SWINBURNE UNIVERSITY OF TECHNOLOGY

Using a lack of source address filtering to create 'quota-free' tunnels between collaborators

Warren Harrop

wharrop@swin.edu.au

Centre for Advanced Internet Architectures (CAIA)
Swinburne University of Technology

Outline

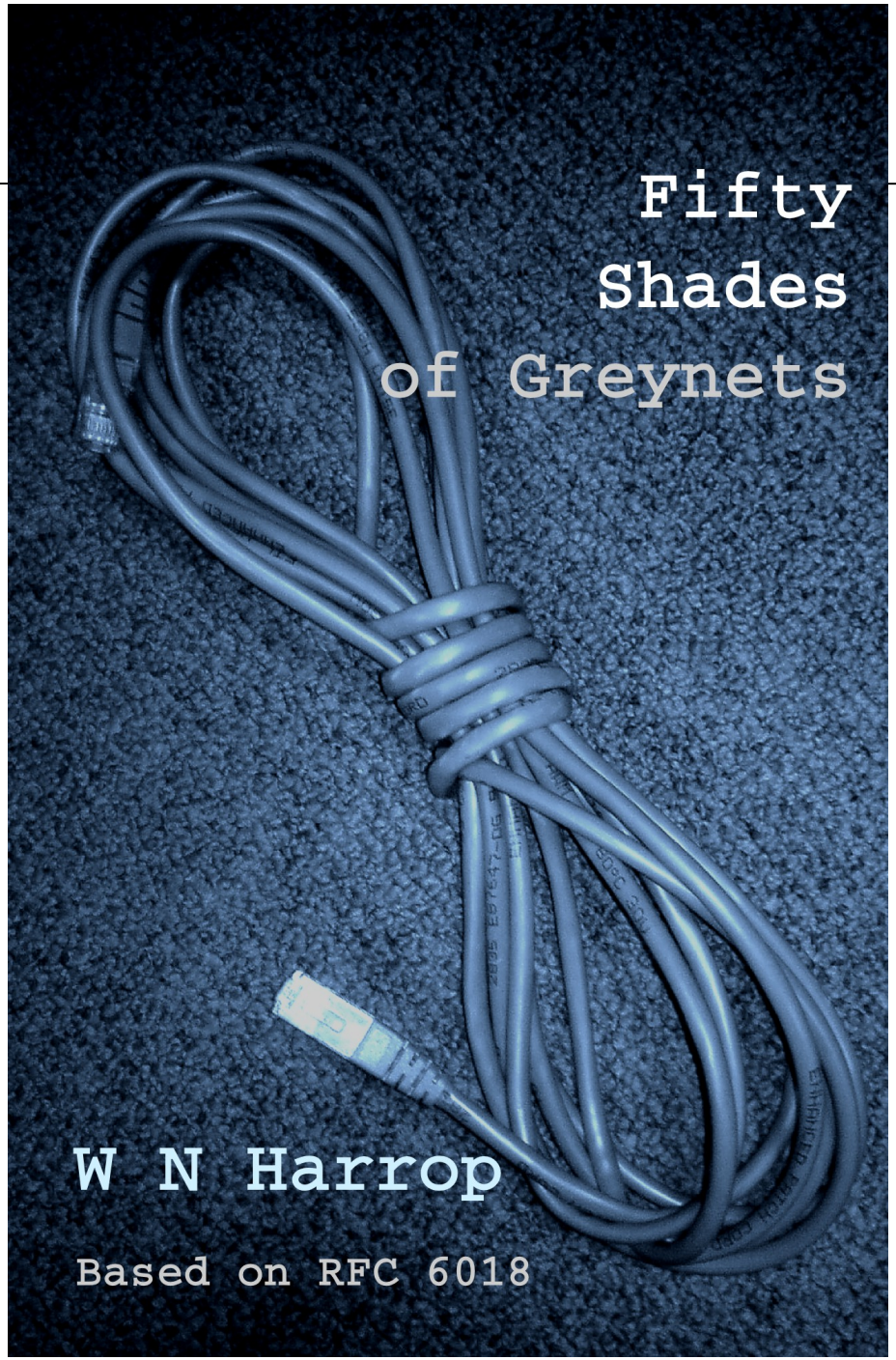
- Brief update: Greynets (AusNOG 2008)
- Details of the issue
  - Variants
- Mitigation
  - An argument for implementing BCP38 (src address filtering)
- Conclusion

Greynets - AusNOG 2008

- Passive listener (darknet) hosts scattered amongst normal (lit) hosts on an edge network
  - When scans occur they inevitably scan a greynet host
- Originally only implemented using VLAN trunks [1]
- Since last AusNOG, further defined in RFC 6018 “IPv4 and IPv6 Greynets” (Baker, Harrop, Armitage)
  - Router assisted greynets
- … & a book

[1] W.Harrop, G.Armitage "Defining and Evaluating Greynets (Sparse Darknets)," *IEEE 30th Conference on Local Computer Networks (LCN 2005) Sydney, Australia, 15-17 November, 2005.*

Book



The issue

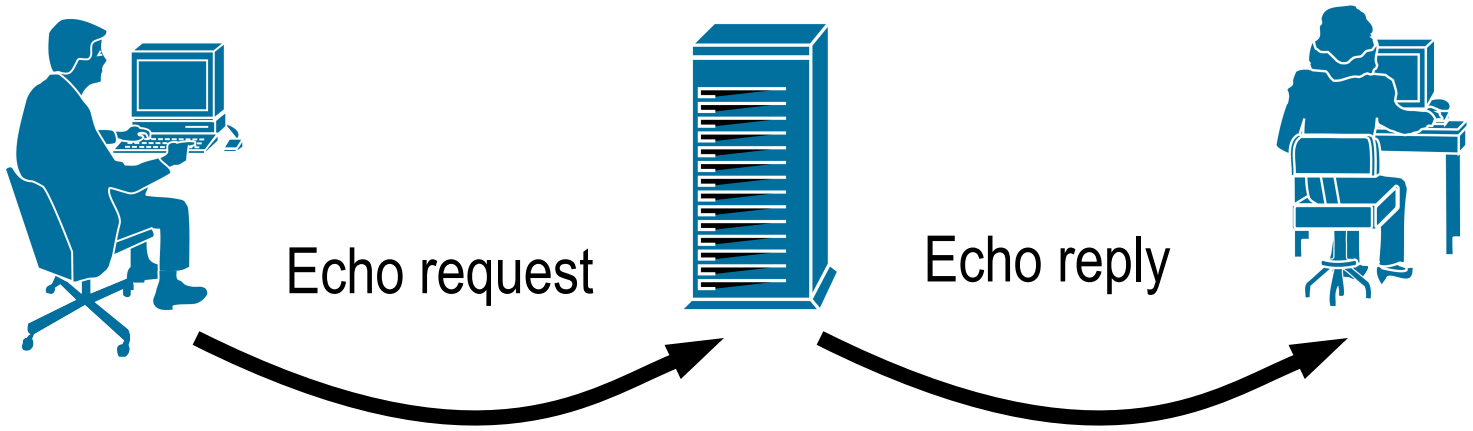
- I hesitate to call it an “exploit”
  - Not an exploit for a specific device & software version
  - More: “an evil idea with some proof of concept experiments”
- History
  - Max Tulyev outlines the issue in a 2004 mailing list post
    http://archive.cert.uni-stuttgart.de/bugtraq/2004/09/msg00267.html

Background

- Three generalisations that hold true for many consumer-grade products offered by ISPs:
  - Usage is metered on a per-byte-transfered basis
  - Consumers generally have '*quota-free*' access to certain services (or IP addresses) as a 'value-add'
  - IP packets with forged source-addresses are allowed to move within and leave the network (ie. there is no BCP 38 on the network).
- We can use the last two to create quota-free tunnels between two collaborators
  - Using ICMP...

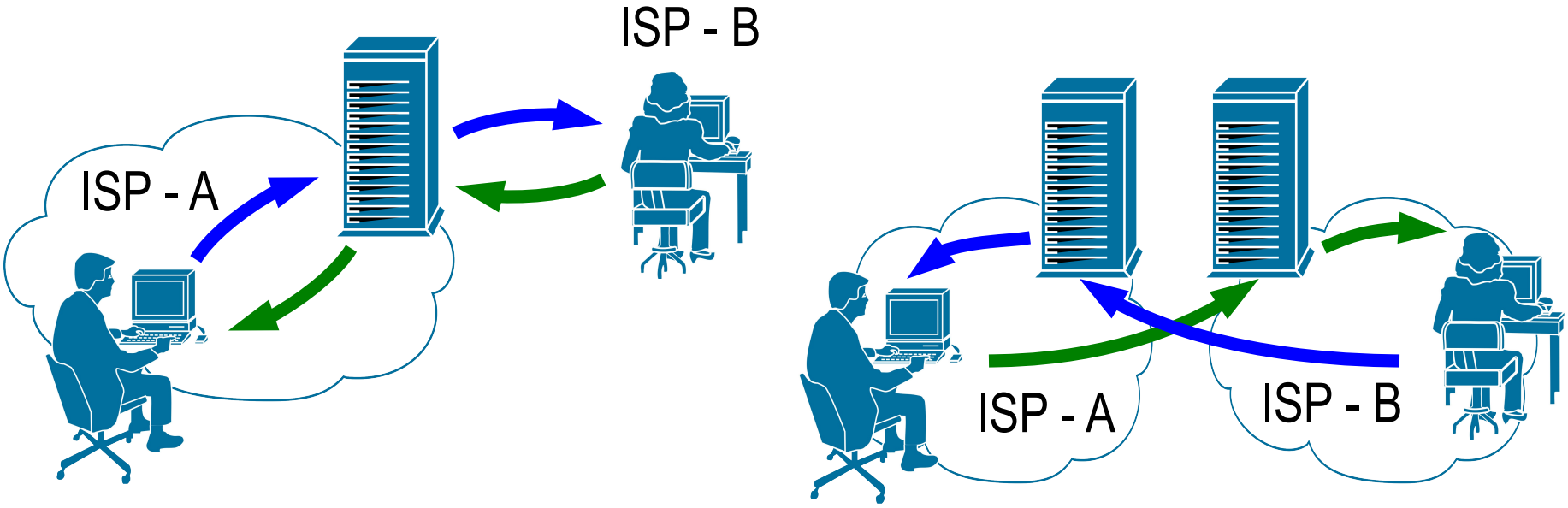
Creating a tunnel (within a single ISP)

- Create an ICMP echo request packet
  - Place an IP packet to be tunnelled in its payload
- Forge the source address to that of your collaborator
- Set destination address to quota-free server
- Same concept for the reverse path



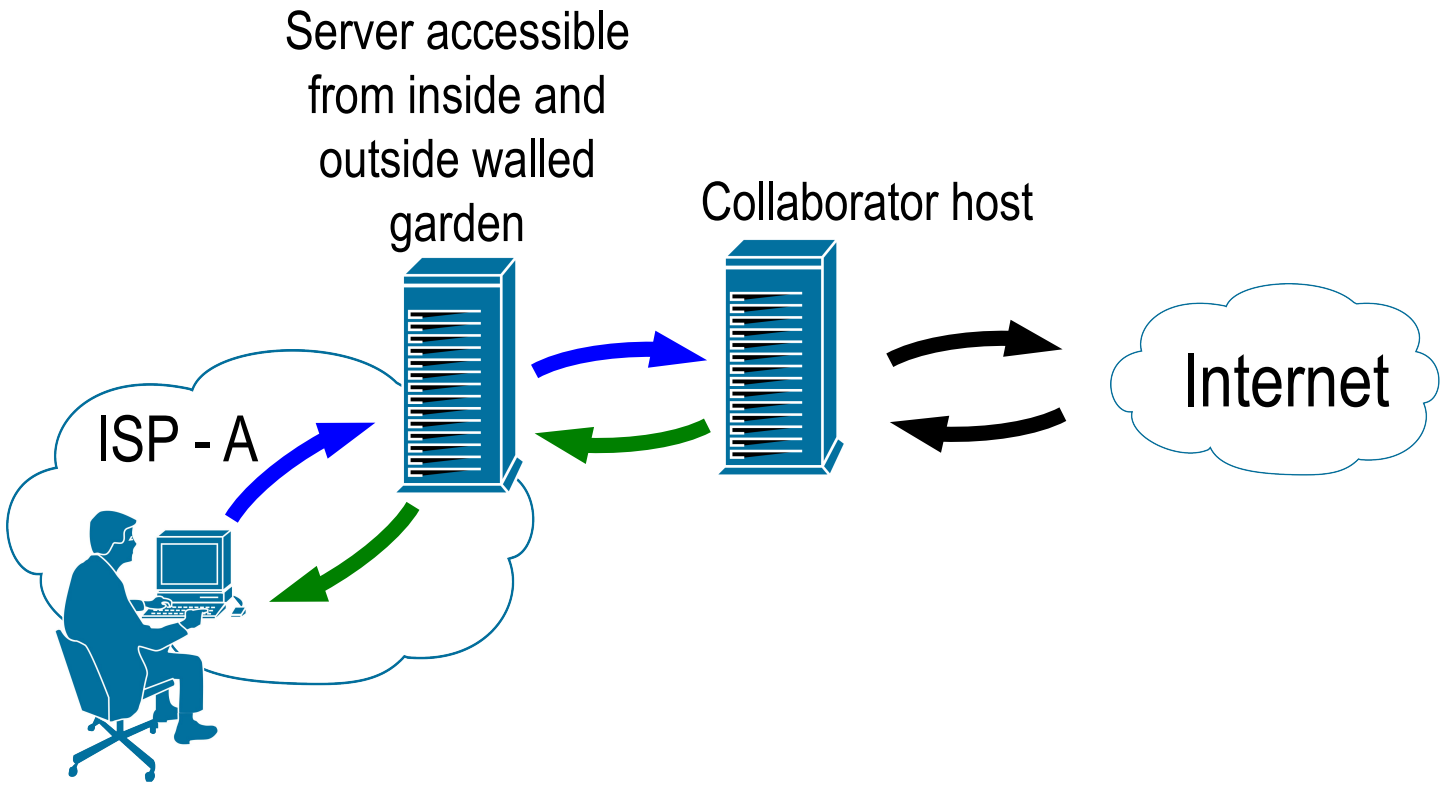
Creating a tunnel (between ISPs)

- One collaborator 'pays', other not [left]
- Each 'pays' for upstream, not for downstream [right]
  - Or vice-versa



Getting out of a walled-garden

- External collaborator host (de)-encapsulates
- Forwards packets to wider internet



Share the load

- Use multiple quota-free servers in a round-robin manner so the ICMP rate of any one server does not spike
- Use the 'right' server and get free QoS

An alternative to using ICMP

- A TCP based tunnel
  - Using covert channel methodologies
- Place data in a TCP:
  - Sequence number (4 byte)
  - Time stamp (4 byte)
- The rate of these packets required to make a usable channel is quite evil though
- There might be others methods...

But...

- NAT breaks all of this
- Collaborators need a globally reachable address
  - And the ability to generate arbitrary packets

Testing

- hping3
  - A nice program to enable the arbitrary generation of packets
  - An example for testing:

```
hping3 ${quota-free_host} -c 1 \
--data 1000 --file ${payload_file} \
-V –icmp \
-a ${collaborator_host}
```

  - tcpdump for ICMP on the collaborator host to see if the packet arrives

Experiments (ICMP based)

- I have confirmed this works with a number of ISPs
- But, with some it did not
- I don't want to publish exact details
- Why?
  - I don't have the resources for exhaustive testing
    - Results would be an arbitrary name and shame
  - I don't want to get in any sort of trouble
    - Unlikely? I've seen enough messengers get shot to play it safe
- No publicly released code for creating a tunnel

Mitigation

- BCP38 – source address filtering
  - Filter early, filter often
  - Helps build a better world
- Reduce the scope of 'quota-free'
  - Specific ports, rather than IPs (won't stop TCP based)
- Looking for unusual patterns of traffic
  - Many ICMP packets
  - Many, many hanging TCP connections
    - Might already trigger DDoS alarms

Is this a big problem?

- Most people run a NAT
- Need to generate arbitrary packets on a public IP
  - But the 'power-users' who can, might be a worry (eg. those who terminate their connection on a UNIX box)
- But! NATs are going away. Right?
  - Could see its day in an IPv6 world?
- Will it matter when plans are > terabyte?
- Carriers using this on each other?
  - Left as a thought for the audience

Conclusion

- A method to create quota-free tunnels
  - Inter- and intra-ISP
  - Escaping a walled-garden
- Mitigation
  - A selfish argument for implementing BCP38
  - Think very carefully about what exactly is made quota-free
- Works, but I'll leave it to others to work out with what networks...