RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

InetVis – Visualising Scans and Evaluating Scan Detection

Barry Irwin and Jean-Pierre van Riel

Security and Networks Research Group
Department of Computer Science
Rhodes University

VizSEC '07 Presentation - October 29th, 2007

Sponsored by

Telkom · COMVERSE · Business Connexion · THRIP TECHNOLOGY AND HUMAN RESOURCES FOR INDUSTRY PROGRAMME · STORTECH For Your Information · tellabs · VERSO TECHNOLOGIES · amatole telecommunication services · Bright Ideas Projects

Overview

- Why bother with scan detection?
- IDS and scan detection
- InetVis
  - Concept
  - Visualising different types of scans with InetVis
  - Key features
- Network telescope traffic
- Results
  - False negative for Snort
  - Pseudo-random phenomena
    - Backscatter or stealth scan?
- Conclusion and questions

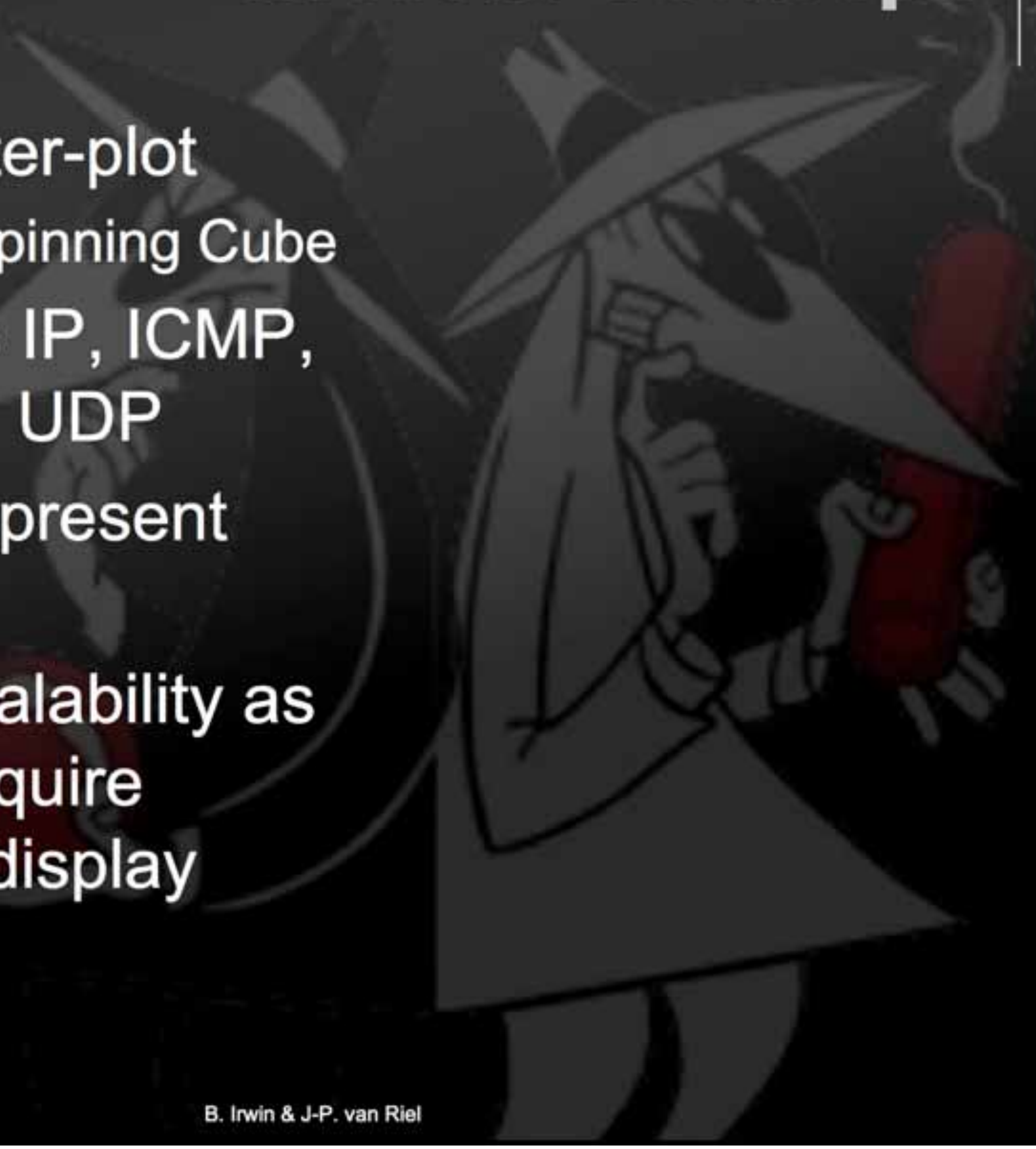
To detect scans or not?

- Arguments against
  - Scan activity is very prevalent but only a vague indication of threat
  - Actual exploit attempts warrant more concern
- Arguments for
  - Detect worm activity without reliance on signatures (and identify infected sources)
  - IPS application – preemptively block scanners (but be careful about DoS)

IDS scan detection

- Snort and Bro are two popular open source IDS solutions
- Both have scan detection algorithms
  - Simply count unique destination IPs and ports
  - Alert at thresholds
  - Include time thresholds
  - Snort’s ‘sfportscan’ detector has 3 preset threshold levels – ‘low’, ‘medium’ and ‘high’
  - The Bro scan policy facilitates variable and multiple thresholds

InetVis concept



- 3-D scatter-plot
  - Lau's Spinning Cube
- Supports IP, ICMP, TCP and UDP
- Points represent packets
- Good Scalability as points require minimal display space

RHODES UNIVERSITY

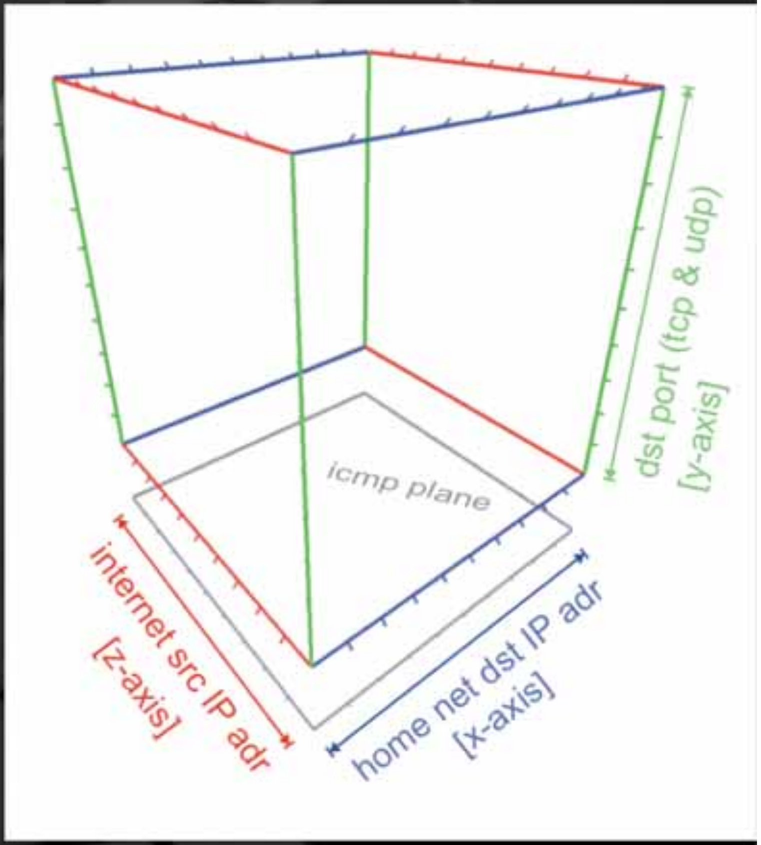
Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

InetVis concept

- 3-D scatter-plot
  - Lau's Spinning Cube
- Supports IP, ICMP, TCP and UDP
- Points represent packets
- Good Scalability as points require minimal display space

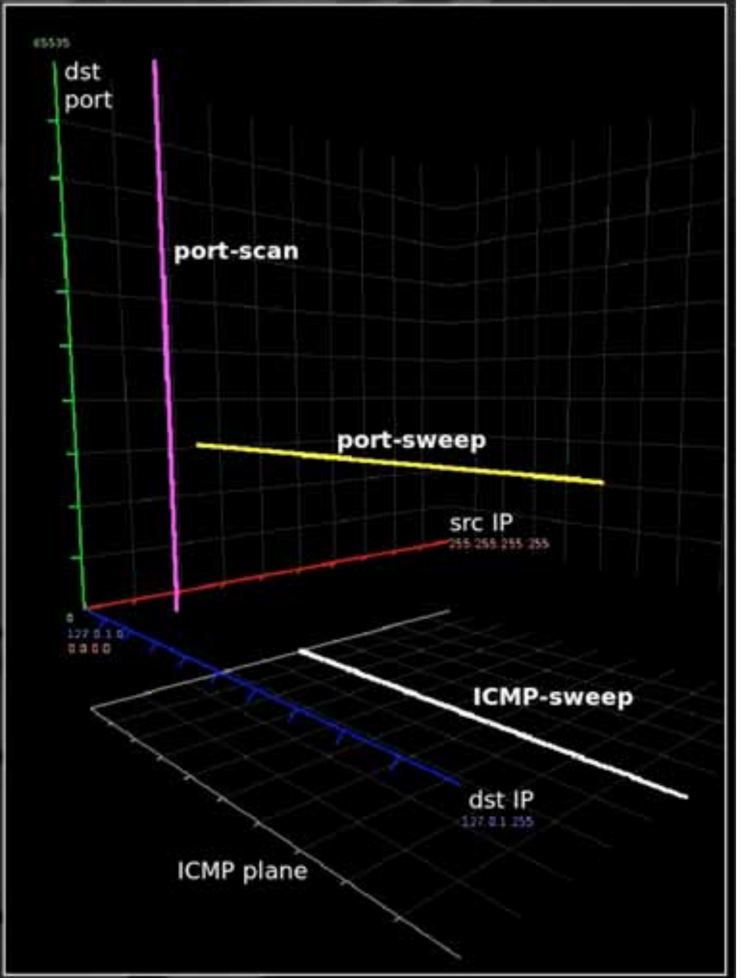


InetVis key features

- Scaling into network and port ranges
- Logarithmic port axis option
- Time-frame control with replay position and time-window
  - Time-window acts as a filter
- Time-scaling (replay rate)
  - Min = 0.001x = 1 millisecond per second
  - Max = 86400x = 1 day per second
- Transparent decay and new event pulse
- Colour schemes and BPF filtering

Conventional scan types

- Generated with nmap
- Colour by protocol
  - TCP, UDP, ICMP
- Port-scans
  - Vertical
  - Targets host
- Address-scans
  - Horizontal
  - Targets network
  - Port-sweep (TCP/UDP)
  - ICMP-sweep



Rhodes University

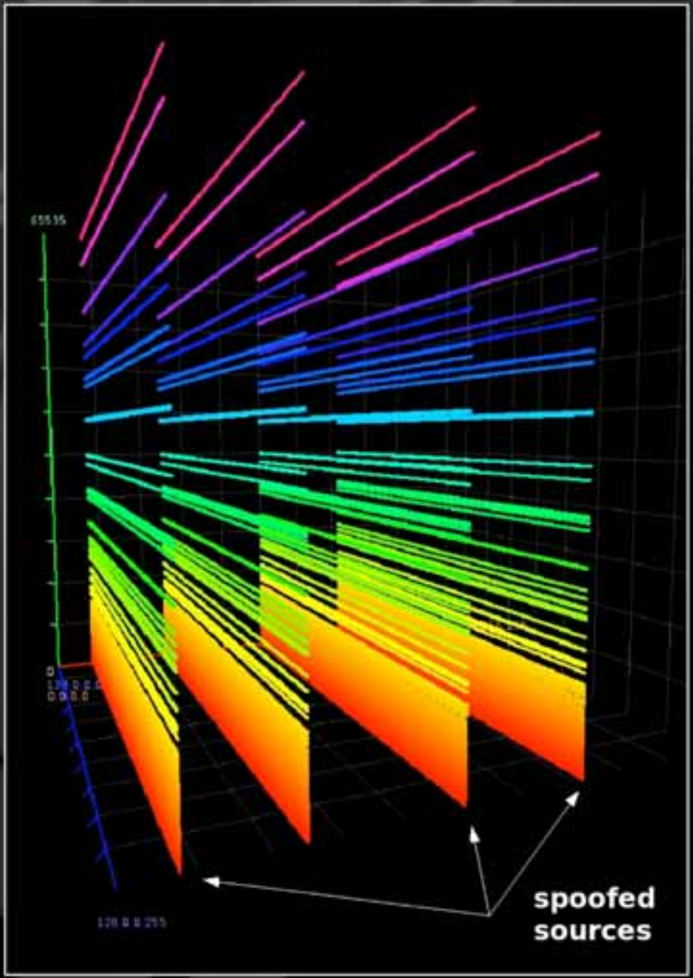
Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

Other types of scans

- 'Grid-sweeps'
  - Combination of port-scan and port-sweep
  - Targets network and hosts for multiple vulnerabilities
- Evasion-techniques
  - Slow
  - Randomized
  - Distributed between sources
  - Spoof multiple sources as decoys



spoofed sources

Network telescope data

- Unallocated/empty address space
  - Class C network telescope (our NetScope)
  - Since August 2005
  - 6.6 million packets captured in 2006 (65% TCP, 20% UCP, 15% ICMP)
- Passive monitoring
  - No responses
  - No connections initiated
- Less traffic to deal with
- Less worry about false positives
- Observations limited to scans and backscatter
  - Address-scans are most common as most port-scans first establish presence of target

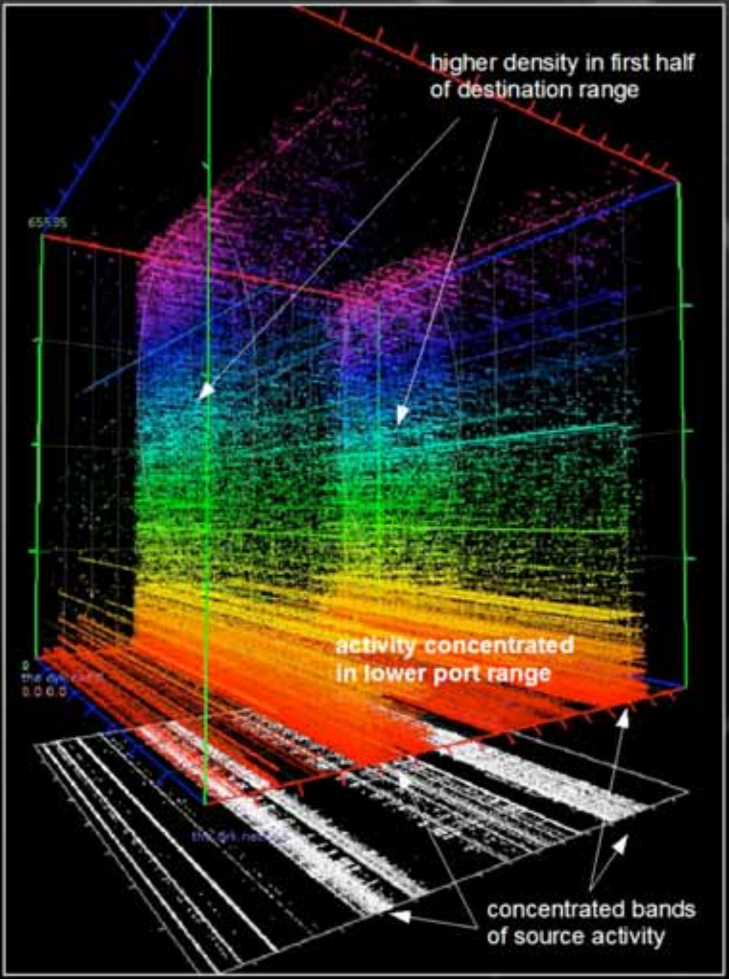
RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

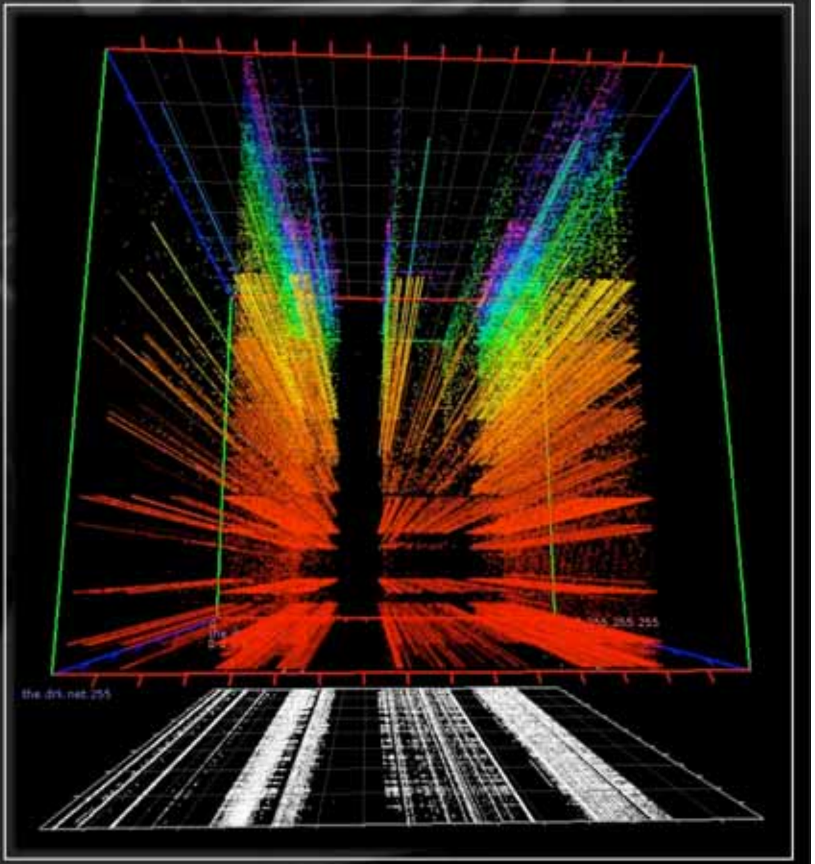
Network telescope data for 2006 visualized



higher density in first half of destination range

activity concentrated in lower port range

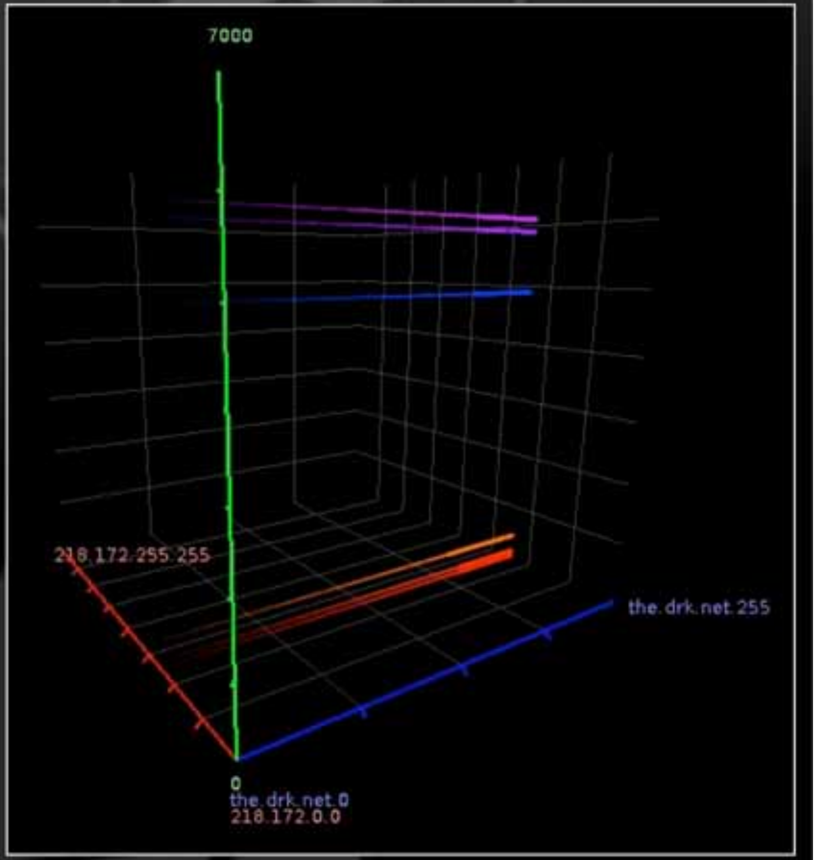
concentrated bands of source activity



Logarithmic plot

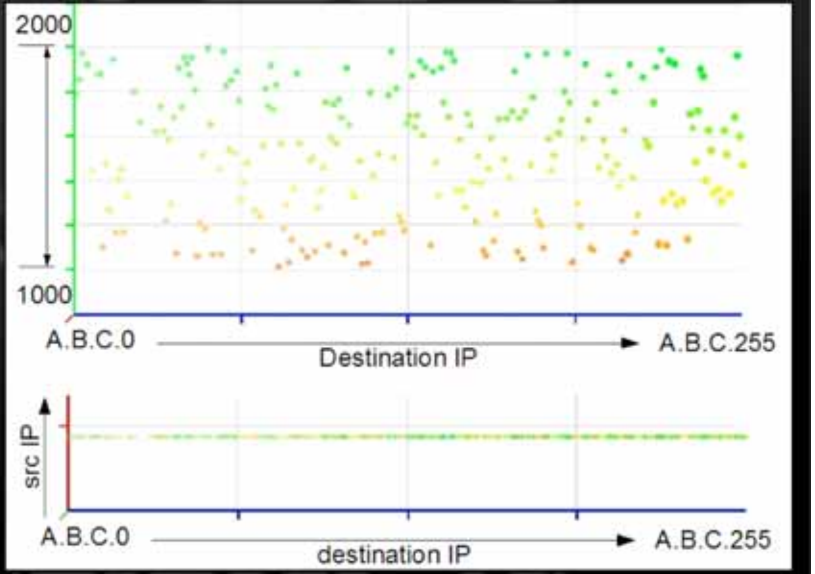
Snort False Negative

- 6 simultaneous port-sweeps
  - All ports have known vulnerabilities
- Snort fails to alert
  - flaw in counting unique destination addresses and ports
- Snort does alert on just one port-sweep



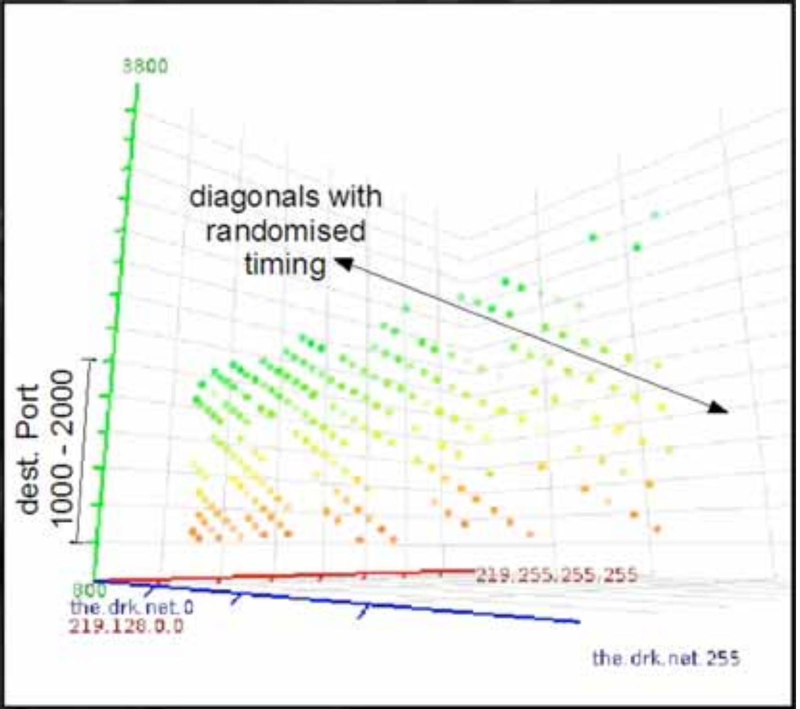
Pseudo-random Patterns – backscatter or stealth scan?

- Scattered between port 1000-2000
- Very rapid (50ms)
- Each packet strikes a unique IP address
- Source port 80 with SYN/ACK flags set
- Pattern can be detected by Bro* as an address scan
- Not detected by Snort



Pseudo-random Patterns – backscatter or stealth scan?

- Also occurs between port 1000 and 2000
- Much slower (36hr)
- Less random, with clear diagonal pattern
- Not every packet hits a unique address



Conclusion (and Future Work)

- Without the insights provided by InetVis, the flaw in the Snort IDS would not have been discovered
- Future work
  - Add scan detection overlay that superimposes detected scans over the backdrop of the raw traffic
  - Evaluate additional scan detection algorithms

Questions?

Barry Irwin

- b.irwin@ru.ac.za
- Project supervisor

Jean-Pierre van Riel

- jp.vanriel@gmail.com
- Final year M.Sc. Student