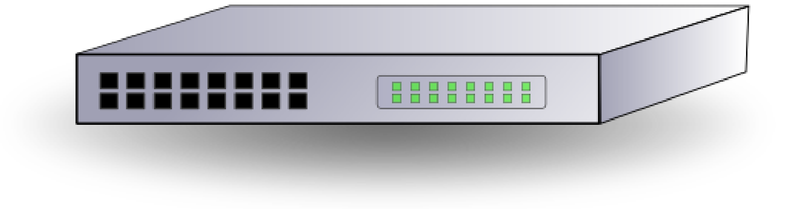
How do I use this though?

- Gather metadata
- Create windows
- Perform analysis
- Make decisions



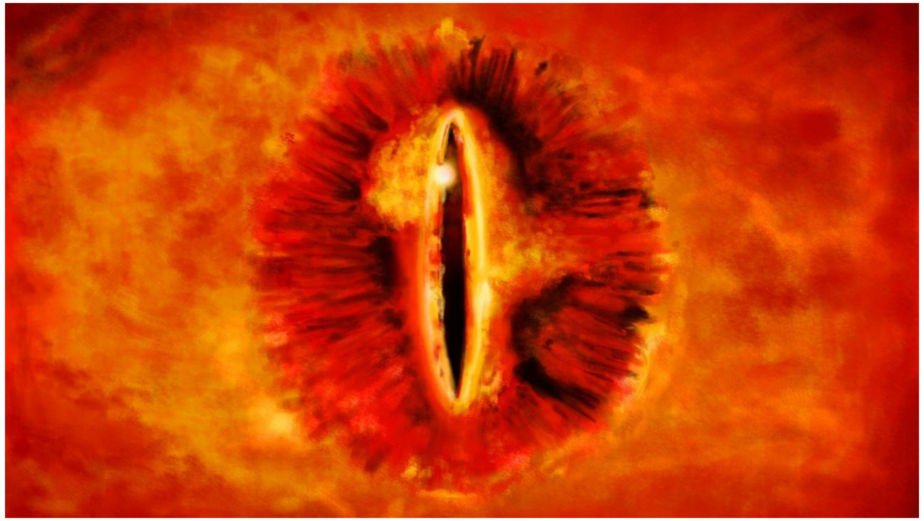
PEIMA framework

- Running on a gateway
- Detects DoS/DDoS
- Configures Iptables to adapt
- Silent DoS mitigation



Example One

- Running alongside SIEM
- Performs analysis to assist SIEM alert generation
- More accurate alerts
- Better alert severity



Example Two

- Very early days for power law based analysis
- Possible that all kinds of computer metrics are power law compliant
- PEIMA solutions are coming.

Conclusions

Black Hat Sound Bytes

A brand new and fast method of detecting DoS/DDoS attacks.

How to implement a PEIMA system.

A new, power law based way of analysing networks.

Thank you!

Contact @ Stefan.Prandl@curtin.edu.au