Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation

Bernhard Plattner, ETH Zürich

Joint work with

Matthias Bossardt and Thomas Dübendorfer

UK ProgNet Workshop, 1st December 2004

The trouble with AN

Landmark technology leading to paradigm shift	Research / basic technology development	Entry into market
PCs	Intel 4004: 1971 Xerox Alto, 1972	IBM 5150 (PC): 1981
2-D Graphical User Interface	Xerox Alto, 1972	Apple Lisa, 1983
Ethernet	Xerox, 1970-73	Approximately 1980-83
TCP/IP	Internet: 1973	First commercial routers (Cisco Systems): 1986
UNIX	Edition 1: 1970	System IV: 1982 Sun Workstation with BSD: 1982
Active Networks	1969? 1982? 1993? 1996? 2004?	Not here yet!

What Went Wrong?

- Capsule model is scary, a security nightmare: Anybody can inject code into the network!
- Maintained equality (AN == Capsules) for too long
- Anything can be done statically, if of broad interest
- No killer application
- Did we eliminate the need for standardization?
- No real business case / business model

➢ Did not convince the industry
➢ Ran out of funding

➢ Challenge of promoting and introducing a disruptive technology was underestimated

Three Ways Out

a) Switch to research in life sciences
b) Reboot and do purely basic research on AN/mobile code
c) Consider non-disruptive approaches

➢ b) and c) can be followed in combination

Outline

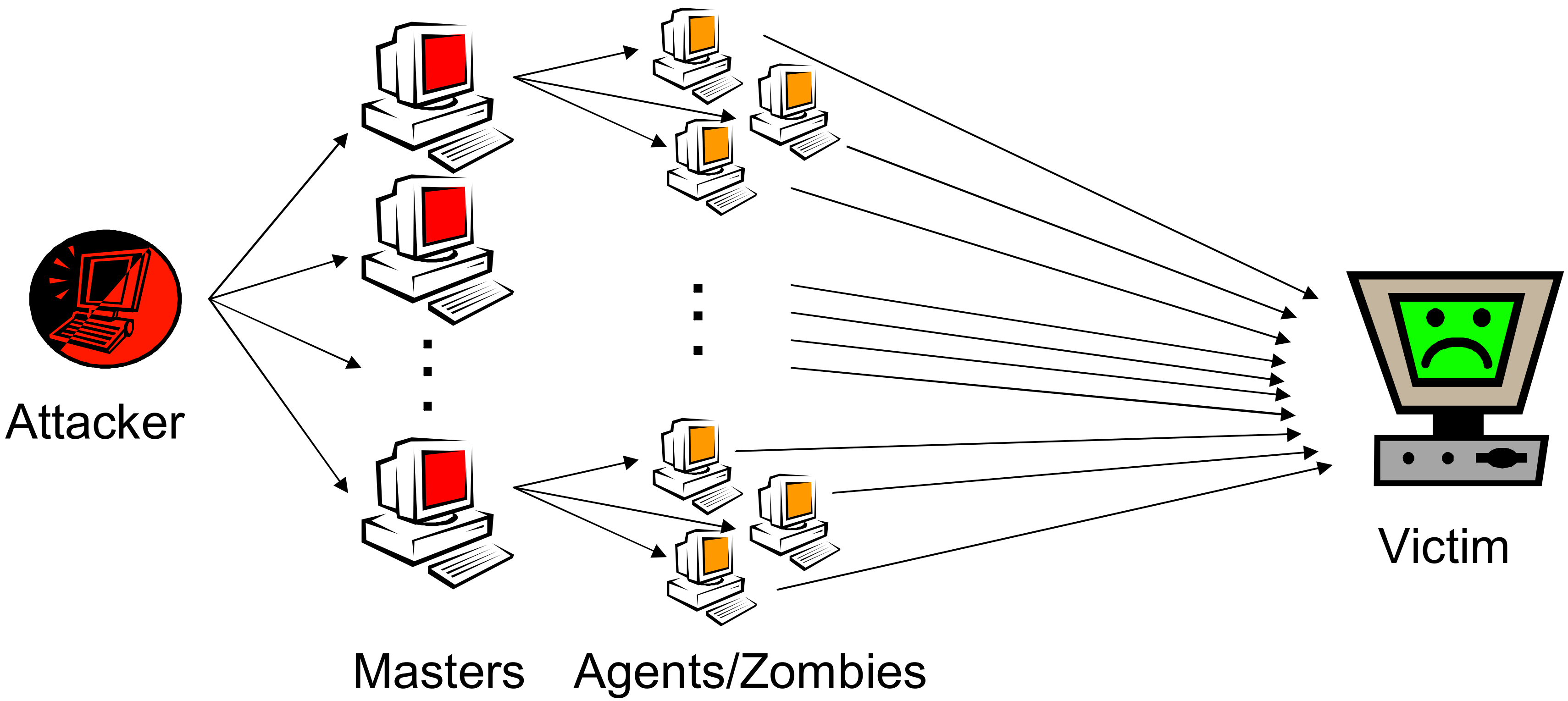
1. Introduction and problem statement
2. Approaches to denial of service mitigation
3. Distributed Traffic Control: Concepts and approach
4. Deployment Infrastructure
5. Conclusions

Introduction and problem statement

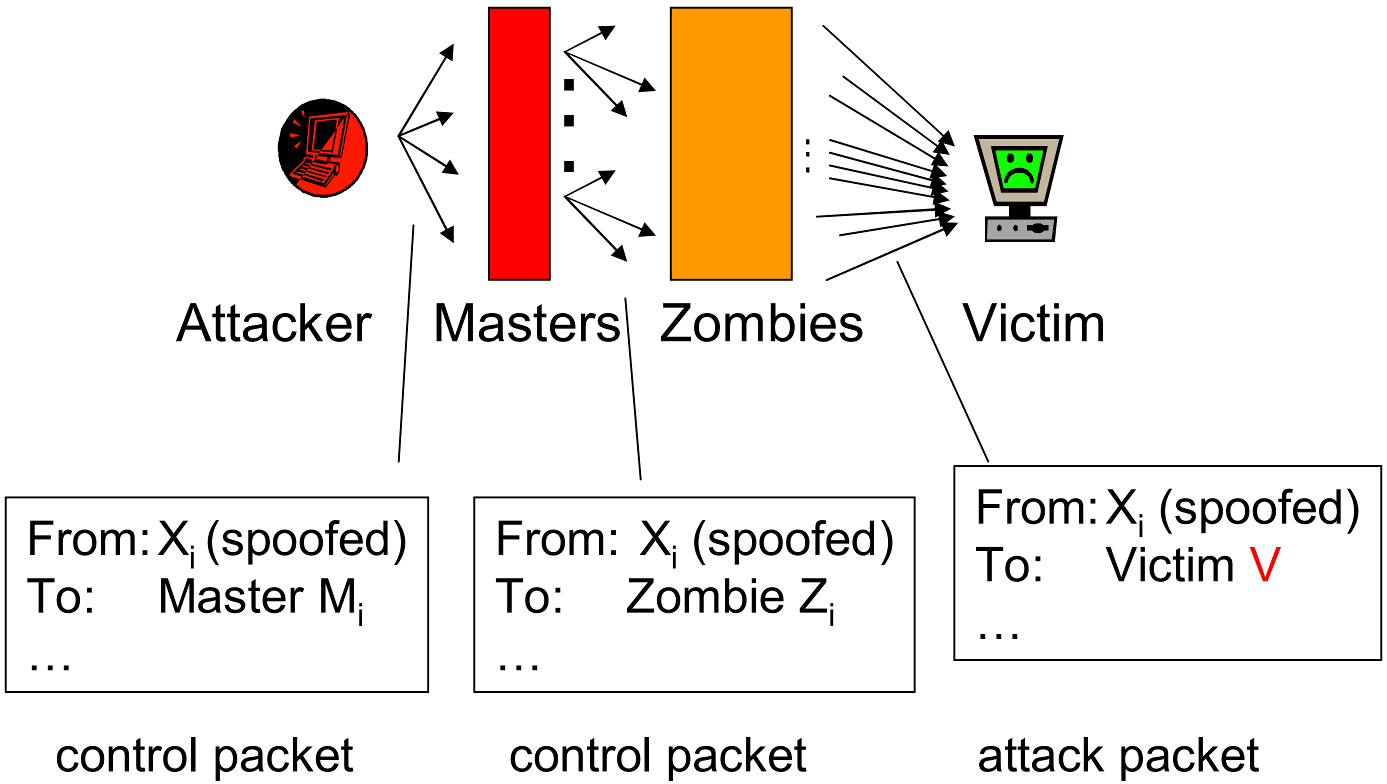
- Frequency of reported security incidents grows exponentially
  - 1988: 6 → 2003: 137‘529 [CERT]
- We will have to live with masses of ill-configured hosts
- Knowledge and tools for attackers abound
- Danger of massive attacks grows with the number of compromised hosts and the ease of mounting attacks
- Distributed denial of service (DDoS) attacks will be more frequent
- Defence focuses on hosts and company networks

➢ Need for security services *within* the network → a case for programmable networks!

Direct DDoS attack



Analysis of direct DDoS attack



From: X_i (spoofed)
To: Master M_i
…

control packet

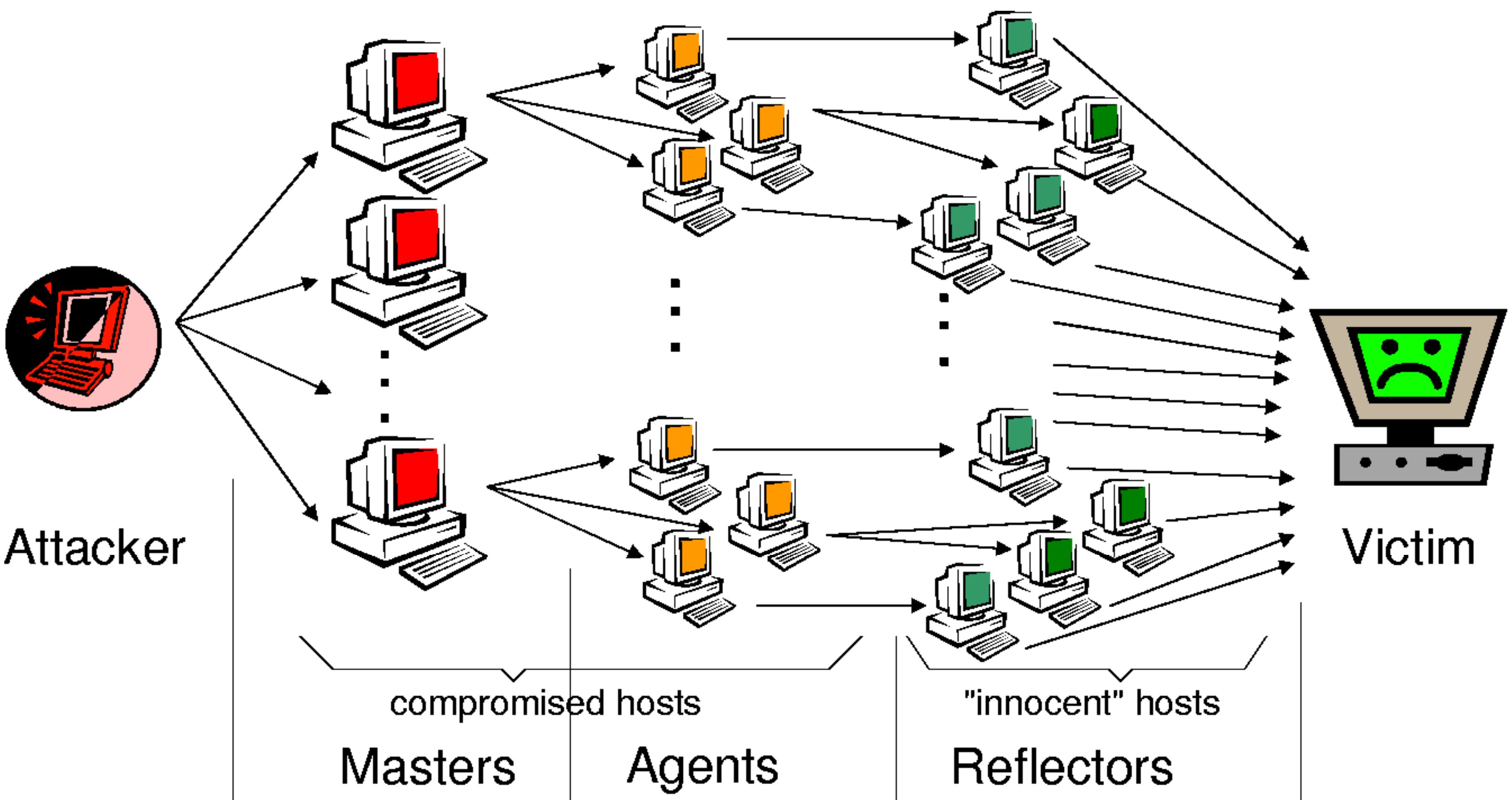
From: X_i (spoofed)
To: Zombie Z_i
…

control packet

From: X_i (spoofed)
To: Victim V
…

attack packet

Reflector DDoS attack



From: X_i (spoofed) To: Master M_i ...	From: X_i (spoofed) To: Zombie Z_i ...	From: **V(spoofed)** To: Reflector R_i ...	From: R_i To: Victim V ...
control packet	control packet	attack packet	legitimately looking attack packet

Role of amplification network

- Increase the rate of attack packets
  - Attacker sends a few control packets, victim gets it all
- Increase attack traffic by increasing packet size
  - If request packet size < reply packet size
- Increase the difficulty of counteraction
  - By making traceback difficult

Note:

- Attack traffic has V as a destination address (direct and reflector DDoS attack)
- Attack packet to reflector has V as the source address (reflector DDoS attack)

Approaches to denial of service mitigation

- Reactive approaches: Detect – identify - react – relax
  - Detection of DDoS attack
    - Sysadmin‘s experience
    - Traffic statistics (e.g. entropy of addresses, ports found in packets)
  - Identification
    - Source addresses are often spoofed
    - traceback to identify attack source
  - Reaction
    - Filter incoming attack traffic
    - Pushback (recursively follow congestion and rate-limit traffic)
    - Mount counter-attack
- Proactive approaches
  - Ingress filtering
  - Secure overlay networks, VPNs

Assessment of The State of The Art

Current mitigation schemes not effective enough:

- Detection is often difficult, due to differentiation between good and bad traffic
- Identification
  - Traceback may be useless, since it identifies zombies or reflectors
- Reaction
  - Filtering: what, where, and who?
  - Pushback may hit legitimate sources and needs ubiquitous deployment
  - Counter-attacks may hit the wrong targets
- Ingress filtering: quite simple, but not done (incentive?)
- Secure overlay networks, VPNs:
  - Scalability problems due to number of trust relations needed
  - Not adequate for generally accessible information services (Google, Yahoo, …)

Distributed Traffic Control: Concepts and Approach

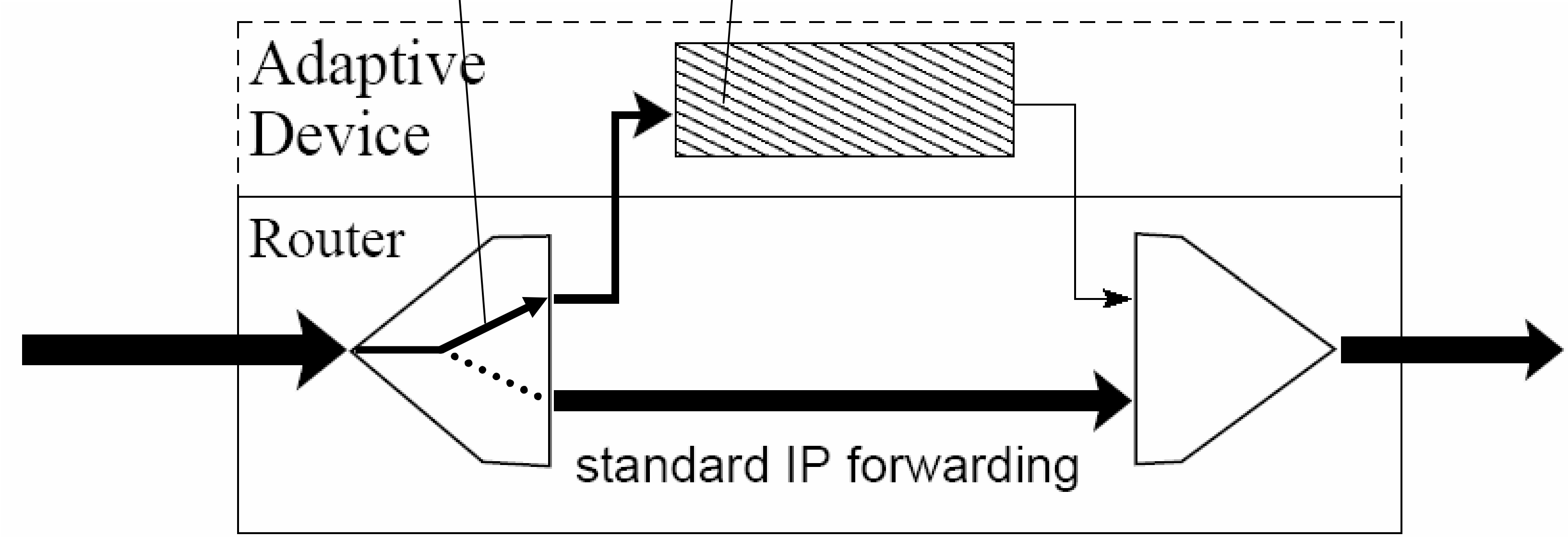
- What would you want to do as an operator of a service under attack?
  - 1a Direct DDoS attack: block packet coming towards you from certain ASes
  - 1b Reflector DDoS attack: block trigger packets flowing towards reflectors → „customer-specific“ ingress filtering
  - 2 Ask trustworthy ISPs/BSPs to install „suitable“ filters
- Suitable filters
  - – Act on packets that have your address as the source, destination or both
- Definition of traffic ownership
  - – Packet is „owned“ by network user who is officially registered to hold either the source or destination address or both

➢ You request ISPs/BSPs to take specific action on your (and only your!) packets

Traffic Control Device

This path only taken by user‘s own packets

User-programmable action
Virtualized per network user



Actions

- Restricted to prevent misuse
  - Acts only on packets owned by network user
  - No modification of source or destination addresses
  - No change of time to live (TTL)
  - No increase of packet rate and/or size
- Properties of user-defined functionality checked at installation or run time
- Context information available to user code
  - Allow for context-specific actions
Where am I? What type of traffic am I acting on?
  - Router state and configuration

➢ Prevention of collateral damage

➢ ISPs/BSPs don‘t lose control over their network

Actions for DDoS attack mitigation

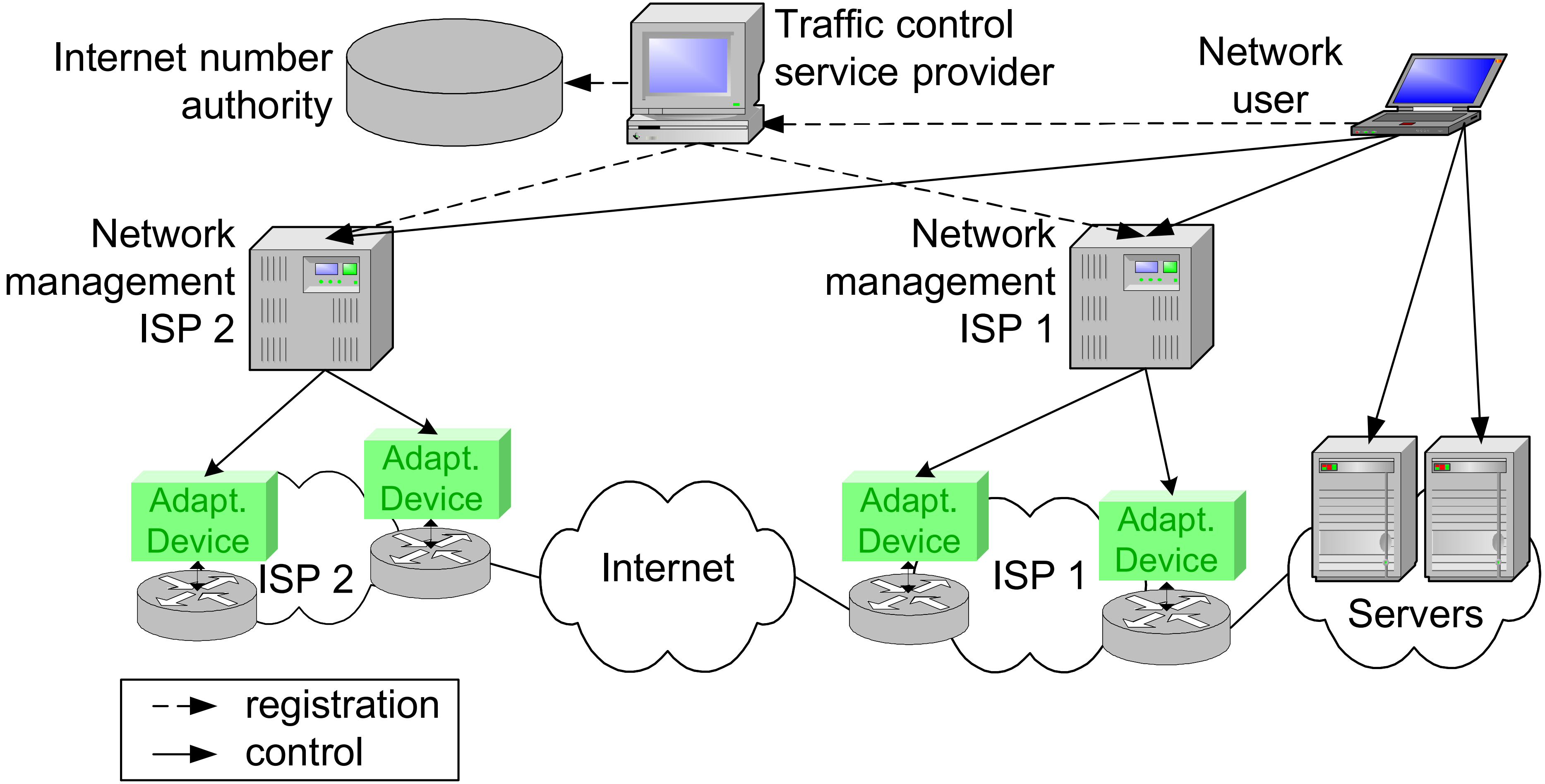
- Actions triggered by matching source/dest address, ports, payload, payload hashes
- Packet dropping
- Payload deletion
- Source blacklisting
- Traffic rate control

- ➢ User-specific ingress control
- ➢ Reactive or proactive
- ➢ Filtering close to source of attack traffic

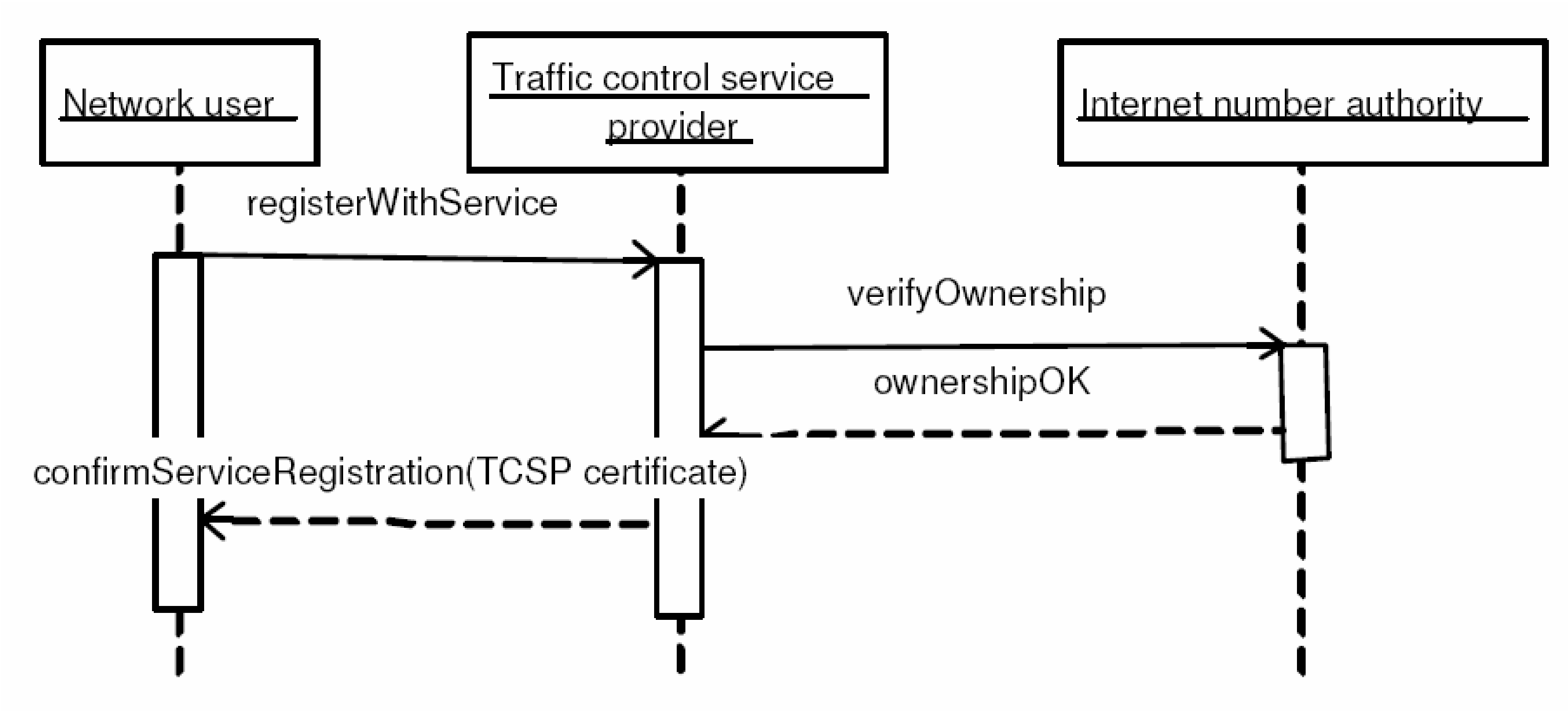
Other applications

- Traceback
  - Proactively collect packet hashes
  - Supporting network forensics
  - Locate origin of spoofed network traffic
- Automated reaction to traffic anomalies
  - Suspicious increase in connection attempts from/to server or network
  - Entropy variations in addresses and or ports
  - Detection of spoofing attempts
- Network debugging and optimization
  - Measure link delays, packet loss
  - Optimize content distribution network

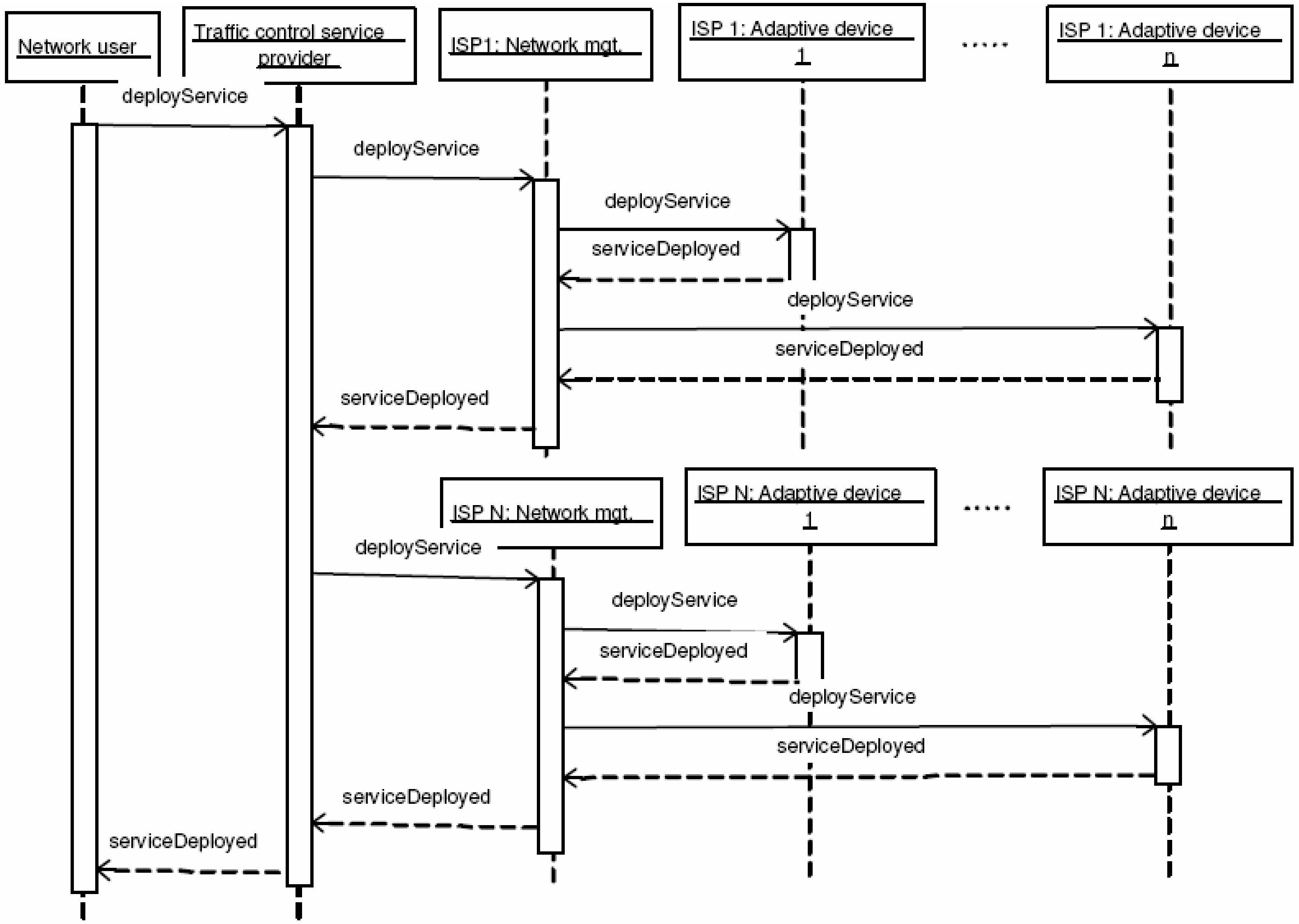
Deployment Infrastructure: Network Model



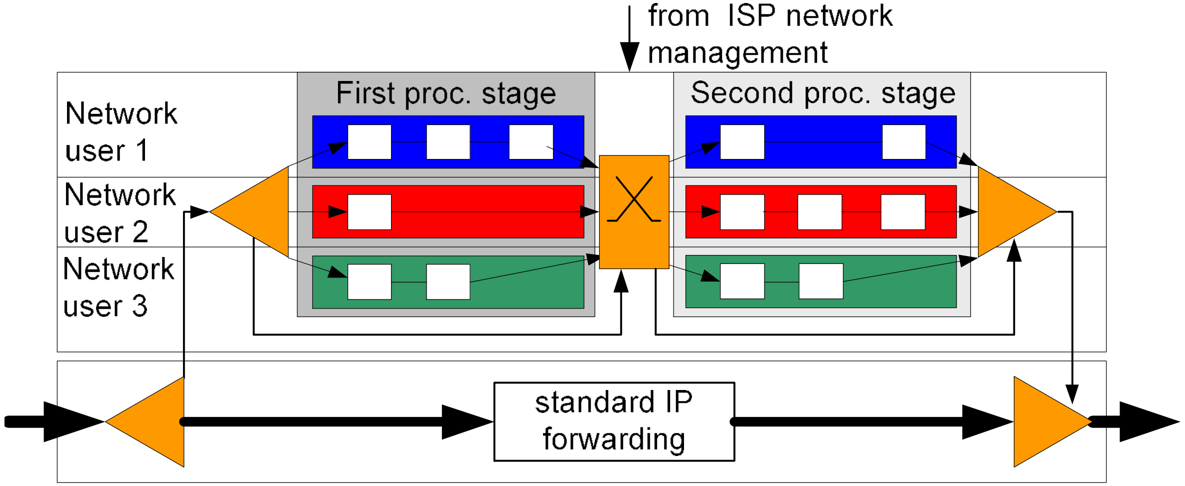
Service Registration


Network user
Traffic control service provider
Internet number authority
registerWithService
verifyOwnership
ownershipOK
confirmServiceRegistration(TCSP certificate)

Service Deployment



Node Architecture



- Premium service; few packets are rerouted through adaptive device
- Authenticated IP address owners can reprogram adaptive devices
- Filter order:
  1. Actions on behalf or owner of source IP address
  2. Actions on behalf or owner of destination IP address

Current status and future work

- International patent application filed (PCT/CH2004/000631)
- Proof of concept implementation underway
  - PromethOS environment
  - To be ported to Network Processor (Intel IXP line)
- Commercialisation
  - Box and service business
  - Start-up company
  - Patent licencing
  - Co-operation with interested company: Trade patent against research money.

➢ Example of „modest“ active networking. More to follow?

Conclusions

- Any chance of success?
  - Control remains with the network service providers
  - Incrementally deployable
    - Add-on box
    - Function may be integrated in future routers
    - Not necessary to have complete coverage on all routers
  - Premium (paid) service for large customers (not home users!)
  - Business incentive for network service providers
- Did we address the issues?
  - Approach not scary for ISPs: Safe, scalable, controllable
  - Ever changing shape of DDoS threat needs adaptive solution
  - Standardization may happen through market forces
  - We have a business model and business proposition
  - Technology is *not* disruptive

Thank you!

Questions?