Towards a Corporate Incident Response Policy Framework

By

Dimitrios G. Patsos,

Ph.D. (C), M.Sc., CMA, CME
University of Piraeus,
Department of Informatics,
80 Karaoli and Dimitriou Str.,
Piraeus 185 34, Greece

AGENDA

- Introduction
- Managing Incident Response
- Structuring an Incident Response Capability within an organization
- Network Forensics: Tracing back a security incident
- Automating the trace-back process
- Conclusions

INTRODUCTION

- **Security incident:**
  - *“any related activity with negative security implications”*
- **Incident Response:**
  - *“the process that aims to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents”*

- What about Responding to a security incident ?
- Is it a technical or a management issue (or both) ?

INTRODUCTION (2)

- **Why management?**
- Incident Response is not described in any globally accepted IT Security Standard
  - ISO/IEC 17799:2000 (Part 1) – The standard is incomplete (deal with Incident Handling)
  - …So does BS 7799 (Part 1)
- **But…**
  - Federal Agencies are obliged to comply with Incident Response requirements of Federal Information Security Management Act (FISMA 2002)
  - …and OMB’s Circular No. A-130, Appendix III
  - …and RFC 2350
  - …and A.D.A.E. requirements (Greece)

How can we mirror certain (high-level) Policy requirement to (low-level) security controls ?

INTRODUCTION (3)

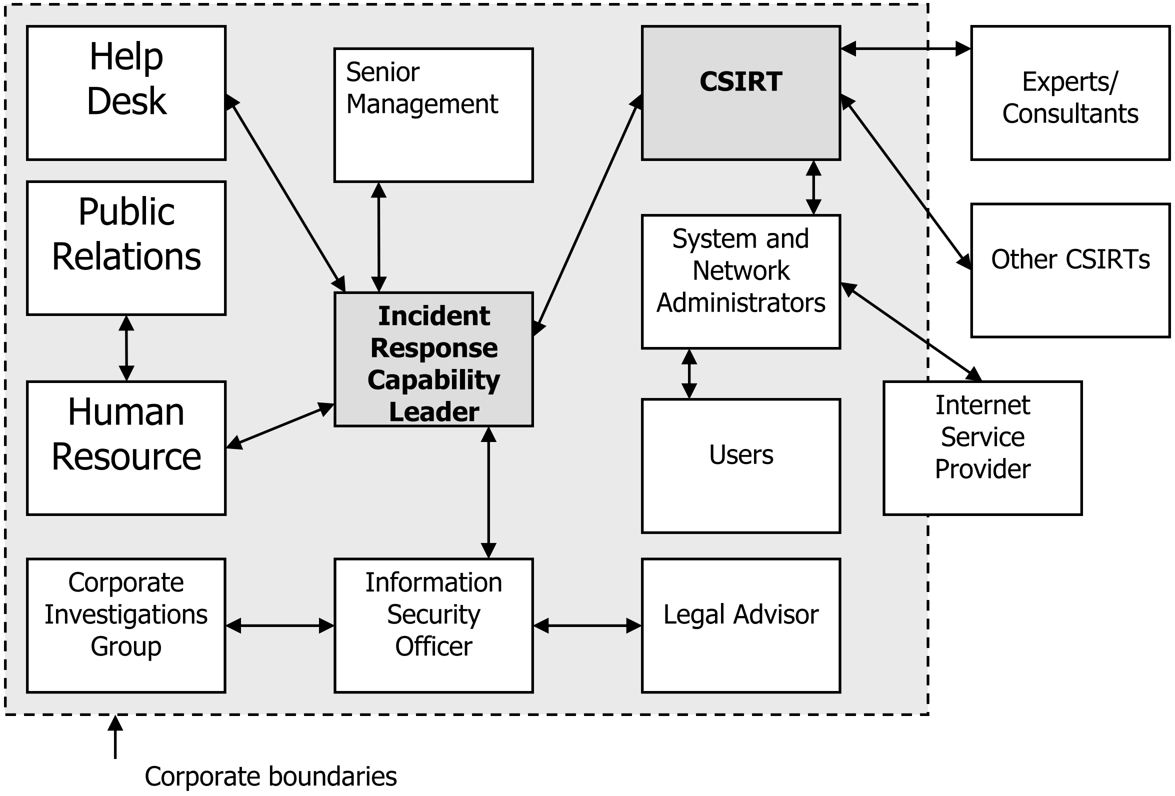
- **Why technical ?**
- Even if an Incident Response Policy is formally accepted within an organization:
  - How can we identify a real security incident with limited security infrastructure ?
  - How can we minimize the incident’s effects ?
  - How can we isolate the incident ?
  - How can we trace the source(s) ?
  - How can we be sure that the attacker(s) traced is the real one(s) ?

INTRODUCTION (4)

- **We propose:**
  - A management framework for a corporate environment
  - A structured technical methodology of six (6) distinct phases
  - A classification of threat escalation levels
  - An integration with automated trace-back mechanisms
  - An example case study
- **We examine:**
  - Celebrated automated trace-back mechanisms at all possible layers

MANAGING INCIDENT RESPONSE

- The necessary parties that have to be involved in an Incident Response Capability are known as “Contacts”, and include:


Help Desk
Public Relations
Human Resource
Corporate Investigations Group
Senior Management
Incident Response Capability Leader
Information Security Officer
CSIRT
System and Network Administrators
Users
Legal Advisor
Experts/ Consultants
Other CSIRTs
Internet Service Provider
Corporate boundaries

STRUCTURING AN INCIDENT RESPONSE CAPABILITY WITHIN AN ORGANIZATION

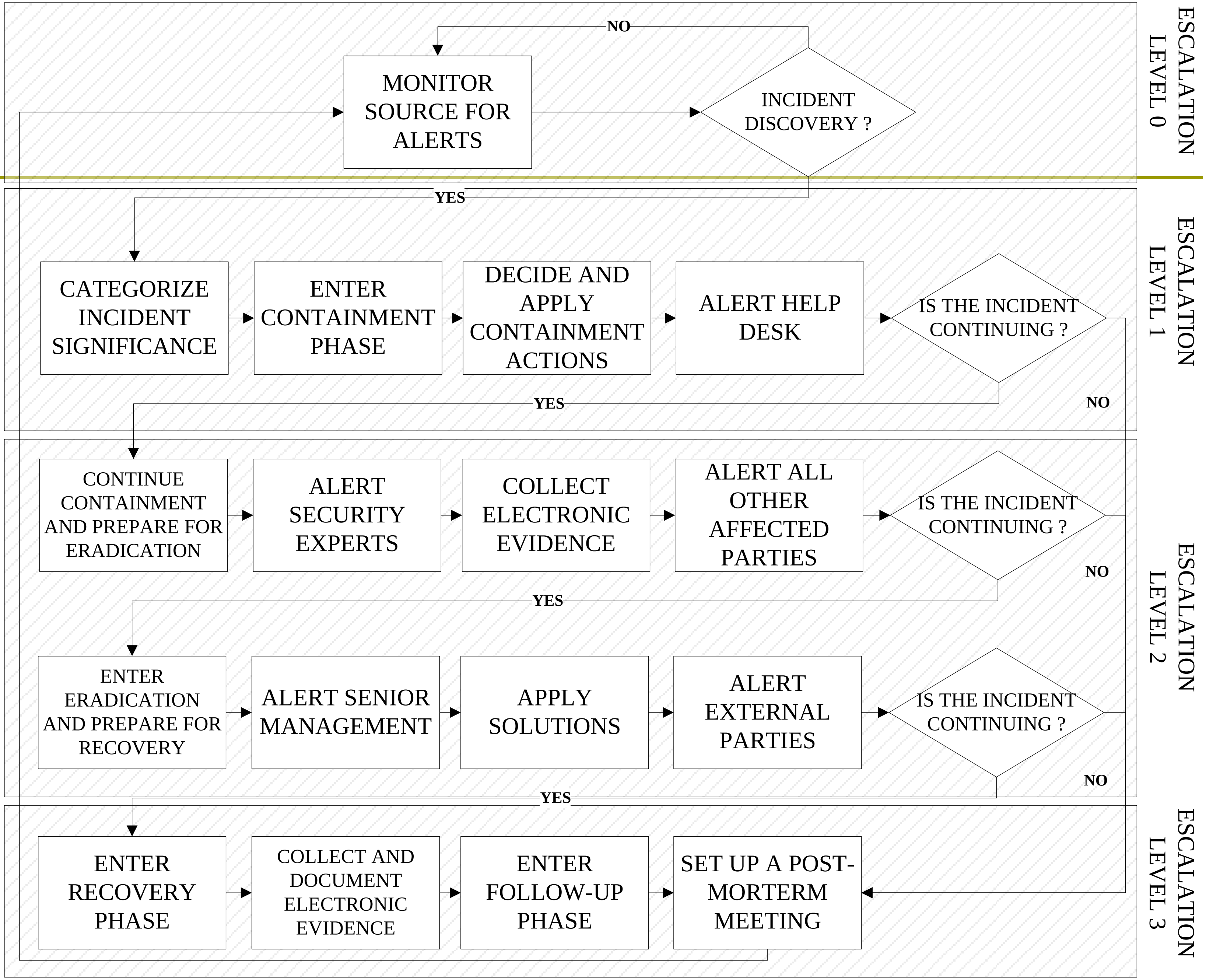
- A structured methodology is needed. We divide the whole process in the:
  - **Preparation Phase:** to prepare for the inevitable…
  - **Identification Phase:** to positively identify a security incident from “security noise”
  - **Containment Phase:** to apply-short term solution to the incident
  - **Eradication Phase:** to completely eliminate the incident’s occurrence
  - **Recovery Phase:** to recover from the effects of the incident
  - **Follow-Up Phase:** to learn from the incident

STRUCTURING AN INCIDENT RESPONSE CAPABILITY WITHIN AN ORGANIZATION (2)

- An incident's significance is increasing as time passes (true for the most of known security incidents). This parameter is called "escalation level" and usually falls within one of the following –broad- categories:
  - **Level 0**, where the operations are normal and there is no evidence that a security incident is occurring
  - **Level 1**, where a threat is discovered and the initial responses are taken
  - **Level 2**, where the threat is spreading and containment actions are taken
  - **Level 3**, where the threat has become significant and containment along with recovery actions are taken.

STRUCTURING AN INCIDENT RESPONSE CAPABILITY WITHIN AN ORGANIZATION (3)

- So far we have:
  - A management framework
  - A structured methodology
  - A classification of an incident’s impact (escalation levels)
- The case is to combine all these dimensions in a formal process
- We therefore present an example (and rather limited) case-study



ESCALATION LEVEL 0

MONITOR SOURCE FOR ALERTS

INCIDENT DISCOVERY ?

NO

YES

ESCALATION LEVEL 1

CATEGORIZE INCIDENT SIGNIFICANCE

ENTER CONTAINMENT PHASE

DECIDE AND APPLY CONTAINMENT ACTIONS

ALERT HELP DESK

IS THE INCIDENT CONTINUING ?

YES

NO

ESCALATION LEVEL 2

CONTINUE CONTAINMENT AND PREPARE FOR ERADICATION

ALERT SECURITY EXPERTS

COLLECT ELECTRONIC EVIDENCE

ALERT ALL OTHER AFFECTED PARTIES

IS THE INCIDENT CONTINUING ?

NO

YES

ENTER ERADICATION AND PREPARE FOR RECOVERY

ALERT SENIOR MANAGEMENT

APPLY SOLUTIONS

ALERT EXTERNAL PARTIES

IS THE INCIDENT CONTINUING ?

NO

YES

ESCALATION LEVEL 3

ENTER RECOVERY PHASE

COLLECT AND DOCUMENT ELECTRONIC EVIDENCE

ENTER FOLLOW-UP PHASE

SET UP A POST-MORTERM MEETING

TRACING BACK A SECURITY INCIDENT

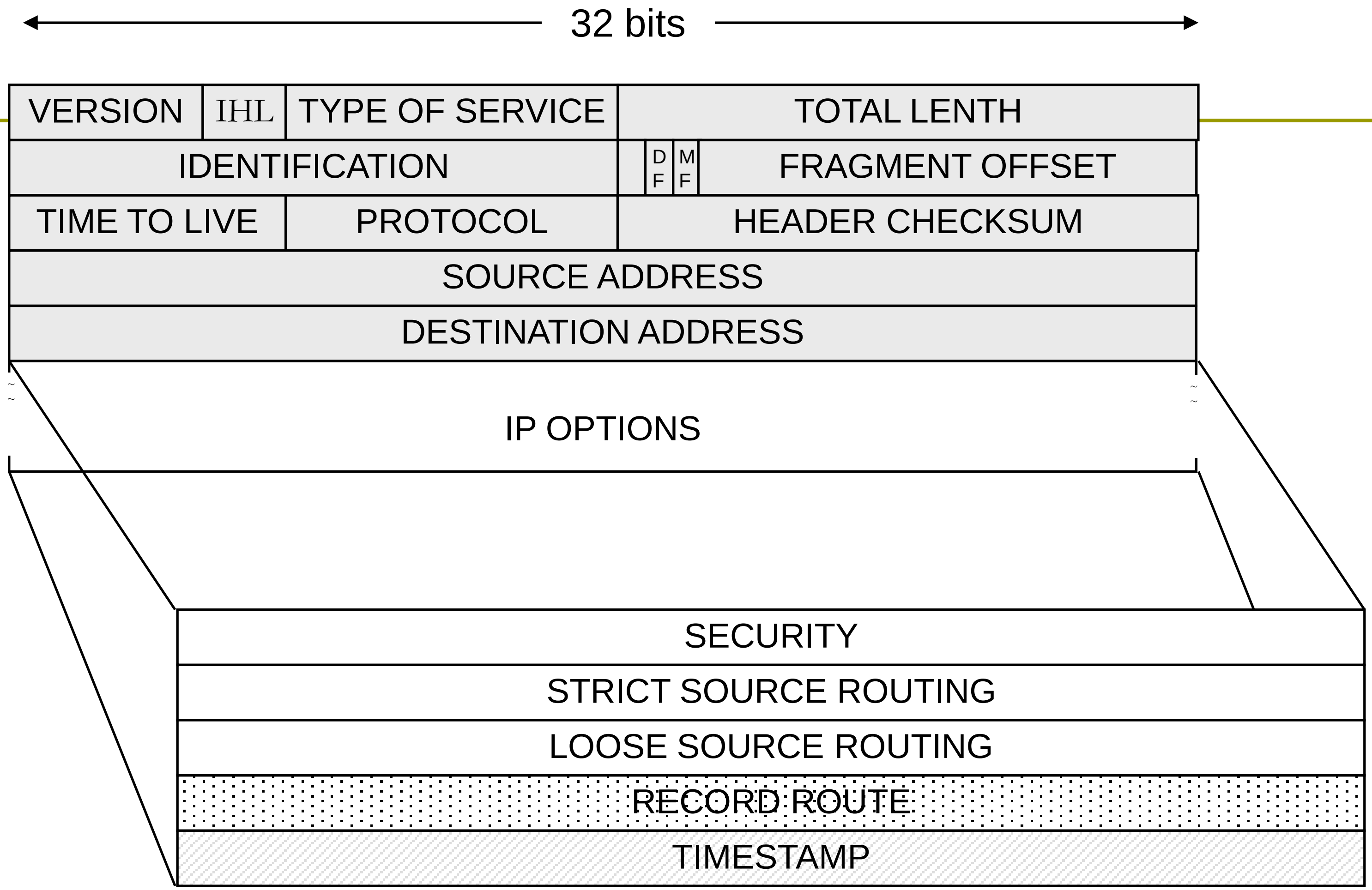
- Handling a security incident is not always efficient
- There are cases that the actual source has to be traced and the attacker(s) held accountable – (i.e. Incident Response vs. Incident Handling)
- **Computer Forensics** provide a state analysis of a compromised end system
- How can we deal with stateless and volatile data found in network connections so that we can trace an attacker?
- The solution seems to be the automated trace-back mechanisms, a subset of the science of **Network Forensics**

TRACING BACK A SECURITY INCIDENT (2)

- What is trace-back?
  - 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
- An attacker uses multiple techniques to hide his real identity, so trace-back is non-trivial. For example:
  - Link Layer Spoofing
  - IP source address spoofing
  - Port forwarding
  - Application spoofing
  - “Stepping stones”, in modern DDoS attacks

TRACING BACK A SECURITY INCIDENT (3)

- 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
- 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



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 BACK A SECURITY INCIDENT (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)

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)

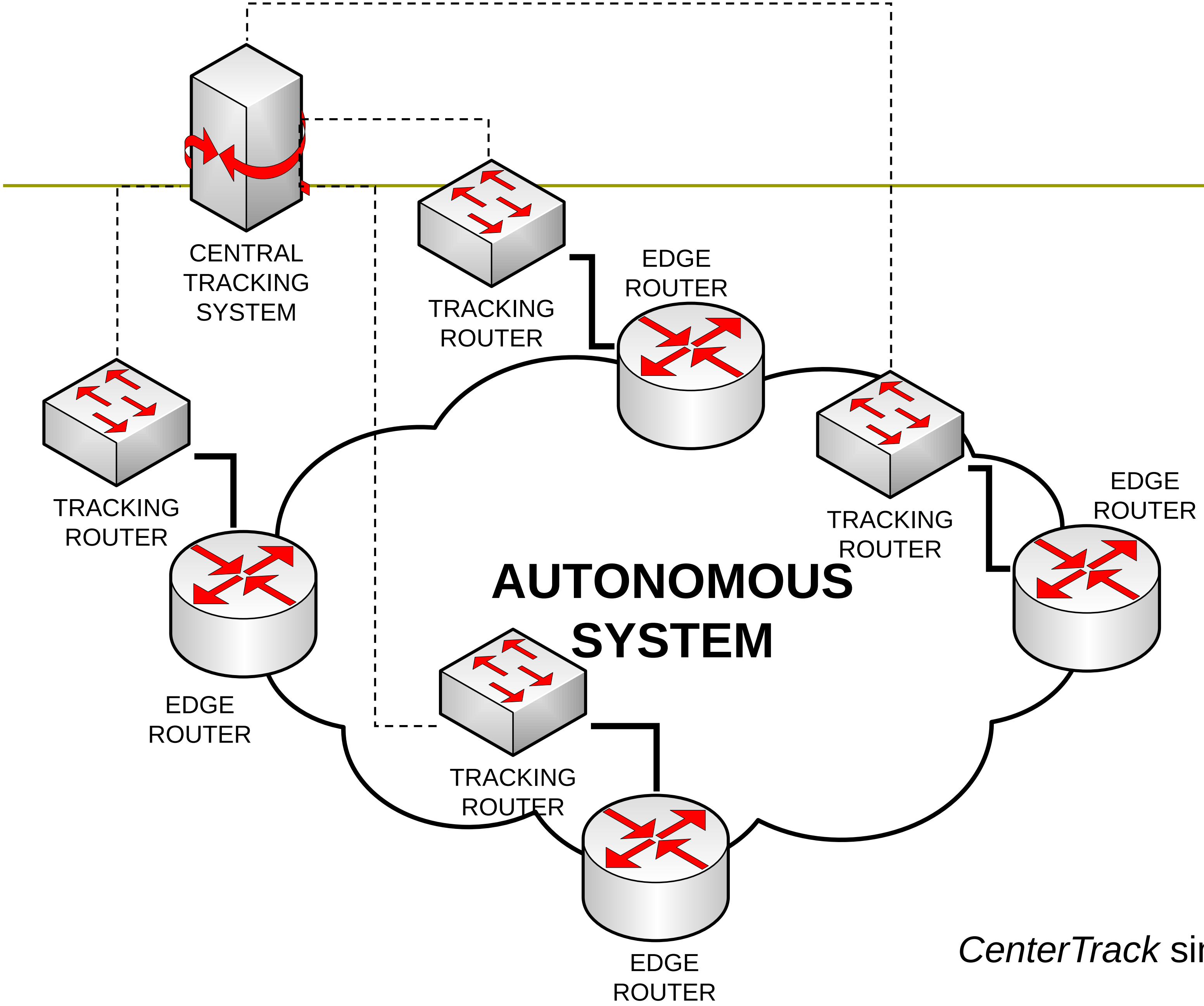
- The number of *iTrace* packets generated by a router is small, which implies a low overhead (statistically, around 0.005%)
- It mainly addresses attacks where a significant amount of traffic comes from a rather small number of sources, due to the lower probability of generating *iTrace* packets
- **Enhancement:**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

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)

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

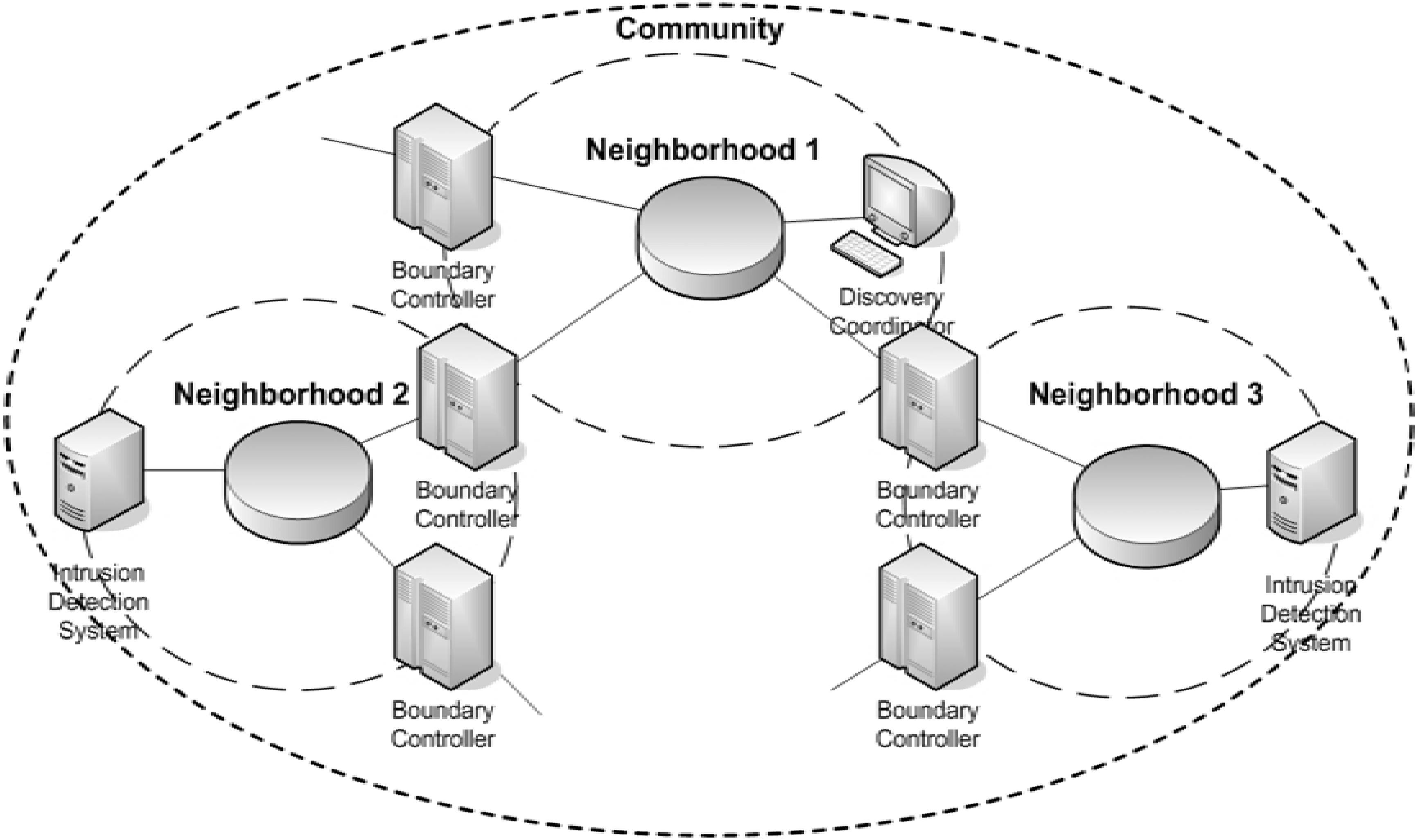
Application Level (2)

- **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)



Summary and Conclusions

- Incident Response stretches the capabilities of Incident Handling by actively handling a security incident
- Lot of work has to be done in International Standardization Bodies in order to provide a complete framework
- Automated trace-back mechanisms are still in their early infancy (and still filtered by firewalls or other security devices)
- On the other-hand, policy-driven responses through automated trace-back mechanisms could provide completeness
- Our next step is to incorporate specific policy requirements into a security information management system to provide guidance for automated responses.

Acknowledgements

- This work has been partially supported by GSRT under a PENED grant and by the IST FET Coordination Action ACCA (006475)

Questions ???

Thank you !