Analyzing Distributed Denial of Service Tools:
The Shaft Case

Sven Dietrich
NASA GSFC/Raytheon ITSS
spock@netsec.gsfc.nasa.gov

Neil Long
Oxford University
neil.long@computing-services.oxford.ac.uk

David Dittrich
University of Washington
dittrich@cac.washington.edu

December 8, 2000

Overview

- Terminology
- Evolution of DoS into DDoS
- DDoS impact overview
- Shaft
- Defensive measures
- Summary
- Future trends

Terminology

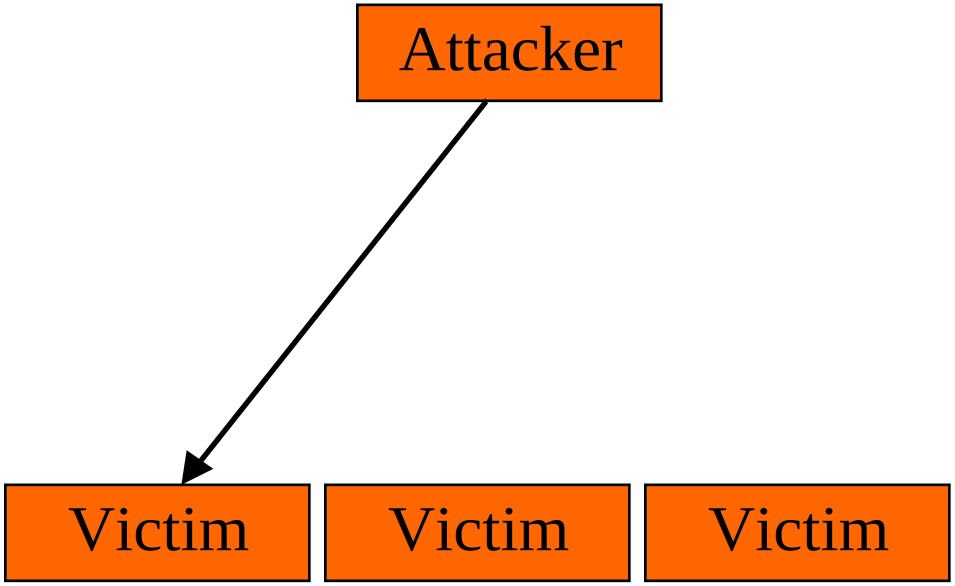
- Denial of Service
  - ➢ Overwhelming the victim to the point of unresponsiveness to the legitimate user
  - ➢ By carefully constructing a sequence of packets with certain characteristics, an intruder can cause vulnerable systems to crash, hang, or behave in unpredictable ways

Evolution of DoS

- Simple DoS
- Smurf DoS
- Coordinated DoS
- Distributed DoS

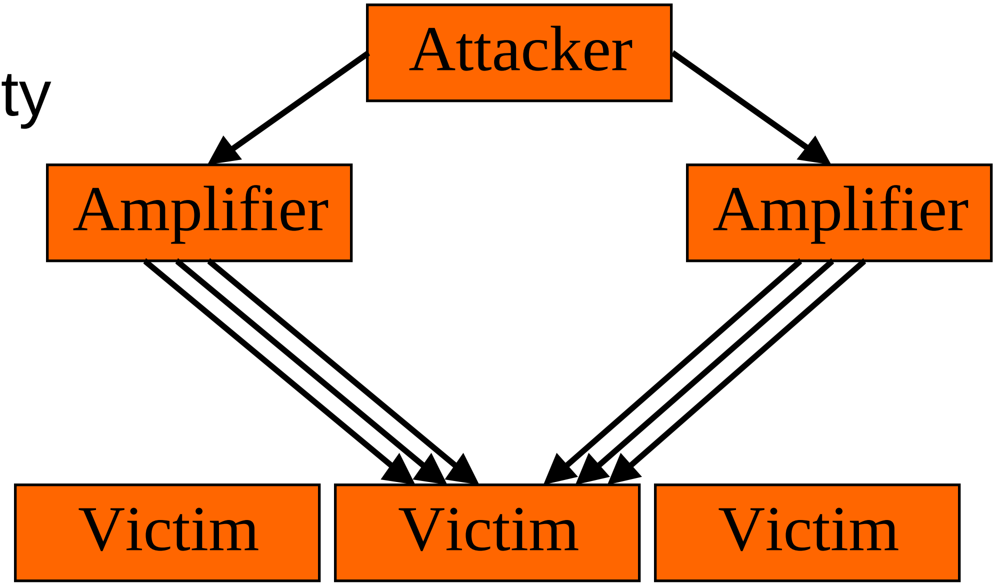
Simple Denial of Service (DoS)

- Point to point, direct phenomenon
- Examples:
  - ➢ TCP SYN flooding
  - ➢ ICMP flooding
  - ➢ UDP flooding
  - ➢ Ping of Death



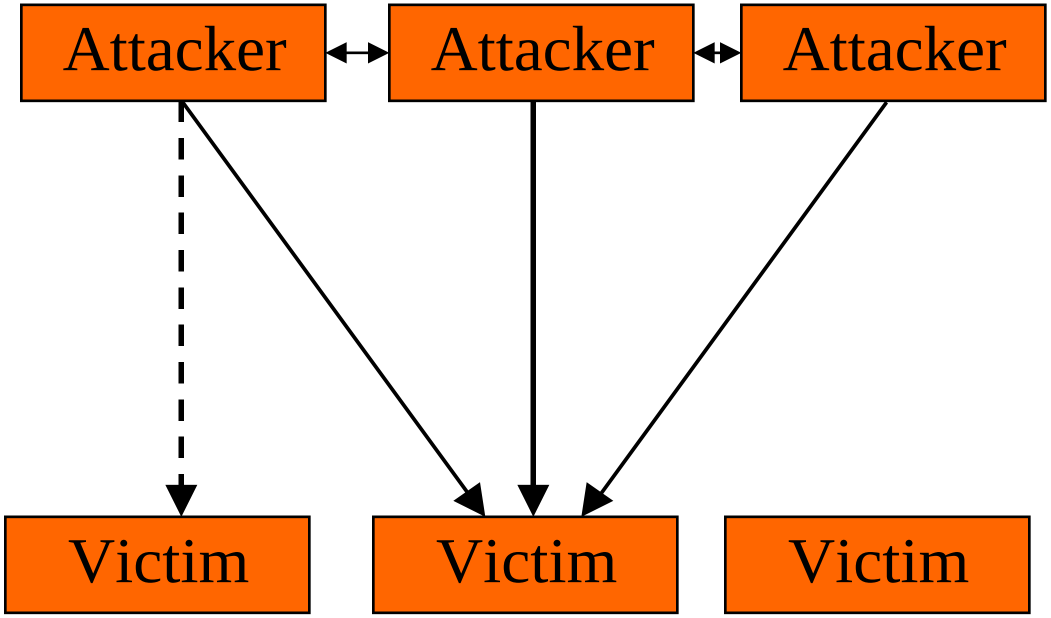
Smurf-type Denial of Service

- Indirect phenomenon
- Requires help from a (misconfigured) third party



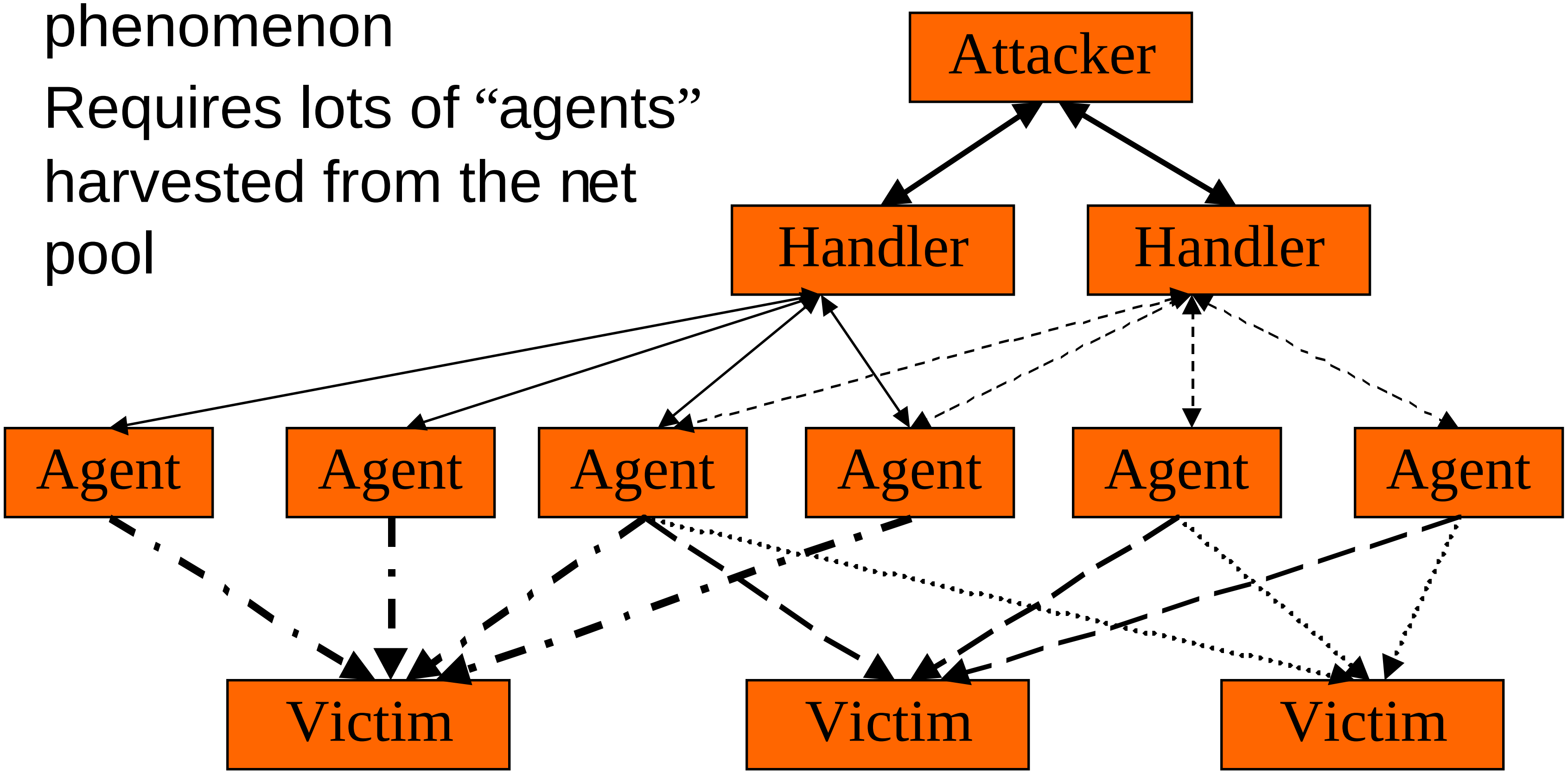
Coordinated Denial of Service

- Collaborative phenomenon
- Requires help from and coordination with multiple parties



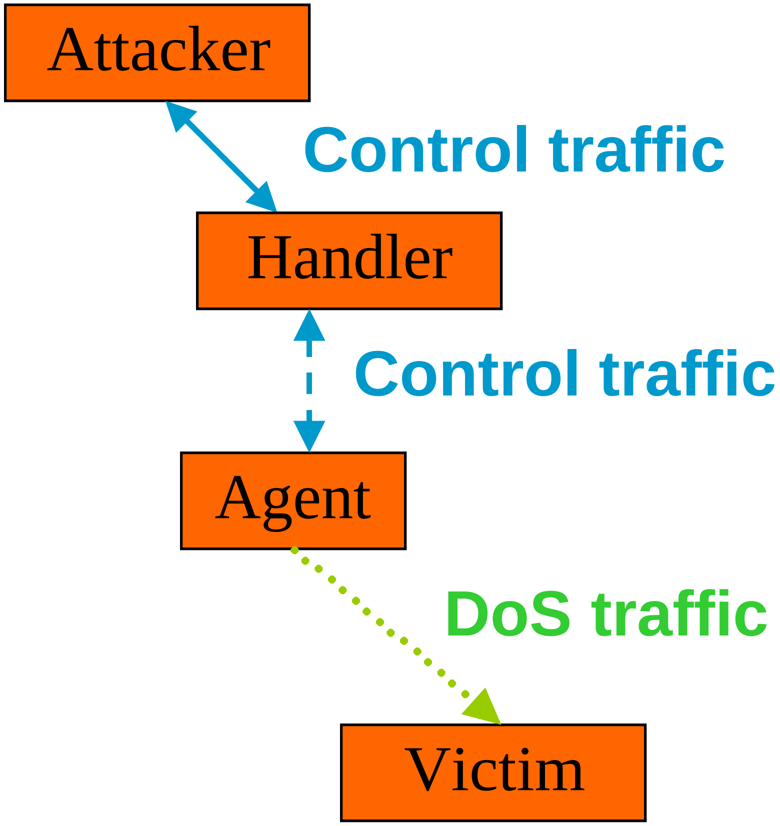
Distributed Denial of Service (DDoS)

- Multi-source, multi-target phenomenon
- Requires lots of "agents" harvested from the net pool



DDoS 101

- One single thread, attacker to victim
- Handler: the program that controls the agents
- Agent: performing the actual DoS attack on behalf of the handler
- Command sets for attacker-handler and handler-agent communications



So what’s the big deal with DDoS?

- Problem recognized at CERT DSIT workshop (November 1999)
- Higher complexity
- Greater distance from victim to attacker
  - ➢ Traceback problem
- Offensive capabilities of a “single attacker” enhanced
  - ➢ Attacks can be sized accordingly (e.g. 25, 250, 2500, 25000 agents), dynamically, if necessary
- Attacks are quite effective (U of MN - August 1999, February 2000 events, etc.)

DDoS impacts

- Packet payloads
- TCP SYN packets
  - ➢ Fill state tables, buffers
- UDP packets
  - ➢ Bandwidth consumption
- ICMP packets
  - ➢ Ping floods, malformed packets, oversized packets
- TCP options, fragments, etc.
- IP Spoofing
  - ➢ None whatsoever
  - ➢ Spoofing at subnet boundaries
  - ➢ Full spoofing

The network level

- Determining whether you are under attack or attacking someone else
    - ➢ Anomaly detection
    - ➢ Performance
    - ➢ Gateways
    - ➢ Uplinks/ISP(s)
- More signs
    - ➢ Network failure
    - ➢ Complaints

The host level

- Host performance impacted
- Agent/handler binaries sometimes hidden
  - ➢ by rootkits, at times for months!!!
  - ➢ Trying to ‘blend’, by naming schemes:
    - /usr/bin/rpc.listen
    - /usr/bin/rpc.bind
    - httpd
    - idle.so
- Need for good forensics
  - ➢ find_ddos [NIPC]
  - ➢ TCT [Venema, Farmer]
  - ➢ lsof

Where does Shaft fit in?

- Trinoo [Dittrich, 1999]
- Tribe Flood Network [Dittrich,1999]
- Stacheldraht [Dittrich, 1999]
- TFN2K [Barlow,Thrower, 2000]
- Shaft [Dietrich, Long, Dittrich, LISA 2000]
- Mstream [Dittrich, Weaver, Dietrich, Long, 2000] [CERT2000]
- Stacheldraht 1.666 [Dittrich, Dietrich, Long, unpublished] [NIPC2000]
- Omega [Dittrich, Weaver, Long, Dietrich, unpublished]
- Trinity, Entitee, Plague, myServer, ...

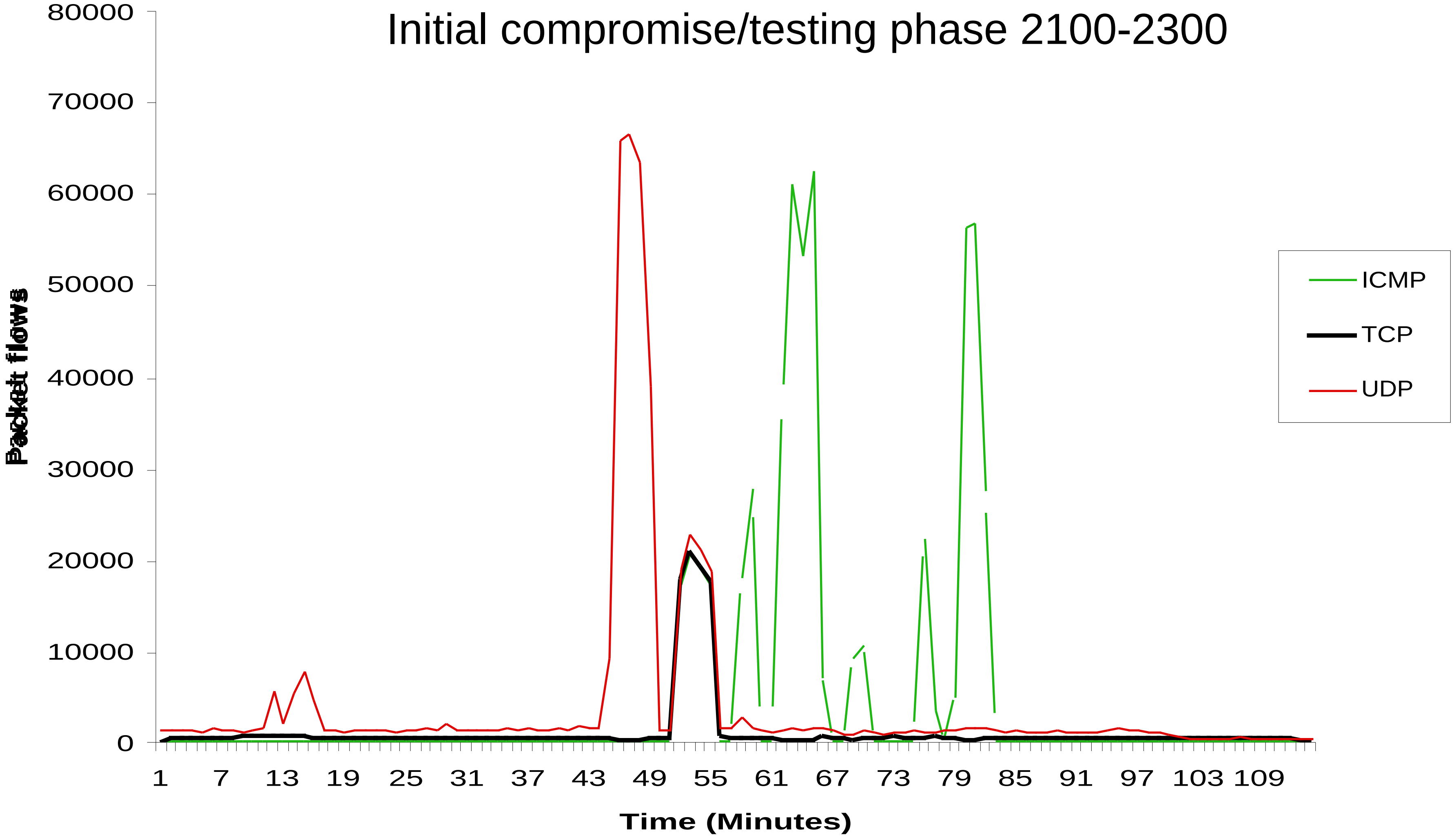
Shaft analysis goals

Know thy enemy

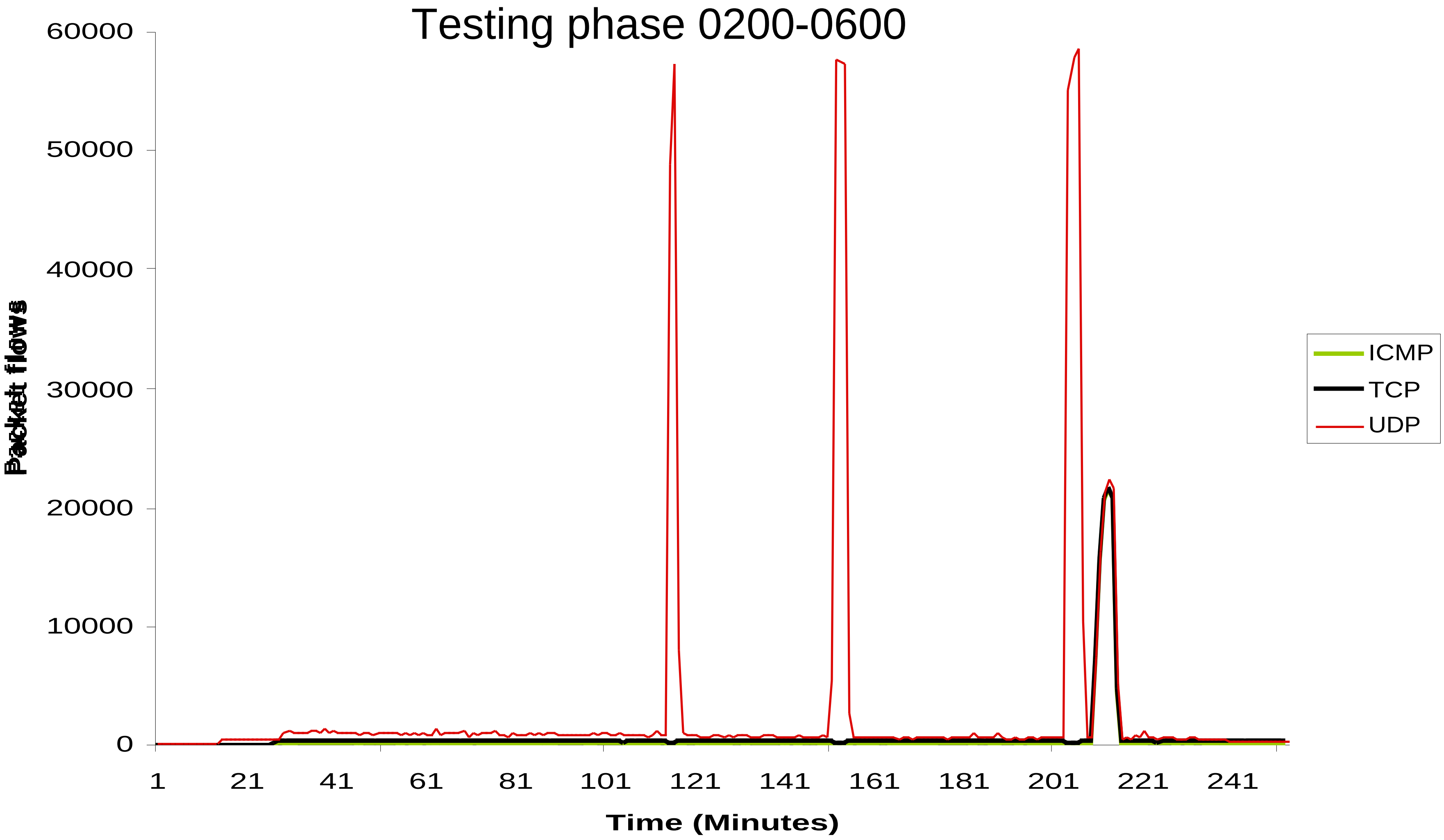
The Shaft incident

- Data shown as seen by an agent network
- Observed data 28 November 1999 - 4 December 1999
  - ➢ Data sampling rather coarse
  - ➢ Various tools: Argus, NeTraMet, tcpdump
- The handler
  - ➢ Taken offline in March 2000 (!)
  - ➢ Online since ???

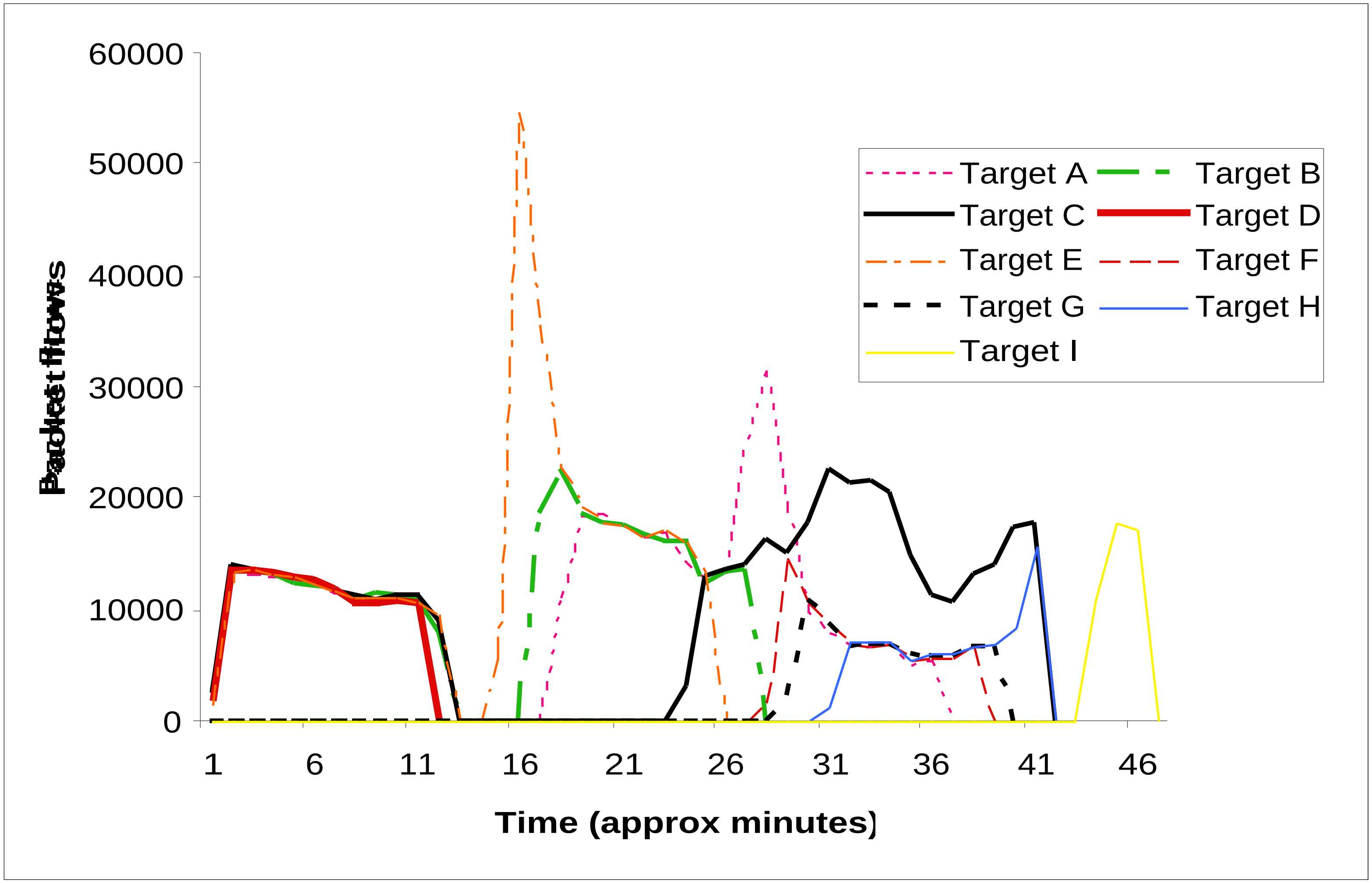
Shaft floods



More Shaft floods



Multi-target Shaft flood



Challenges in the Shaft analysis

- Reconstructing the tool command set
- Passwords for commands encrypted with Caesar cipher
- Access passwords were super-encrypted
  - ➢ String in binary looked like crypt() string, e.g.

    mk-Nw/TTjr4n1

  - ➢ But '-' is not in the 64-character output set of crypt()!
    Shifting the string by 1 character gives

    nl.Ox0UUks5o2

    which is a valid crypt() string

  - ➢ Decrypts to 'lisa2000'

Network defenses

- Network analysis tools overwhelmed or confused
  - ➢ Accuracy of data, dropped packets, better log raw packets
  - ➢ Differentiate flood and control traffic
- Impact reduction
  - ➢ Traffic limiting, redundant pathways, deflection
- Source of IP packets
  - ➢ Need to trace spoofed packets to find agents
  - ➢ Traceback efforts
    - l ICMP Traceback [Bellovin 2000]
    - l Packet marking scheme [Savage et al. 2000]
    - l Advanced packet marking scheme [Song, Perrig, 2000]
    - l Tracing anonymous packets [Cheswick, Burch, 2000]
- Guidelines in CERT DSIT Report

Host defenses

- Protecting the host as a target
  - ➢ Host hardening against network attack [Schuba et al., Oakland 1997]
  - ➢ Kernel tuning
- Protecting the host as a source
  - ➢ Host hardening against compromise
  - ➢ Integrity checking
  - ➢ Removing host offensiveness [Rosti et al, ACSAC 2000]

What can we do?

- Commercial solutions?
  - ➢ Bigger, better IDS?
- Anomaly detection
  - ➢ Free tools work fine, but difficult to maintain
  - ➢ Must know what is ‘normal’
- Check networks for known DDoS tools
- Coordinate efforts
  - ➢ Interdisciplinary
  - ➢ National/international
- Forensics
  - ➢ Recover as much as possible

Summary

- The DDoS problem is not going away
  - ➢ Political/cyberwarfare consequences
  - ➢ No silver bullet
  - ➢ Even crude, buggy DDoS code has tremendous impact
    - l Trinoo
- Education is the key
  - ➢ The earlier this gets recognized/stopped, the better
- Tracking/tracing
  - ➢ Need is obvious
  - ➢ Legal and privacy issues

Future trends

- Sophistication
  - ➢ Hybrid tools
  - ➢ Anonymization
  - ➢ Encryption of communication channels
  - ➢ Use of “non-removable” channels
  - ➢ Hidden channels
  - ➢ Combination/probabilistic attacks
    - l “whack-a-mole” attacks [Longstaff, NISSC 2000]
- Simplification
  - ➢ Disposable, one-time use DDoS tools
  - ➢ Fire and forget

Acknowledgements & Contact info

- Special thanks to:
  - CERT/CC
  - FIRST
  - NASIRC
- Contact info:
  - http://netsec.gsfc.nasa.gov/~spock/
  - http://staff.washington.edu/dittrich/