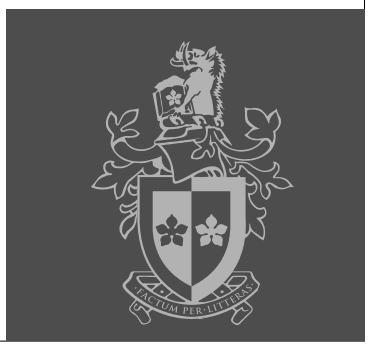
SWINBURNE

CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Defining and Evaluating Greynets (Sparse Darknets)

Warren Harrop,
Grenville Armitage

{wazz,garmitage}@swin.edu.au



Outline

- Darknet Background
- Previous work
- Enterprise and campus darknets
- Terminology
  - Defining and characterising a greynet
  - Terms and definitions
- Analysis
  - Establishing the efficacy of a greynet
- Conclusion

Darknet Background

- A darknet can be a component of an Intrusion Detection System (IDS)
- Monitors unused IP address space
- Key assumption: packets heading for darknet IP addresses - should not be
- We can use this information to infer ongoing and potential network issues

Previous Work

- Emphasis on inferring wider Internet activity
  - “Size” of darknet is important here
    - Internet Motion Sensor (IMS)
    - Network telescope (caida)
    - Cymru darknet project
- Spinning cube of potential doom – worthy of note
  - Unique visualisation of darknet data

Enterprise and Campus Darknets

- Intent is different to a “traditional” darknet
- An “internal” darknet
  - Important for inferring local rather than wide area activity
- Scan activity within the enterprise network is of great concern
  - The source is already inside outer defenses
  - Automate detection and clamp-down the source?

Defining and Characterising a Greynet

- Greynets are collections of non-contiguous blocks of IP addresses
  - “Dark” in the traditional sense
  - Also interspersed among groups of “lit” (used) IP addresses
- Interspersing with valid hosts makes it harder for malware to avoid hitting greynet addresses while searching for infection targets

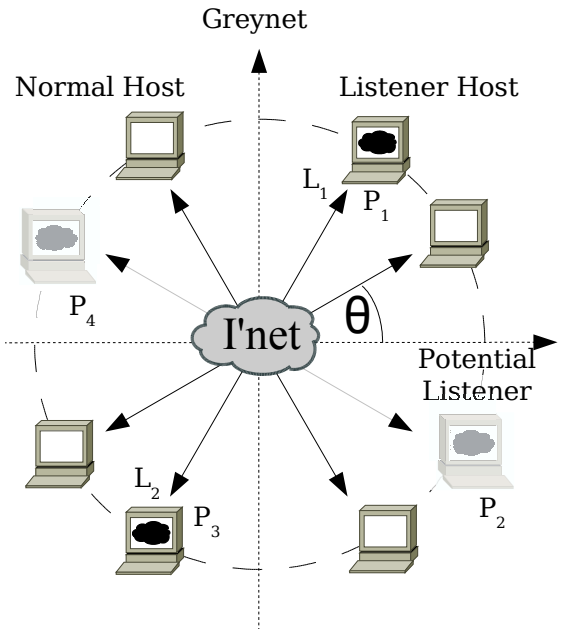
Greynet Terminology

Terms and Definitions

- Greynet
- Potentials
  - Set of 'dark' IP addresses that can be monitored and are unused
- Listeners
  - Set of 'dark' IP addresses being monitored (n)
- Distribution of listeners
  - Pattern of IP address distribution (X)
- Orientation of listeners
  - 'Rotation' of listeners (θ)

Terms and Definitions

- Greynet
- Potentials
  - Set of 'dark' IP addresses that can be monitored and are unused
- Listeners
  - Set of 'dark' IP addresses being monitored (n)
- Distribution of listeners
  - Pattern of IP address distribution (X)
- Orientation of listeners
  - 'Rotation' of listeners (θ)

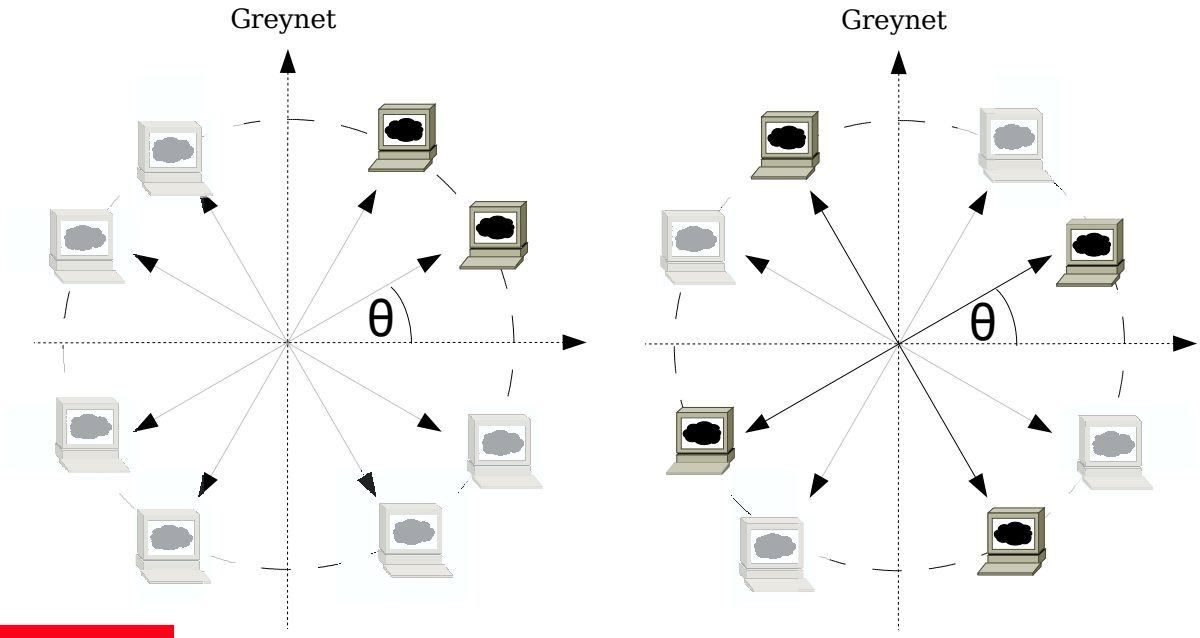


A greynet with an even distribution of potential and listener hosts within it with offset θ

Described by the polar coordinate (L_{nX}, θ)

Types

- A, B

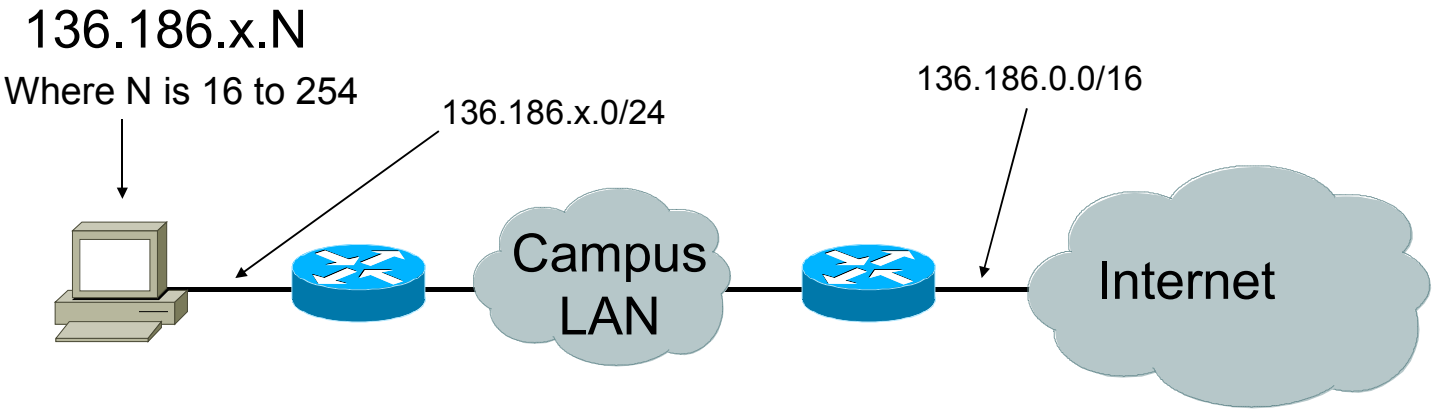


Implementation and Analysis

Establishing the Efficacy of a Greynet

- Two metrics defined for analysis
  - Time to detect (TTD) and median inter-event interval
- Data gathered experimentally from a live darknet
  - 238 contiguous 'dark' IP addresses open to the Internet
  - Simulation run on full data set to simulate various configuration of greynet

Experimental setup



Experimental Results

Summary of packets observed by the full greynet (Trace time ≈ 3.5 months)

Port 445 Malware (96.8%)

Due to firewall

1 RSVP path

	TCP	*UDP*	*ICMP*	*Total*
Internal	993,431	0	717	994,148
External	1,734,286	315,243	121,750	2,171,280
Total	2,727,717	315,243	122,467	3,165,428

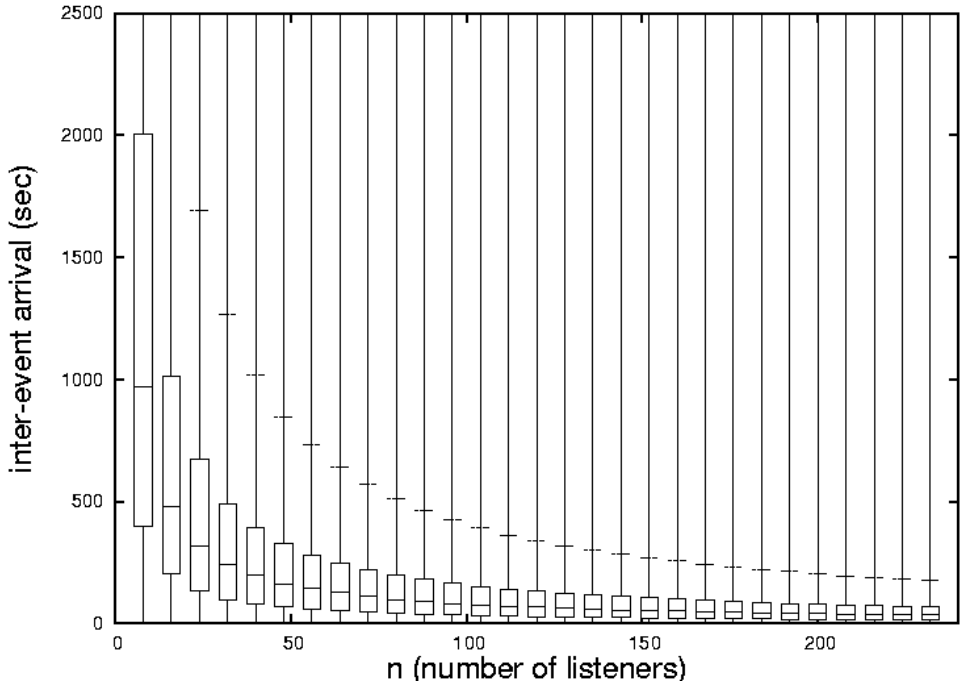
99% "Winpopups"
of these:
62% Fraudulent Windows update
24% Male genitalia enlargement processes
1.3% "non accredited degrees"

```
14:18:00.371475 IP 151.202.88.4.1813 > 136.186.x.117.1026: RADIUS, Accounting Request (4), id: 0x00
length: 512
        0x0000:  4500 021c bfc4 0000 6d11 2c0e 97ca 5804  E.......m.,...X.
        0x0010:  88ba xx75 0715 0402 0208 0175 0400 2800  ...u.......u..(.
        0x0020:  1000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0030:  0000 0000 f891 7b5a 00ff d011 a9b2 00c0  ......{Z........
        0x0040:  4fb6 e6fc 82a6 cfee 3133 3132 3030 3032  O.......13120002
        0x0050:  3230 3130 0000 0000 0100 0000 0000 0000  2010............
        0x0060:  0000 ffff ffff b001 0000 0000 1300 0000  ................
        0x0070:  0000 0000 1300 0000 2020 2020 2054 4845  ............THE
        0x0080:  4249 4747 4553 5420 2020 0000 1300 0000  BIGGEST.........
        0x0090:  0000 0000 1300 0000 2020 2020 2020 2020  ................
        0x00a0:  594f 5520 2020 2020 2020 0000 6401 0000  YOU.........d...
        0x00b0:  0000 0000 6401 0000 0a0a 556e 6976 6572  ....d.....Univer
        0x00c0:  7369 7479 2044 6567 7265 6520 5072 6f67  sity.Degree.Prog
        0x00d0:  7261 6d0a 0a59 4f55 2756 4520 4845 4152  ram..YOU'VE.HEAR
        0x00e0:  4420 4954 2041 4c4c 2042 4546 4f52 450a  D.IT.ALL.BEFORE.
        0x00f0:  4e6f 2044 6567 7265 652c 204e 6f20 4a4f  No.Degree,.No.JO
        0x0100:  4221 0a59 6f75 2064 6f6e 2774 2051 7561  B!.You.don't.Qua
        0x0110:  6c69 6679 3f0a 5768 6174 2773 2079 6f75  lify?.What's.you
        0x0120:  7220 4465 6772 6565 2069 6e3f 0a57 6865  r.Degree.in?.Whe
        0x0130:  7265 2064 6964 2079 6f75 2067 6f20 746f  re.did.you.go.to
        0x0140:  2073 6368 6f6f 6c3f 0a0a 5769 7468 2061  .school?..With.a
        0x0150:  2044 6567 7265 6520 7765 2063 6f75 6c64  .Degree.we.could
        0x0160:  206f 6666 6572 2079 6f75 2061 2068 6967  .offer.you.a.hig
        0x0170:  6865 7220 7361 6c61 7279 3f0a 4e6f 7720  her.salary?.Now.
        0x0180:  796f 7520 6361 6e20 4669 6e61 6c6c 7920  you.can.Finally.
        0x0190:  6861 7665 2074 6865 2044 6567 7265 6520  have.the.Degree.
        0x01a0:  796f 7520 6465 7365 7276 6520 6261 7365  you.deserve.base
        0x01b0:  6420 6f6e 2079 6f75 720a 6c69 6665 2065  d.on.your.life.e
        0x01c0:  7870 6572 6965 6e63 652e 2050 7265 7374  xperience..Prest
        0x01d0:  6967 6f75 7320 6e6f 6e20 6163 6372 6564  igous.non.accred
        0x01e0:  6974 6564 2064 6567 7265 6573 0a4e 6f20  ited.degrees.No.
        0x01f0:  6f6e 6520 6973 2074 7572 6e65 6420 646f  one.is.turned.do
        0x0200:  776e 2e0a 0a43 616c 6c3a 2028 3733 3229  wn...Call:.(732)
        0x0210:  2038 3736 2d30 3339 310a 0a00            .876-0391...
```

```
12:53:57.546054 IP 221.184.223.165.3290 > 136.186.x.134.1027: UDP, length: 760
        0x0000:  4500 0314 fda7 0000 6a11 2292 ddb8 dfa5  E.......j.".....
        0x0010:  88ba xx86 0cda 0403 0300 4186 0400 2800  ..........A...(.
        0x0020:  1000 0000 0000 0000 0000 0000 0000 0000  ................
        0x0030:  0000 0000 f891 7b5a 00ff d011 a9b2 00c0  ......{Z........
        0x0040:  4fb6 e6fc c7d5 6589 3133 3132 3030 3032  O.....e.13120002
        0x0050:  3230 3130 0000 0000 0100 0000 0000 0000  2010............
        0x0060:  0000 ffff ffff a802 0000 0000 1300 0000  ................
        0x0070:  0000 0000 1300 0000 2020 2020 2054 4845  ............THE
        0x0080:  4249 4747 4553 5420 2020 0000 1300 0000  BIGGEST.........
        0x0090:  0000 0000 1300 0000 2020 2020 2020 2020  ................
        0x00a0:  594f 5520 2020 2020 2020 0000 5c02 0000  YOU.........\...
        0x00b0:  0000 0000 5c02 0000 0a0a 4f75 7220 6e61  ....\.....Our.na
        0x00c0:  7475 7261 6c20 4947 4620 7065 6e69 7320  tural.IGF.penis.
        0x00d0:  656e 6c61 7267 656d 656e 7420 7069 6c6c  enlargement.pill
        0x00e0:  7320 7769 6c6c 2065 7870 616e 642c 0a6c  s.will.expand,.l
        0x00f0:  656e 6774 6865 6e20 616e 6420 656e 6c61  engthen.and.enla
        0x0100:  7267 6520 796f 7572 206d 616e 686f 6f64  rge.your.manhood
        0x0110:  2062 7920 332b 2069 6e63 6865 732e 0a31  .by.3+.inches..1
        0x0120:  3030 2520 7361 7469 7366 6163 7469 6f6e  00%.satisfaction
        0x0130:  2067 7561 7261 6e74 6565 6421 204f 5220  .guaranteed!.OR.
        0x0140:  594f 5552 204d 4f4e 4559 2042 4143 4b21  YOUR.MONEY.BACK!
        0x0150:  210a 0a0a 2a20 4761 696e 2033 2b20 696e  !...*.Gain.3+.in
        0x0160:  6368 6573 2069 6e20 6c65 6e67 7468 2e0a  ches.in.length..
        0x0170:  2a20 496e 6372 6561 7365 2079 6f75 7220  *.Increase.your.
        0x0180:  7769 6474 6820 2847 6972 7468 2920 6279  width.(Girth).by
        0x0190:  2032 3025 2e0a 2a20 5374 6f70 2070 7265  .20%..*.
```

[....]

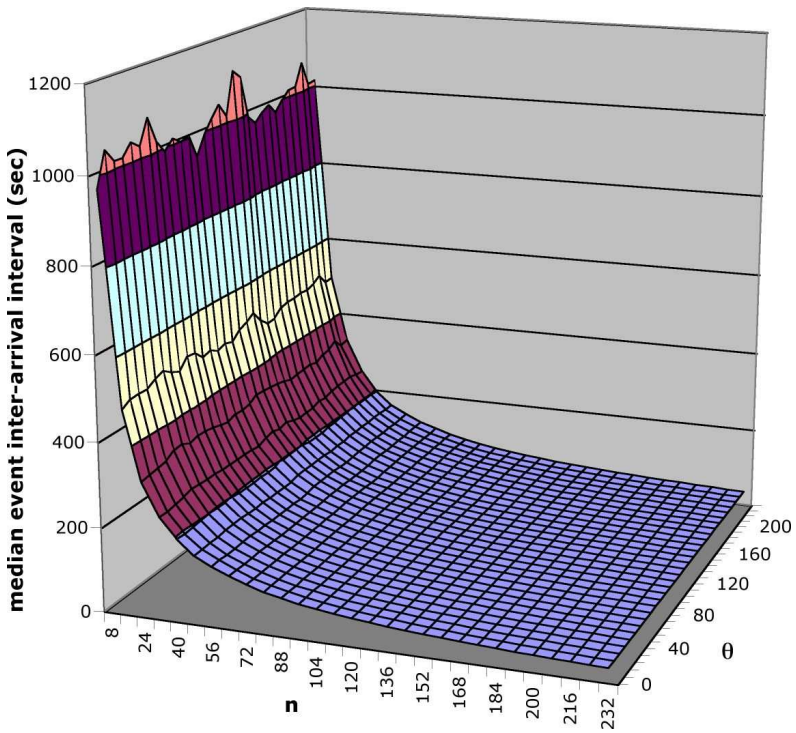
Experimental Results



SWINBURNE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

"Host 174's" TCP scans on port 445 analysed using a series of "type A" greynets increasing in listener numbers (n)

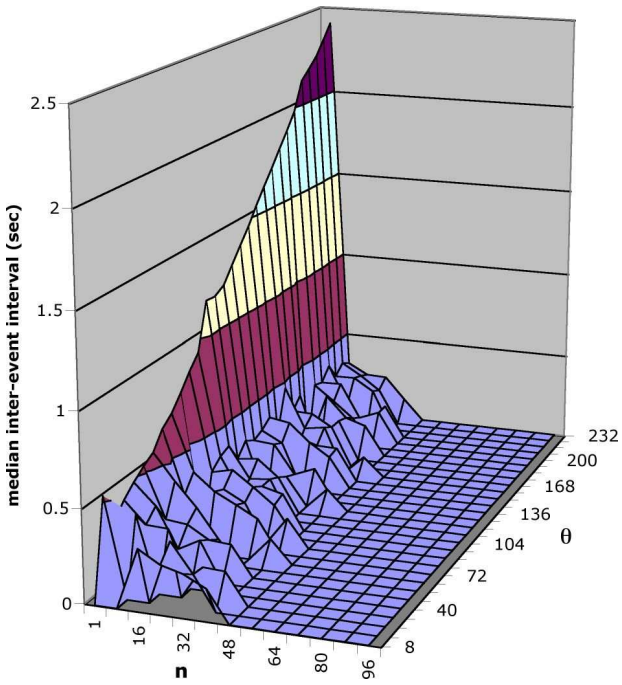
Experimental Results



SWINBURNE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

"Host 174's" TCP scans on port 445 analysed using a series of "type A" greynets increasing in listeners (n) and rotated by θ

Experimental Results



Externally sourced TCP events analysed using a series of "type B" greynets increasing in listeners (n) and rotated by θ

Experimental Results

- To detect sasser infected hosts in < 200 sec
  - 30 greynet hosts
- TCP scans that move linearly across address space
  - With only one listener
  - Less than 2.5 sec to detect

Conclusion

- Greynet – 'dark' IP addresses dispersed among 'lit' IP addresses
- Proposed description of greynets - (L_{nX}, θ)
- Initial experiments - synthesise various greynets from small 238 address darknet over 3 months
- Ideas:
  - Greynet address assignment should be integrated with DHCP
  - A single host on a VLAN trunk switch port could instantiate greynets simultaneously on multiple subnets