Network Forensics: Towards a classification of traceback mechanisms

Sarandis Mitropoulos, Dimitrios Patsos, Christos Douligeris
Department of Informatics / University of Piraeus,
80, Karaoli and Dimitriou Street, Piraeus, GREECE
sarandis@unipi.gr, dpat@space.gr, cdoulig@unipi.gr

AGENDA

- Introduction
- The Problem Space
- Tracing a Network Connection
  - IP marking
  - ICMP traceback
  - Overlay networks
  - Host-based Identification
  - Application Level
- Categorization of traceback methods
- Future Work
- Summary

Introduction ..

- Objectives:
  - To formally define the traceback problem
  - To present the most accredited traceback techniques
  - To present the effectiveness and limitations of these techniques
  - To categorize the examined approaches according to certain factors
  - To propose a baseline method for evaluating traceback mechanisms in the near future

Introduction (2)

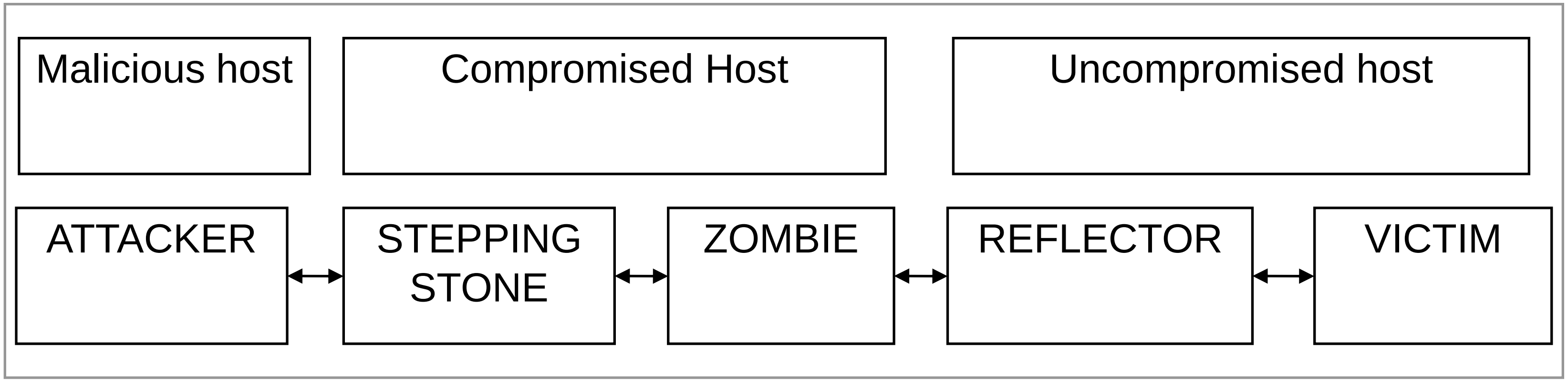
- What is traceback?
  - We define as C = $h_1+h_2+..+h_i+h_{i+1}+..+h_n$ the connection chain between hosts h_i (i=1,..,n)
  - The traceback problem is given the identity of host h_n (i.e. IP address) to recursively identify the identities of h_{n-1}, h_{n-2},…,h_1 in an automated way
  - Usually, host h_1 is the attacker host

The problem space

- Why traceback is not straightforward?
- An attacker uses multiple techniques to hide his real identity, so traceback is non-trivial. For example:
  - Link Layer Spoofing
  - IP source address spoofing
  - Port forwarding
  - Application spoofing
  - "Stepping stones", in modern DDoS attacks
- We examine "stepping stones" and other limitations in the following

The problem space (2)

- Stepping stones are intermediate hosts between an attacker an a “zombie” machine, typically used in DDoS attacks



Malicious host

Compromised Host

Uncompromised host

ATTACKER

STEPPING STONE

ZOMBIE

REFLECTOR

VICTIM

- They act as conduits and change the essence of the entire attack (e.g. encrypted communication)

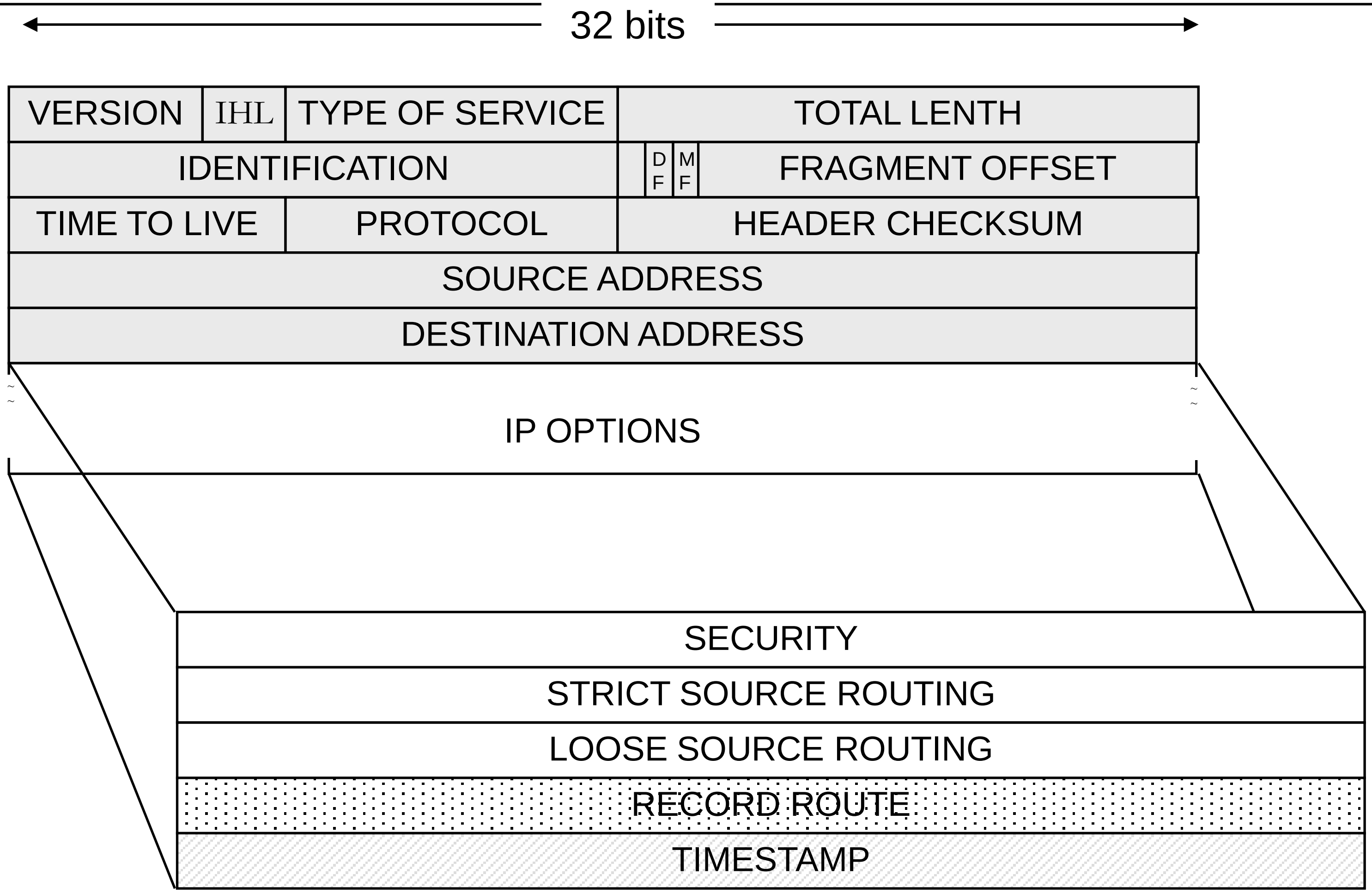
The problem space (3)

- Traceback can be also limited by security devices. Typical ICMP echo-requests or *traceroute* commands are filtered by routers and/or firewalls
- It is not easy to trace the author or a malicious piece of software (e.g. a worm)
- Network data (i.e. routing tables, communication logs) are volatile and ephemeral

Tracing a network connection

- IP provides the IP options field in the protocol header for tracing a network connection: *Record Route & Timestamp*
- Mostly used by network engineers to troubleshoot routing issues
- Limited support for today’s heavy routing information

Tracing a network connection (2)



32 bits

VERSION | IHL | TYPE OF SERVICE | TOTAL LENTH

IDENTIFICATION | DF | MF | FRAGMENT OFFSET

TIME TO LIVE | PROTOCOL | HEADER CHECKSUM

SOURCE ADDRESS

DESTINATION ADDRESS

IP OPTIONS

SECURITY

STRICT SOURCE ROUTING

LOOSE SOURCE ROUTING

RECORD ROUTE

TIMESTAMP

Tracing a network connection (3)

- Reverse engineering the IP Options field:
  - IP datagram header has a 20-byte fixed size and a variable size
  - Maximum IP datagram header size mandated by the value of 4-bit IHL (IP Header Length), which is max 1111 (in binary). This results to 4*15=60 bytes
  - Only 40 bytes left for the IP Options field, i.e. the number of 10 IP addresses
- *Record Route* is not effective

Tracing a network connection (4)

- A tremendous amount of processing overhead in routing devices, since at least 32-bit information (at least for one hop) has to be appended to data in flight in every routing device
- A packet may be routed through different time-zones, so there is a need of a globally synchronized clock for the time-stamps consistency
- A wily attacker can use another option in the IP header options field (e.g. the *Loose Source Routing* that mandatory defines a list of routers that should not be missed during routing), "invent" additional hops in the path and fill the 40 bytes available for IP options with false or misleading information.

IP Marking Techniques

- **Features:**
  - Also known as *“packet marking”*
  - Marking lies to appending data with partial path information so that trace-back can be completed
  - IP Marking approaches use quite complicated mathematical algorithms to identify the origins of sequential IP packets, especially when the source IP addresses are false (i.e. spoofed)
  - So far, IP marking techniques have proved robustness, high probability rates in packet marking and scalable deployment.
- **Examples:** Savage et. al (2000), Song & Perrig (2001), Park & Lee (2000)

IP Marking Techniques (2)

- **Limitations**
  - All network traffic has to be in clear while in transit. An obvious issue arising is the compatibility with IPSec.
  - The nature of IP marking aims to reconstruct the edge of the routing path between the attacker and the victim (i.e. the routing devices that were used) and **not** in finding the attacker himself

ICMP-based traceback

- The approach is based upon the capability of routing devices to generate a “trace” packet for every packet they forward and is marked for tracing
- At the destination host, the original packet and the “trace” packet are collected and the route is reconstructed
- Use of HMAC and X.509 for authenticating and evaluating the “trace” messages
- **Examples:** Current IETF Standard - *iTrace* (Bellovin, 2003)

ICMP-based traceback (2)

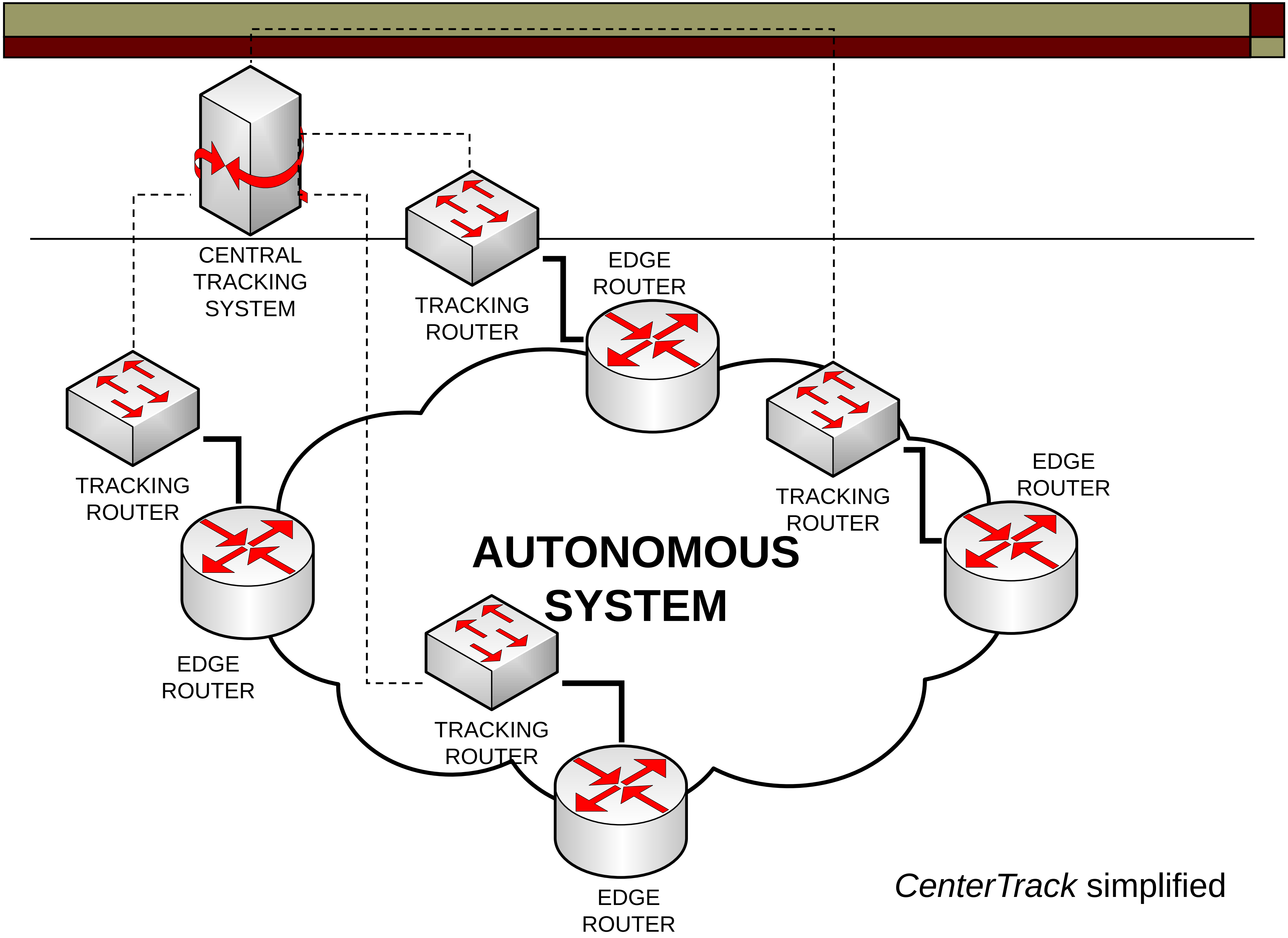
- The number of *iTrace* packets generated by a router is small, which implies a low overhead (statistically, around 0.005%)
- It mainly addresses attacks where a significant amount of traffic comes from a rather small number of sources, due to the lower probability of generating *iTrace* packets
- **Enhancement:** *Intention-Driven iTrace* (Mankin et.al. 2001)

Overlay Networks

- The approach is based onto an overlay network by introducing the concept of special types of routers, called tracking routers
- Tracking routers have a conceptual (physical or virtual) adjacency with edge routers in an autonomous system
- The core of this model is a central tracking system
- **Example:** *CenterTrack* (Stone, 2000)

Overlay Networks (2)

- All edge routers are linked to a central tracking router (or a simple network of tracking routers) via IP tunnels and therefore an overlay network is created
- A necessity for the model to perform is that all edge and tracking routers must perform input debugging functions
- The model supports the use of network sniffers for traffic analysis and attack pattern recognition



CenterTrack simplified

Overlay Networks (3)

- The malicious traffic is routed through the overlay network via dynamic routing protocols
- Static routes must be configured in a way for attack traffic flows only through the overlay network, allowing at the same time the reception of legitimate traffic.
- An alternate mechanism (Baba & Matsuda, 2002) uses the concept of a overlay networks along with an innovative logging approach
- The overlay network is built from sensors that detect attack traffic along with tracing agents (tracers) that log the attack packets and managing agents that coordinate the communication between the sensors and tracers

Overlay Networks (4)

- **Drawbacks**
  - It requires application-level intelligence from the (edge and tracking) routers in order to perform pattern recognition
  - It requires more CPU processing power to succeed in this
  - A wily attacker can detect the presence of tracking systems by statistically measuring the latency via fragmented packets sent to the victim during the information gathering phase of an attack
  - Similar techniques with that used for detection and evasion of IDS systems could be used from an attacker to cause a DoS either to the CenterTrack (a single-point-of-failure) or the overlay network itself
  - If the attack target is the edge router itself then the system would try to reroute traffic destined to the edge router through this specific edge router. This could have either tunnel collapse or routing loops

Host-based Identification

- First Research Efforts, now superseded
- Two important milestones:
  - **Caller Identification System** – CIS (Jung, 1993)
  - **Caller ID**, said to be used by U.S. Air Force, Staniford-Chen and Heberlein, 1995)

Host-based Identification (2)

- **Caller Identification System (CIS)**
  - Fully distributed, aiming out identifying the attacker through the login process
  - Relies upon the login information exchanges through the systems involved in a connection chain
  - When a user from host h_1 connects to system h_n (n>2) through intermediate hosts h_2,..h_{n-1} the h_n system recursively queries the h_{n-1} host about the login information
- **Drawbacks:**
  - authentication techniques that introduce their own vulnerabilities
  - important overhead in the login process (attackers could be possibly alerted)

Host-based Identification (3)

- **Caller ID**
  - Manual traceback in every intermediate host of the connection chain
  - When an attacker connects from host h_1 to h_2,h_3,.., h_{n-1}, h_n, the system owner or security personnel break-into h_{n-1} to verify the origin of the connection, possibly using hacking techniques
  - He later breaks into h_{n-2} until he reaches h_1 which could potentially be the attacker's machine
- **Drawbacks**
  - Ethics and legal complications
  - Not-applicable in today's high-speed networks (manual processes have to be performed for every host traced)

Application Level

- **Intruder Detection and Isolation Protocol (IDIP)**
  - Currently being scaled to multiple administration domains across the Internet
  - Low cost integration with intrusion detection techniques but is also adding new response mechanisms along with new response algorithms
  - Support of Common Intrusion Specification Language (CISL) as the language providing a unified explanation of a security incident
  - Results have shown that the protocol is performing well when integrated with IDS systems within the DARPA research community
  - **Joint Research Effort:** Network Associates & Boeing Phantom Works, 2002

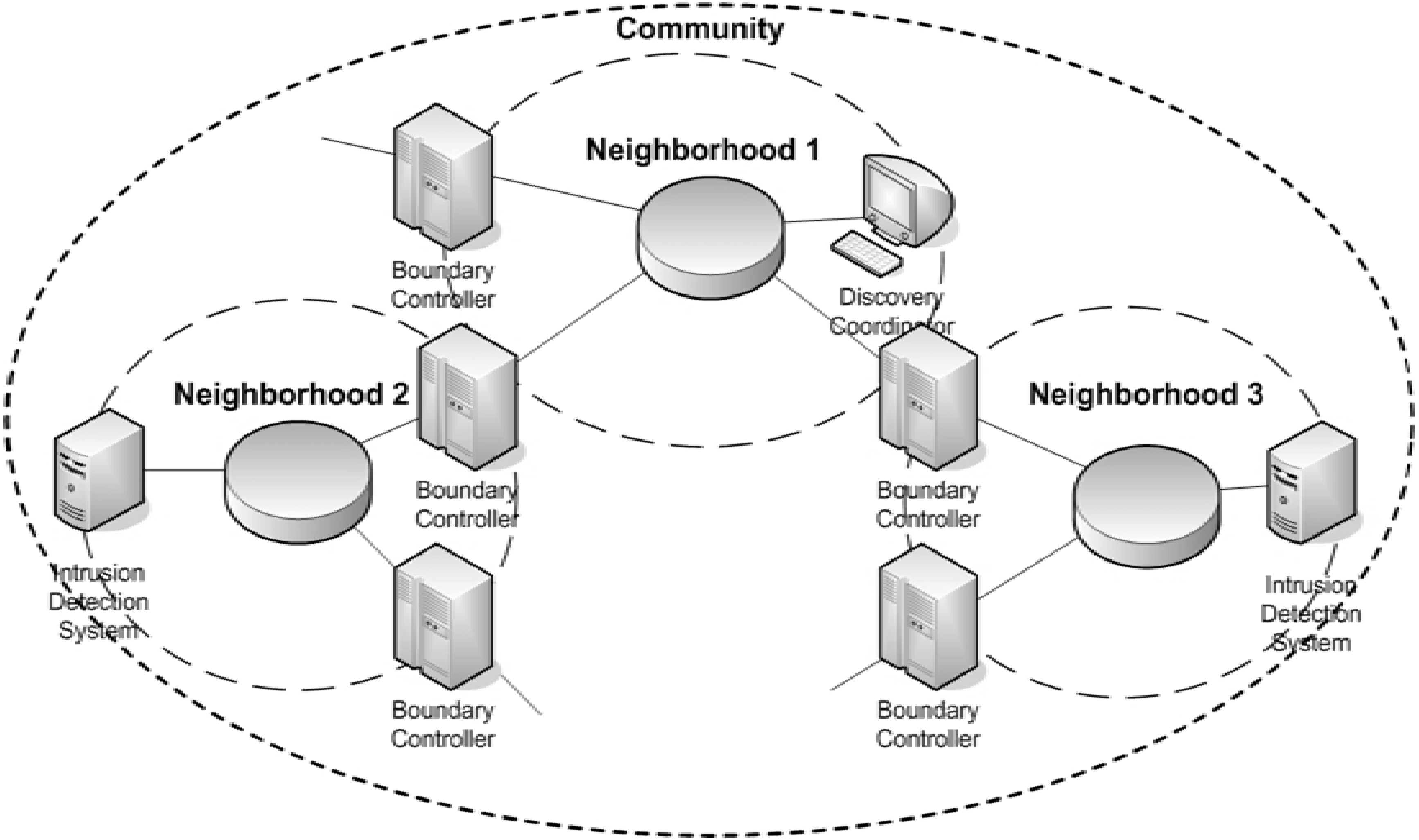
Application Level (2)

- **Architecture:**
  - Systems that belong to the same administrative domain and run the IDIP (IDIP components) are forming an IDIP neighborhood
  - Multiple IDIP neighborhoods, in turn, form an IDIP Community without the need of another coordination component
  - A component called Discovery Coordination is managing all intrusion detection and response actions within an IDIP Community
  - Systems running IDIP that belong to more than one IDIP neighborhood are called boundary controllers

Application Level (3)

- **Operation:**
  - When a connection (or a datagram stream) is in progress within an IDIP-protected network, every IDIP system (node) is auditing the connection for patterns of attack using intrusion detection technologies
  - When signs of an attack are detected by an IDIP component the detector is informed and, in turn, it spreads the attack information to all the systems within the Community (and further to the IDIP Neighborhood)
  - By this, the attack information is distributed along the path of the attack.

Application Level (4)



Categorization of traceback methods

- **Objectives**:
  - To enhance the power of digital forensics methodologies
  - To counter the limitations of classic Incident Handling & Response capabilities
  - To summarize the nature, behavior, architecture, applicability and complexity of traceback methods

Classification Dimensions

- **Nature:** host-based, network-based or both
  - Host-based methods provide accuracy and are more probable to prove the actual attacker while adding more processing overhead
  - Network-based techniques provide automation, efficiency and effectiveness, while (some of them) are able to detect stepping-stones
- **Behavior:** proactive or reactive
  - Proactively relies on the recording of connection states or login information (introduces a significant amount of processing overhead to all tracking devices)
  - Reactively relies on dynamical correlation of ingress and egress traffic (reduces processing overhead but is susceptible to misleading information provided by attackers using stepping stones)

Classification Dimensions (2)

- **Architecture:** centralized or distributed
  - A centralized solution, incorporating a central intrusion response module is a single point of failure while providing coordinated responses and decisions
  - Distributed architectural models provide redundancy but suffer time synchronization and response coordination
- **Applicability:** This field can vary from a private network, an autonomous system, or even the Internet
- **Complexity:** the amount of re-engineering functions that have to be performed in current Internet infrastructure

Classification Results

Method	Nature	Behaviour	Architecture	Applicability	Complexity
IP marking	Network	Proactive	Distributed	Internet	High
ICMP traceback	Network	Proactive	Distributed	Internet	Medium
Overlay Networks	Network	Proactive	Centralized	Autonomous Systems	Medium
Host-based Approaches	Host	Reactive	Centralized	Autonomous Systems, Cross-Administrative Domains	Low
Application Level	Both	Reactive	Centralized	Internet	High

Future Work

- Evaluation of the proposed methods either in test-beds or, hopefully, in controlled real-world deployments
- Technical issues: most of these methods have produced only prototypes,
- Political issues: preventing from testing these methods in cross-administrative domains (cooperation between many ISPs would be required in order to record attack paths or allow for traceback methods within their controlled and protected network infrastructure)
- A detailed operating framework of traceback mechanisms supporting configurable and user-defined policies would provide Network Forensics methodologies a common ground to counter political and legal issues

Summary

- A brief overview of the traceback problem
- Features of Software, Network and Computer Forensics
- Various traceback mechanisms were examined and categorized according to their features and modes of operation
- A classification for all traceback methods was proposed in order to assess and combine their benefits so as to provide enough information for Digital Forensics analyses

Questions ???

Thank you !!!

Christos Douligeris
Department of Informatics / University of Piraeus,
80, Karaoli and Dimitriou Street, Piraeus, GREECE
cdoulig@unipi.gr