Confiabilidade de Sistemas Distribuídos
Dependable Distributed Systems

DI-FCT-UNL, Henrique Domingos, Nuno Preguiça

Lect. 7
Intrusion Detection Systems

2015/2016, 2nd SEM

MIEI
Mestrado Integrado em Engenharia Informática

Last lecture (L6): Pro-Active Recovery

- Intrusion Detection Systems vs Intrusion Recovery
  - Reactive IR vs. Pro-Active IR
- Approach to Pro-Active Recovery Solutions
- PAXOS PR
- COCA

- Suggested Readings (See papers in CLIP):
  - PAXOS-PR
    - Background Inspiration for TP2 Approach (subset)
  - COCA
    - Interesting in the combined use of Threshold-Signatures in a Pro-Active Recovery Solution for Intrusion Tolerant Certification Authority Case (Resgistration/Directory)

Today:
Intrusion Detection

Topics following the bibliography
W. Stallings, L. Brown, Computer Security – Principles and Practice, Chap. 8

Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

Intruders and Intrusion Attacks

- Verizon report about investigated breaches:
  - ~90% from external attackers (outsiders)
  - ~14 from insiders
  - Some of them from both
  - Insiders: responsible by a small number of very large dataset compromises
- Currently, intrusions noticed as increasing attacks in malicious hacking activities and "specifically targeted" systems (ex., SW) ai individuals in organizations and used IT systems
  - Require "in-depth" strategies, because targeted attacks bypass perimeter defenses (FW and other IPS solutions)

Interesting reports

- Verizon, 2013 Data Breach Investigations Report, April 2013 (cyted on Stallings, Computer Security: Principles and Practice, 2015)
  - 2015 Report: http://www.verizonenterprise.com/DBIR/
- Symantec Internet Security Report, 2015
- Both reports provided in the CLIP Docs.

Intruders and motivations

- Cyber-criminals
- Activism (or cyber-hacktivists)
- State-sponsored organizations
- Others (different connotation)
  - Apprentice, script-kiddie, …
  - Journeymans,
  - Masters
  - Other common use characterizations:
    - Black, white, gray, … ethical hackers …
    - Vulnerability testers, Penetration testers (Pen-tests), Offensive-Security , …. using black-box, white-box and gray-box approaches

---

See Bibliography (CLIP) and available reports: Symantec Security Report (2015)
Other sources:
Mandiant: APT1 – Exposing one of China's Cyber Espionage Units, 2013, http://intelreport.mandiant.com
https://en.wikipedia.org/wiki/Penetration_test

Intrusion actions: from “benign” to “serious/malicious” intentions

- Performing remote root compromises of e-mail servers
- Web-server defacing
- Guessing/cracking passwords
- Copying (leakage) of data-bases with sensitive information (credit cards, social-insurance, digital identity information, …)
- Viewing of sensitive data (payroll records, no-authorized medical information – HMRs, …. Ex., Login credentials (uids/pwds) of cloud-computing/cloud storage accounts, …
- To run packet-sniffers on remote computers to inspect traffic from/to, capture of username/ pwds, … or traffic in “targeted network segments”
- To explore permission errors in anonymous FTP servers, as a vehicle for illicit distribution of pirated sw, data-contents, …
- Dialling into unsecured modems, to gain remote-access to internal networks
- Posing as an executive, call help desk to reset executive’s e-mail accounts and access illicitly to the mail account with new passwords …
- Using unattended logged-in workstations without permission
- …
- Others ???

See

W:, Stallings, L. Brown, Computer Security Principles and Practice, Chap 8, Intrusion Detection, 3rd Edition, 2015

Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

Intruder Behavior

- Attack anatomy:
  - **Target acquisition and information gathering**
    - System resources enumeration, SW vulnerability scanning, …)
  - **Initial access (exploiting an identified vulnerability)**
    - Use of exploits, obtaining/guessing weak-authentication credentials, installation of malicious SW components via social-engineering, or drive-by-dowload attacks…
  - **Privilege escalation**
    - Exploring local-access control vulnerabilities to increase privileges for desired goals
  - **More detailed information gathering** or system exploiting to attach other systems, or to compromise in-depth system resources …
  - **Access –maintenance**
    - Installation of backdoors, addition of covert-authentication credentials, configuration changes, …
  - **Covering auditable tracks**
    - Remove selective evidences from logs, disabling of system logging activity, use of rootkits or other measures to hide covertly installed malicious files or code, …

Examples, typical tools, …

- Typical vulnerability scanners and penetration testing tools
  - Ex., see https://en.wikipedia.org/wiki/Penetration_test

Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

Intrusion Detection Systems

- Definitions from the RFC 2828 (Internet Security Glossary)

- **Security Intrusion**
  - A security event or a combination of multiple **security events originating a security incident**
  - in whish an intruder (illicit agent) **gains, or attempts to gain, access to a system (any system resource)**, without having authorization to do so
  - In a Distributed Systems perspective and in general, events captured by evidences from network traffic/traffic shaping, host-based evidences (logging of operations) or possibly by suspected interactions captured by Honeypots and Honeynet-based ecosystems

- **Intrusion detection**
  - A security service to monitor, to analyze computer systems and networks events, with the purpose of finding and providing "real-time" (or soft-real-time) warnings of attempts to access system resources in an authorized manner
  - Intrusion detection as notification of some "incorrect" signature (evidence) or **anomalous state (deviation to expected correct-behavior or system/ resources/operation specification)**

Intrusion Detection Systems: Generic Components

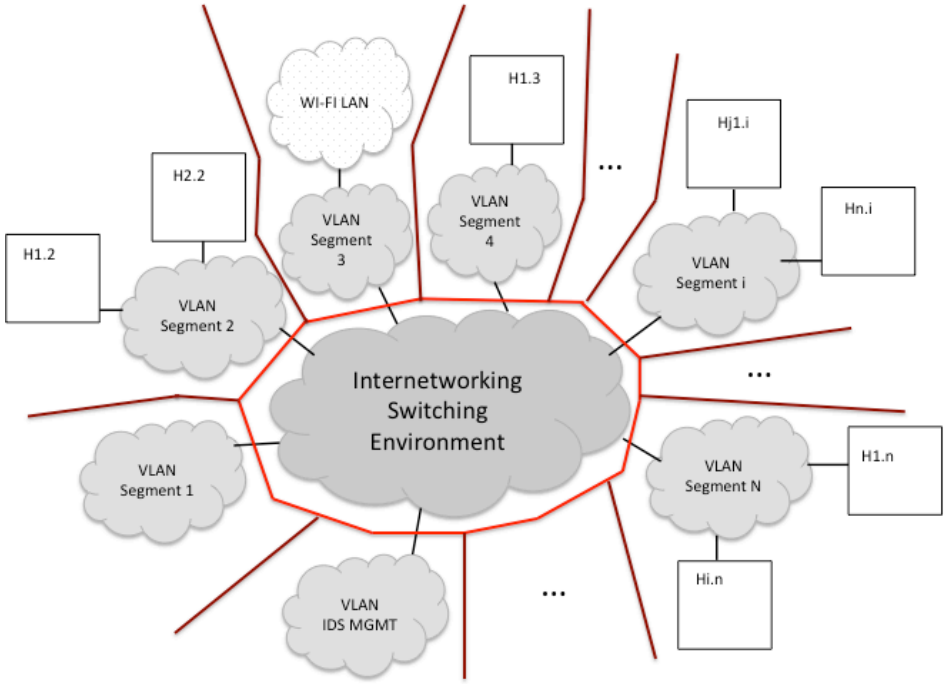
- **Sensors (or probes, intrusion probing detectors)**
  - For colleting data as intrusion evidences (traffic shapes, network packets, entries in log-files, system-call traces, …
- **Analyzers**
  - Components receiving and processing sensing events to determine if intrusion occurred
  - Output: indication + evidence (proof) + actions to be conducted as a result of the detected intrusion
- **User interfaces**
  - User visualization, control of the behavior, reporting activity, …
  - Used for management purposes (report/results to managers, operation directors, but also to system components, to fire a possible automatic reaction

Intrusion Detection Systems: Generic Components

- **Sensors (probing), Analyzers (processing) and User interfaces (visualization)**
- Distributed IDS:
  - Can distribute such components in some way, according to its specialization (IDS types)
    - Possibly using "heterogeneous" sensors and analyzers (local filtering, pre-processing, event dissemination)
    - Use of event-dissemination substrate
  - and probably using centralized points for global monitoring
    - Global analysis: aggregation, correlation and visualization

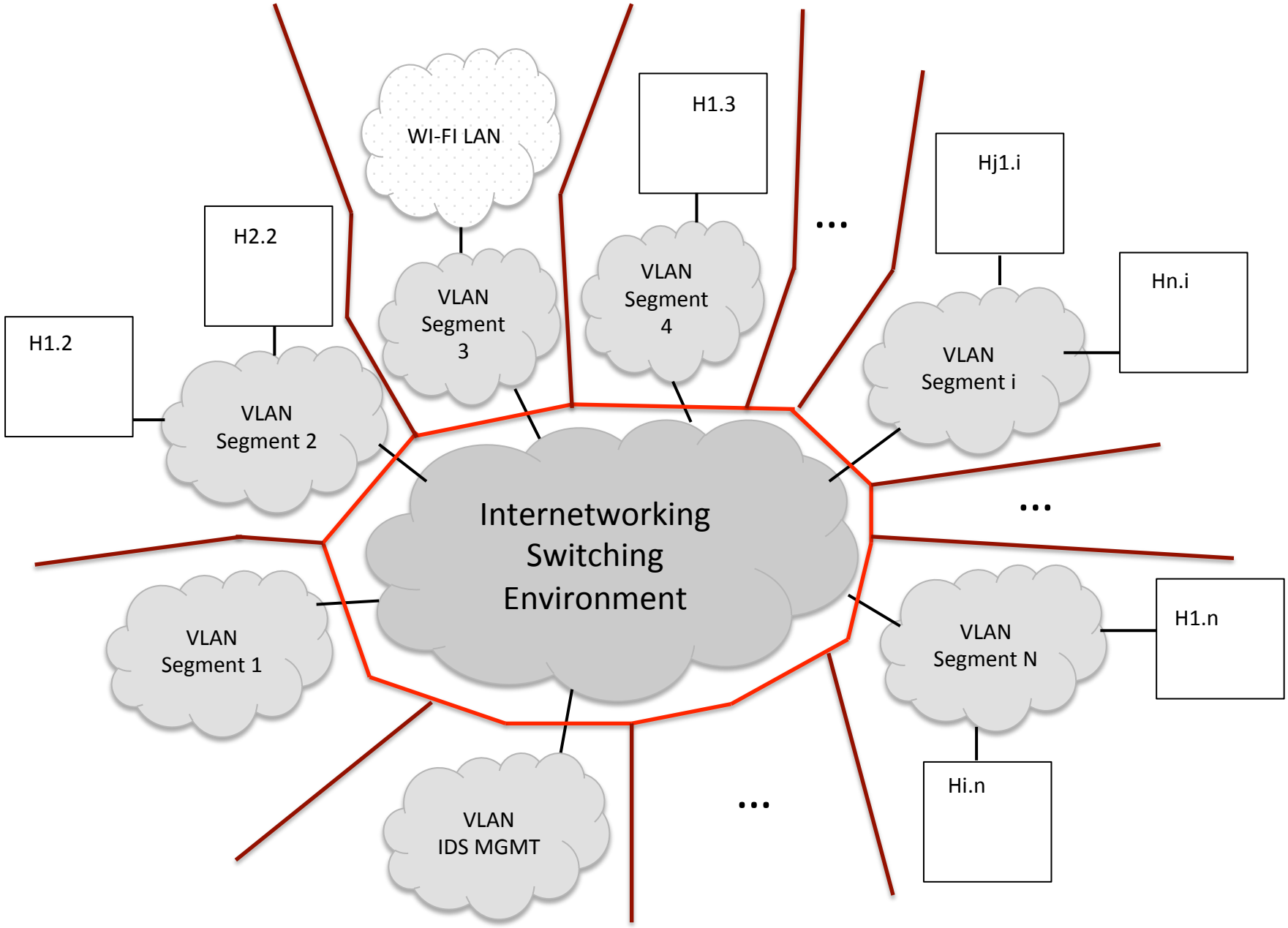
Example (DHIDS Platform)

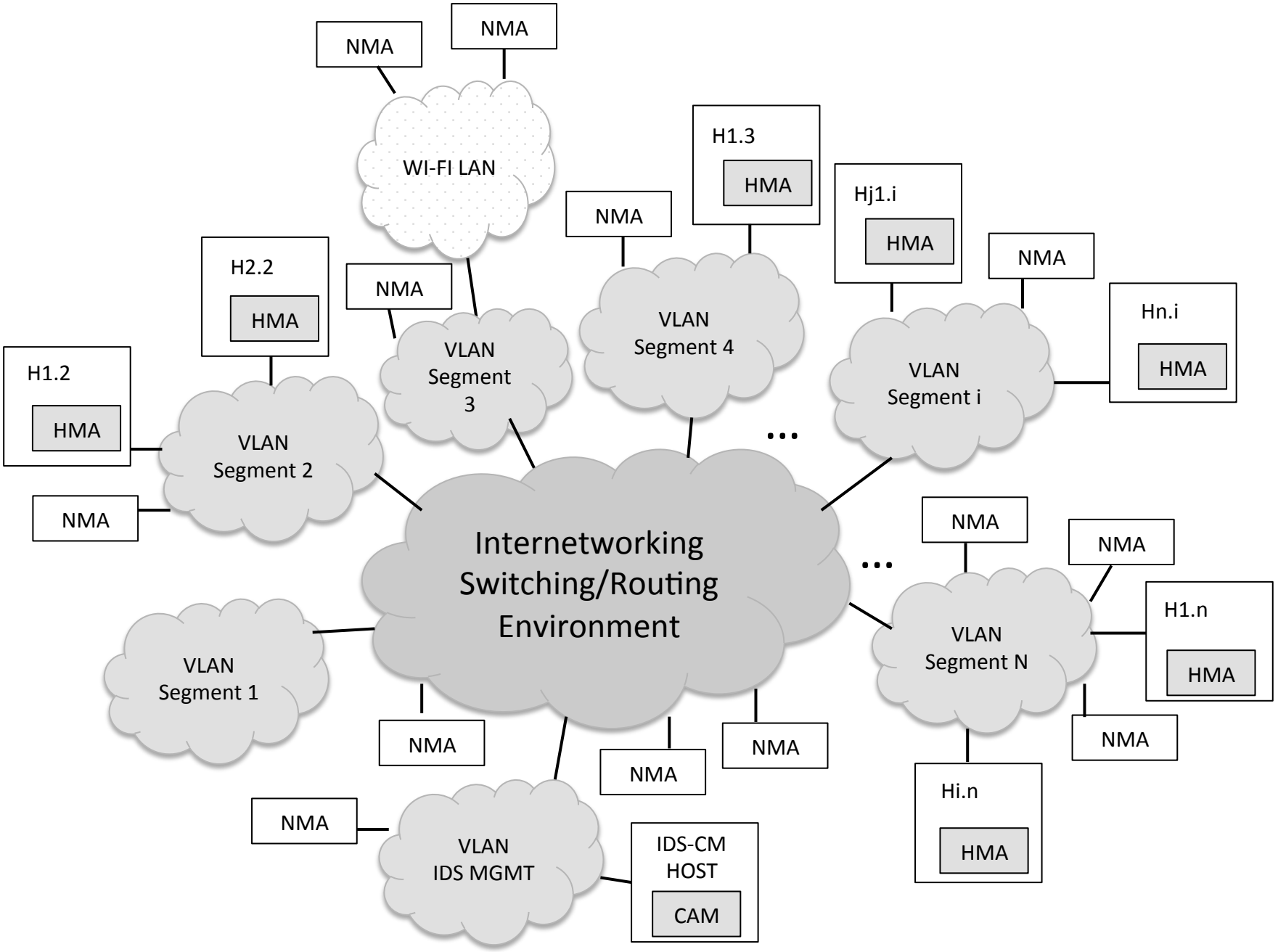
Distributed Heterogeneous Intrusion Detection Platform



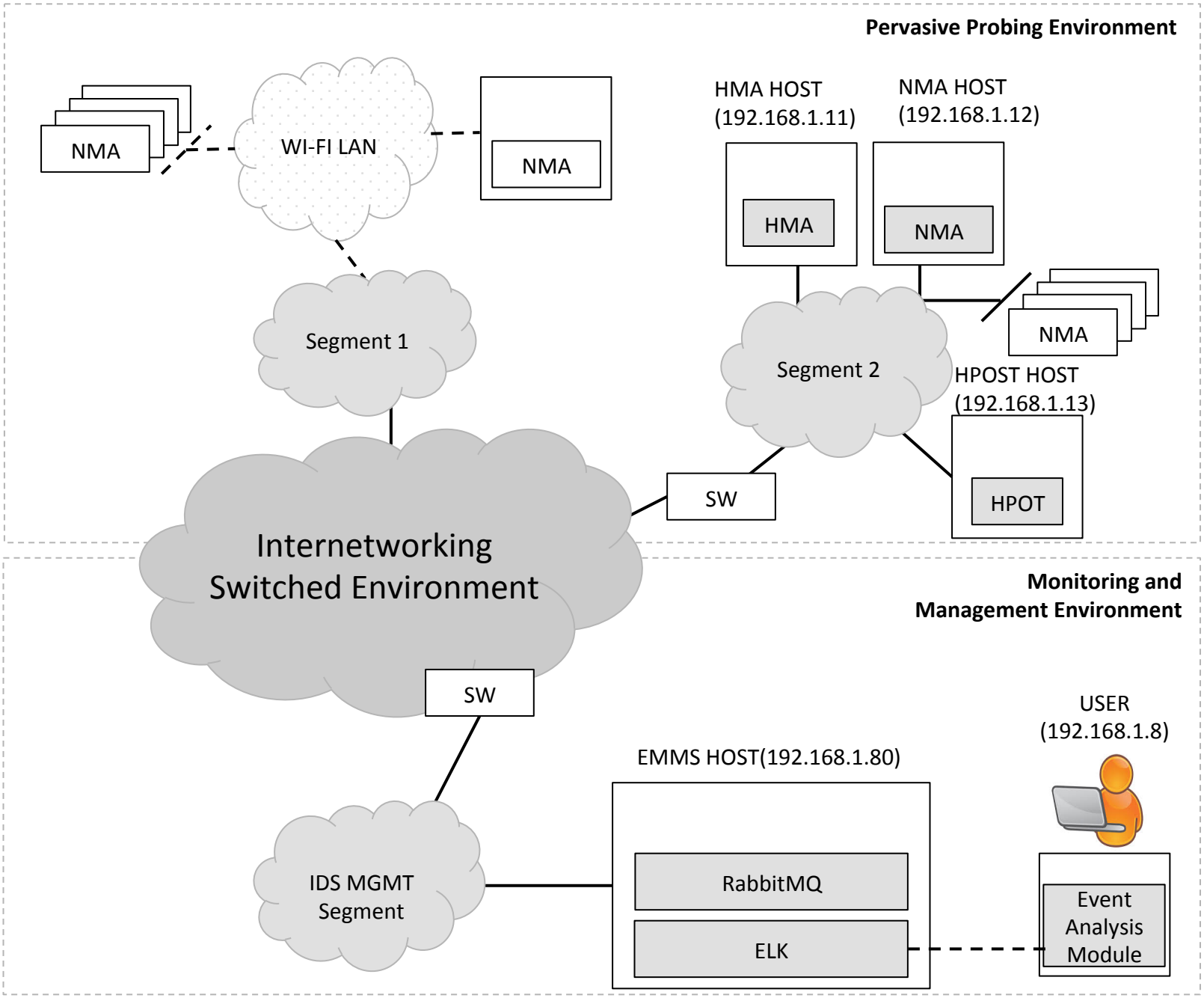
Ex.,
P. Alves, H. Domingos, *Analyzing Audit Trails in a DHIDS Platform* , MSc Thesis (DI/FCT/UN), to appear in DEBS 2016 paper, deployed for operation in a real environment in Portugal Telecom

Product Solution for the Market

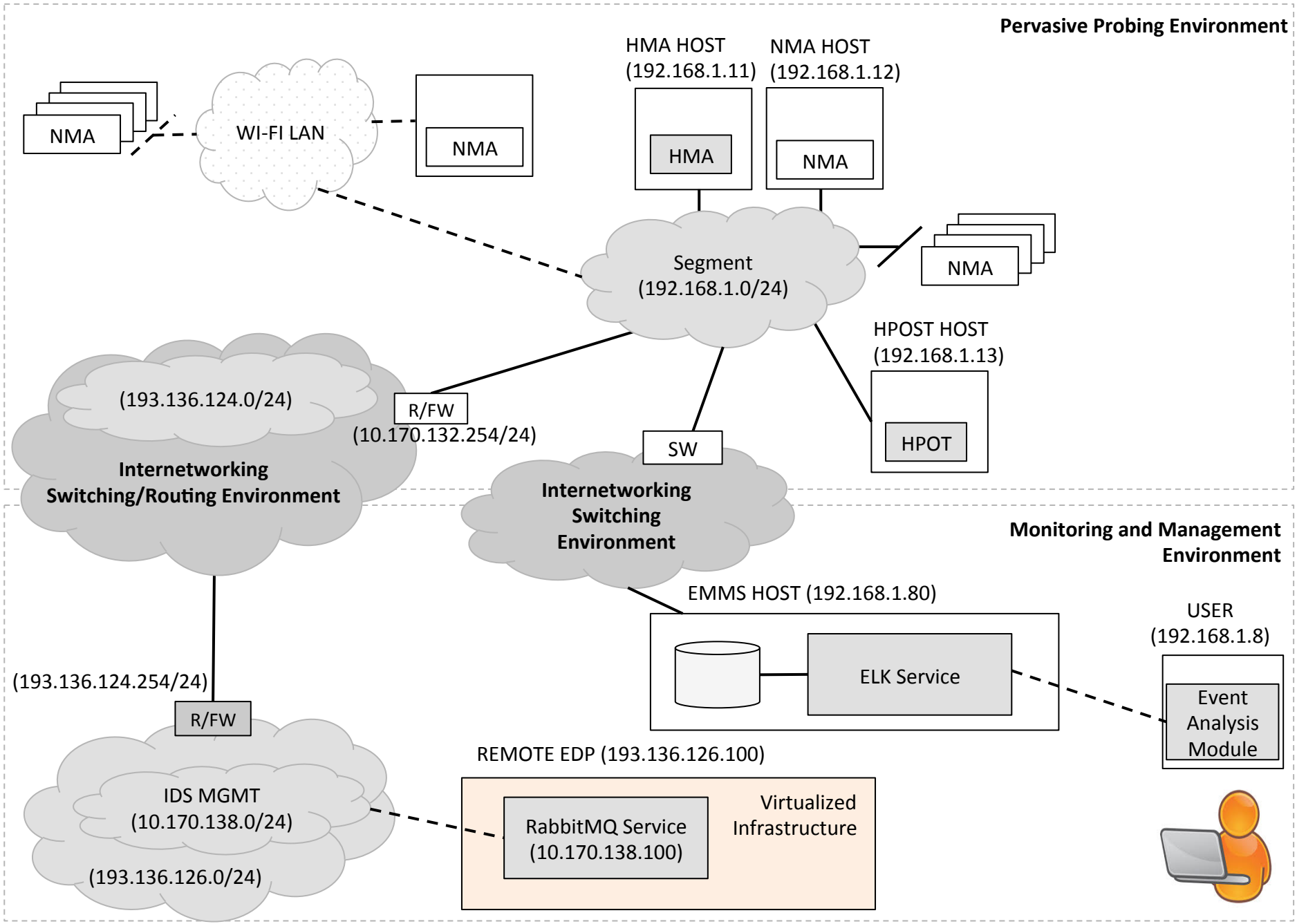

WI-FI LAN
H1.3
Hj1.i
H2.2
VLAN Segment 3
VLAN Segment 4
Hn.i
H1.2
VLAN Segment 2
VLAN Segment i
Internetworking Switching Environment
VLAN Segment 1
VLAN Segment N
H1.n
VLAN IDS MGMT
Hi.n


NMA
NMA
WI-FI LAN
H1.3
HMA
Hj1.i
HMA
NMA
NMA
H2.2
HMA
NMA
VLAN
Segment 4
VLAN
Segment i
Hn.i
HMA
VLAN
Segment
3
H1.2
HMA
VLAN
Segment 2
NMA
Internetworking
Switching/Routing
Environment
NMA
NMA
H1.n
HMA
VLAN
Segment N
VLAN
Segment 1
NMA
NMA
NMA
NMA
NMA
Hi.n
HMA
VLAN
IDS MGMT
IDS-CM
HOST
CAM

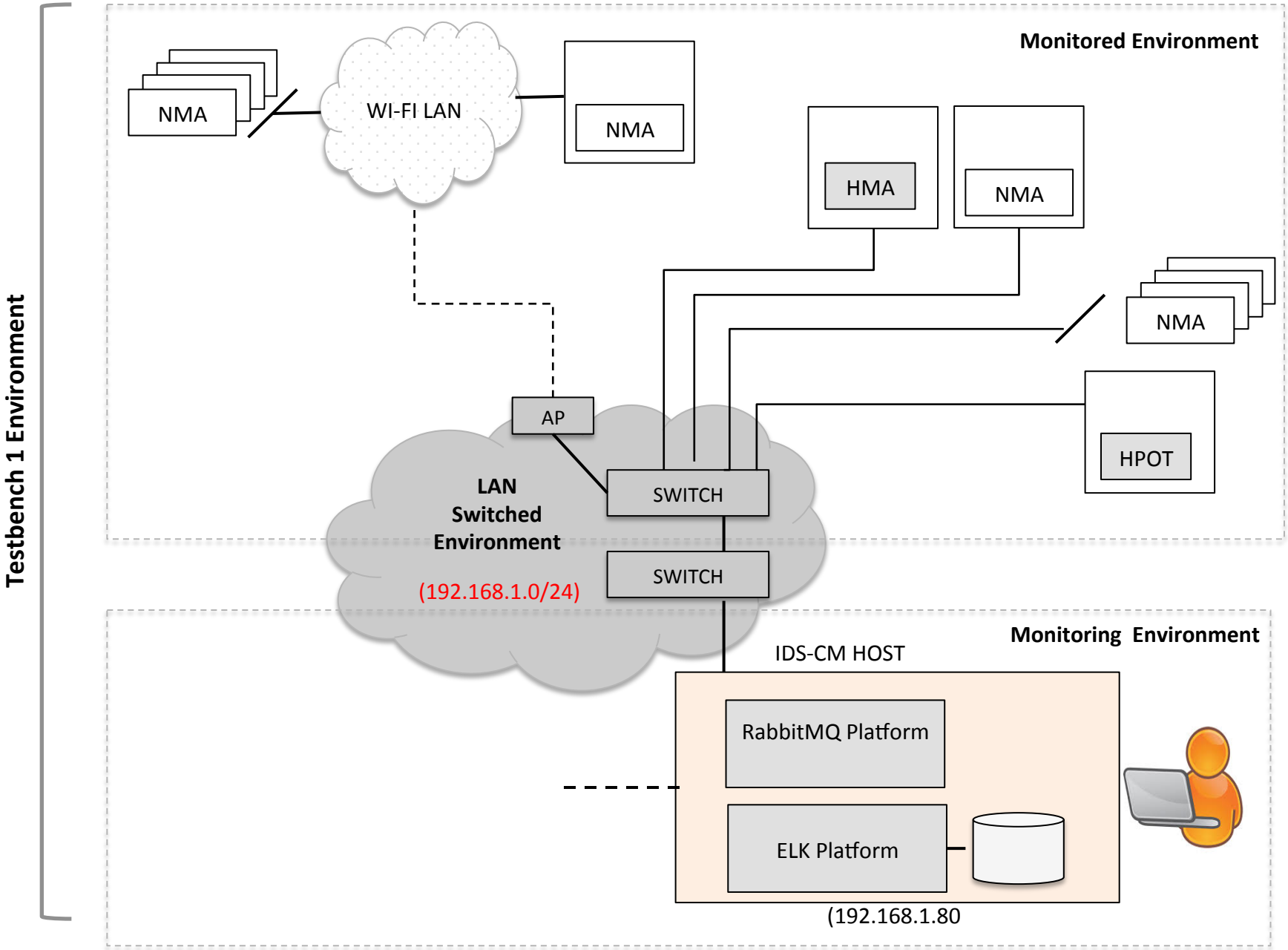
Instantiation of the Generic Internetworking Infrastructure (as introduced in Chap. 1) S1



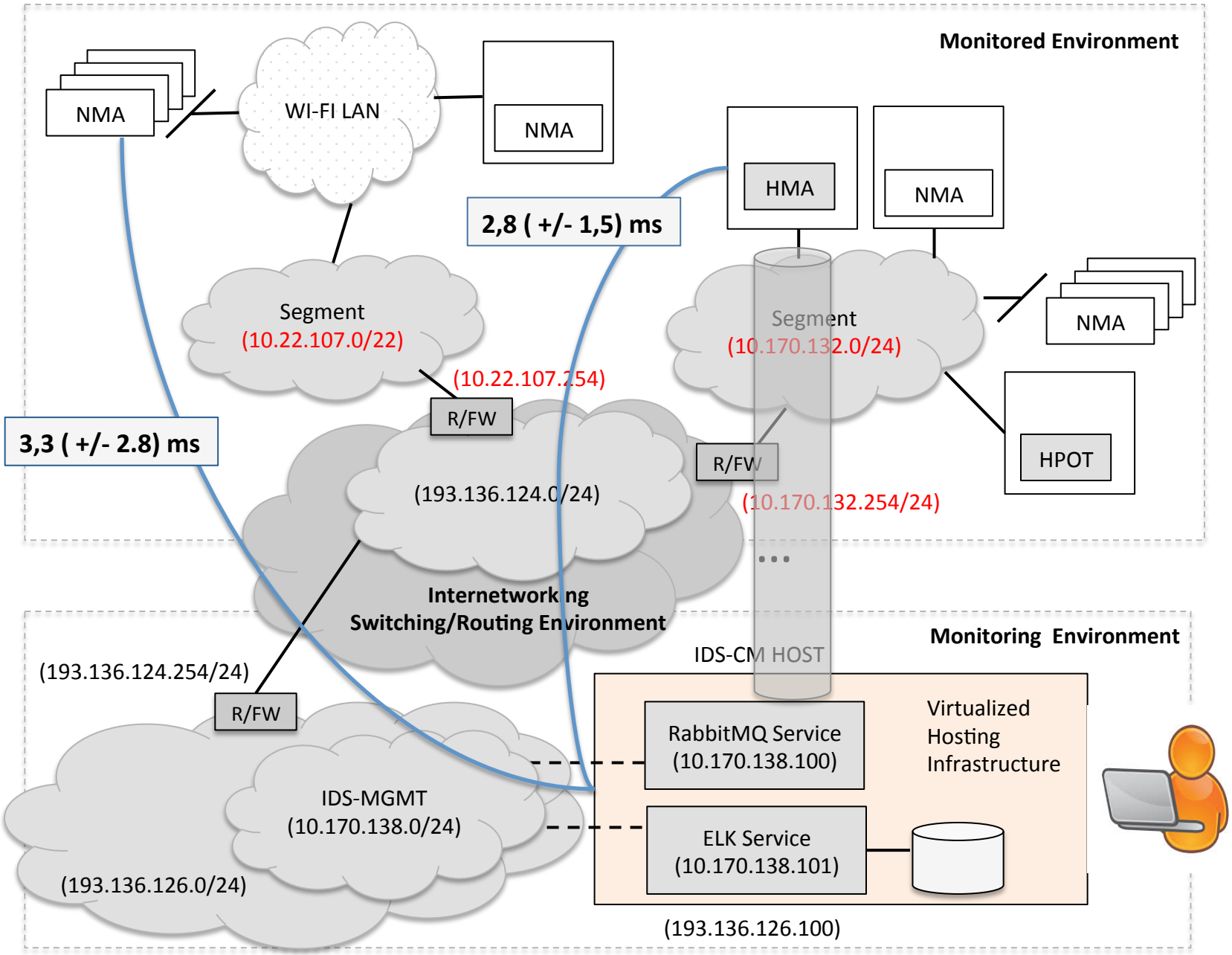
Instantiation of the Generic Internetworking Infrastructure (as introduced in Chap. 1) S2

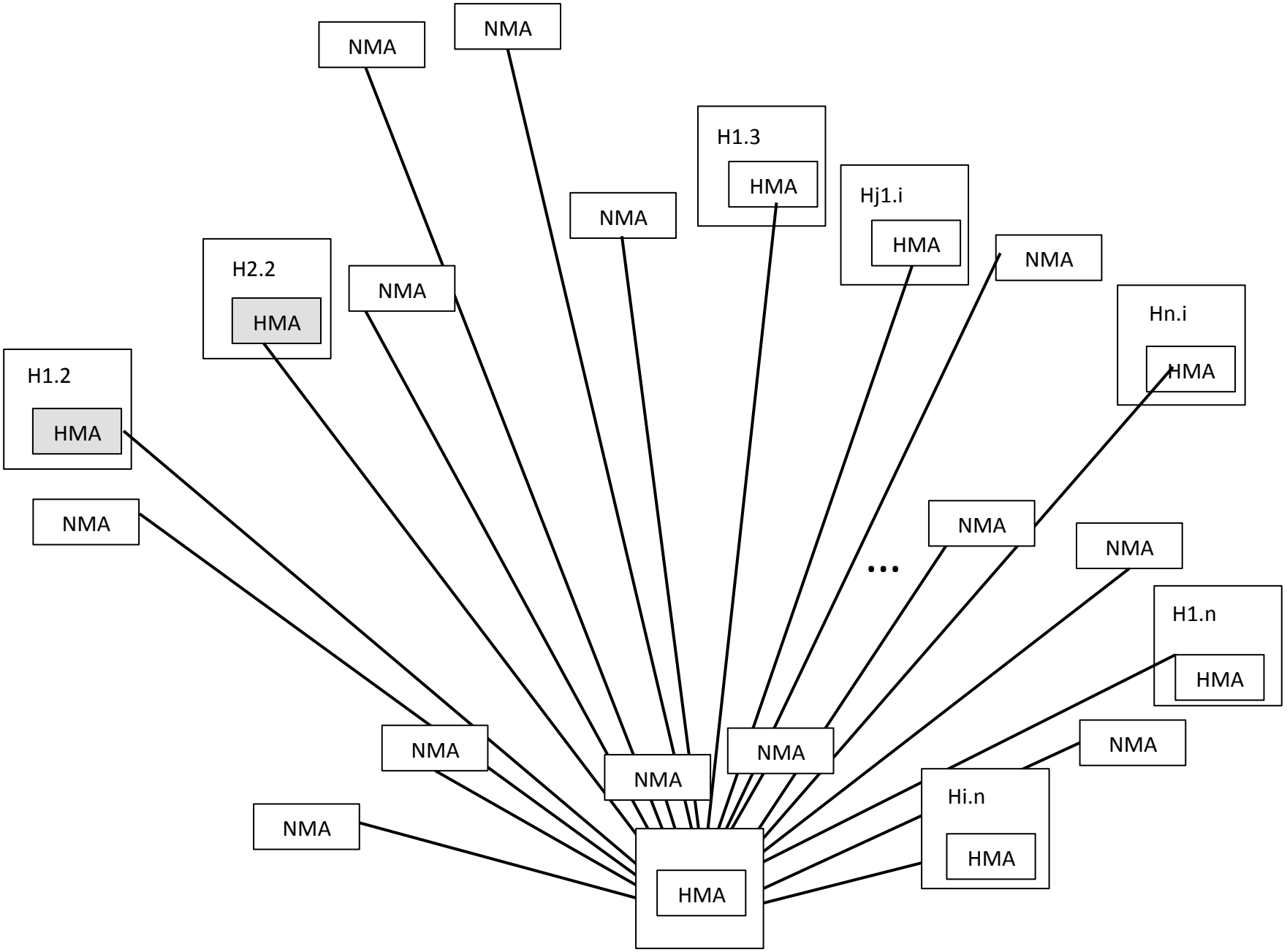


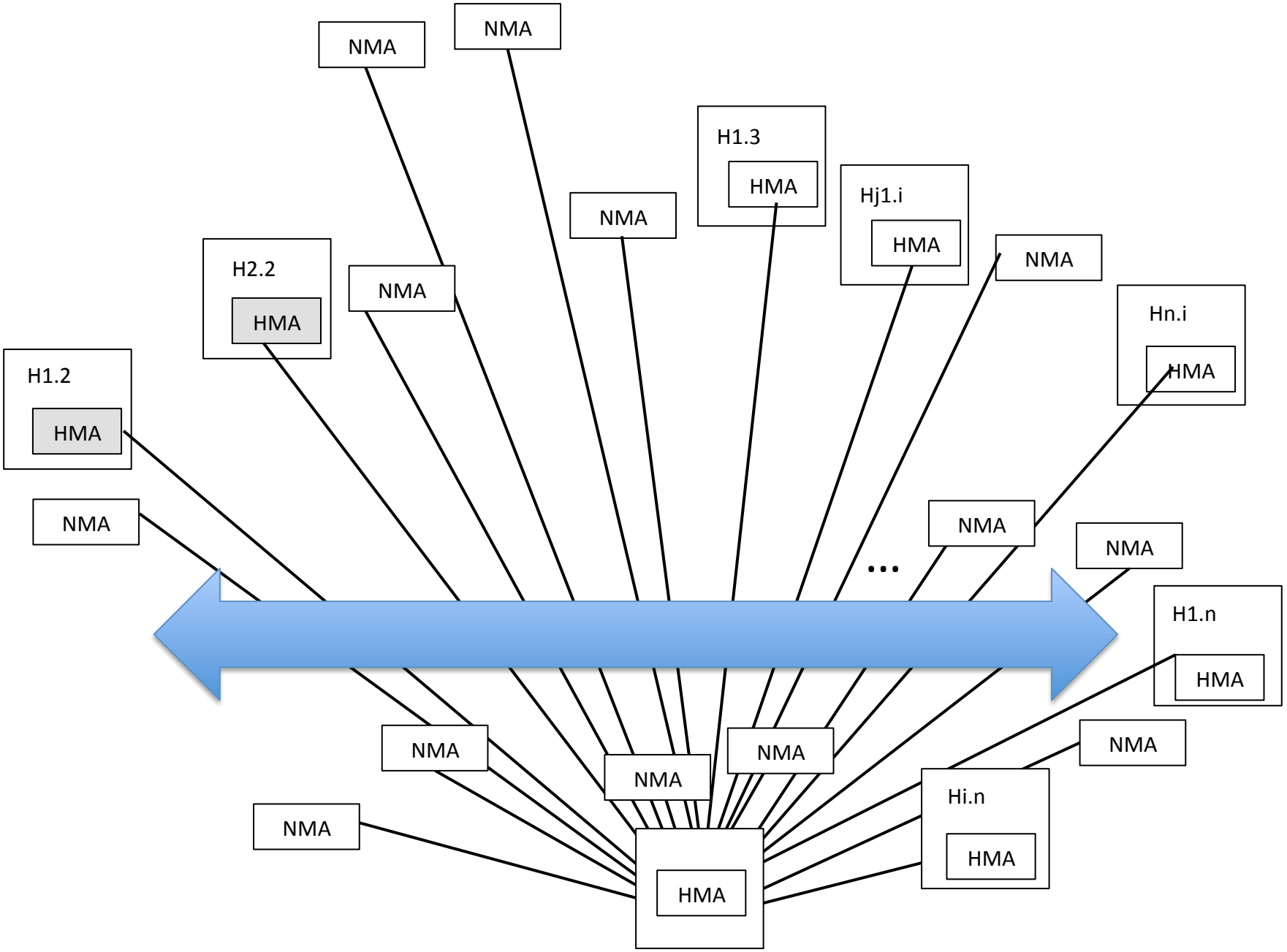
Instantiation of the Generic Internetworking Infrastructure (as introduced in Chap. 1)

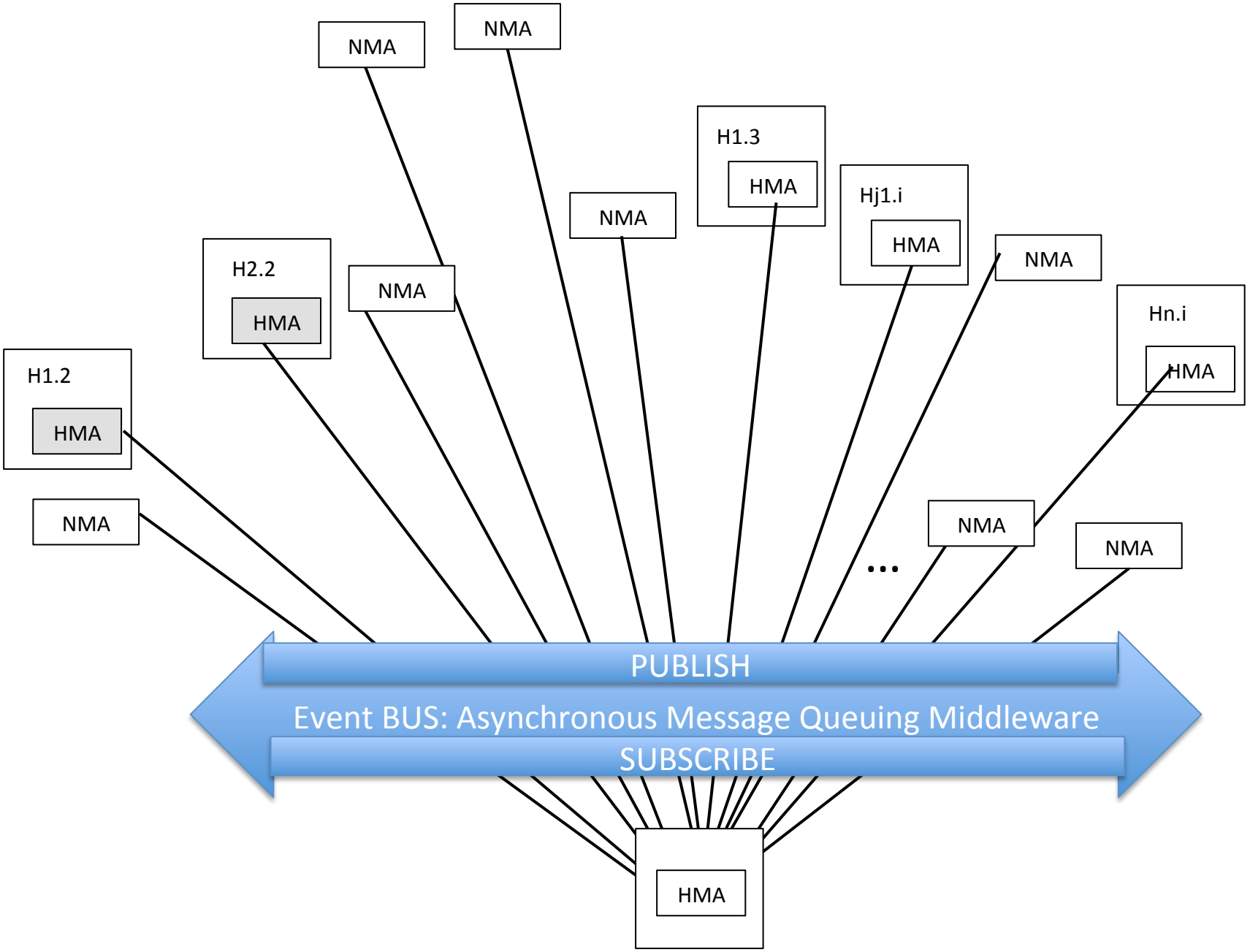


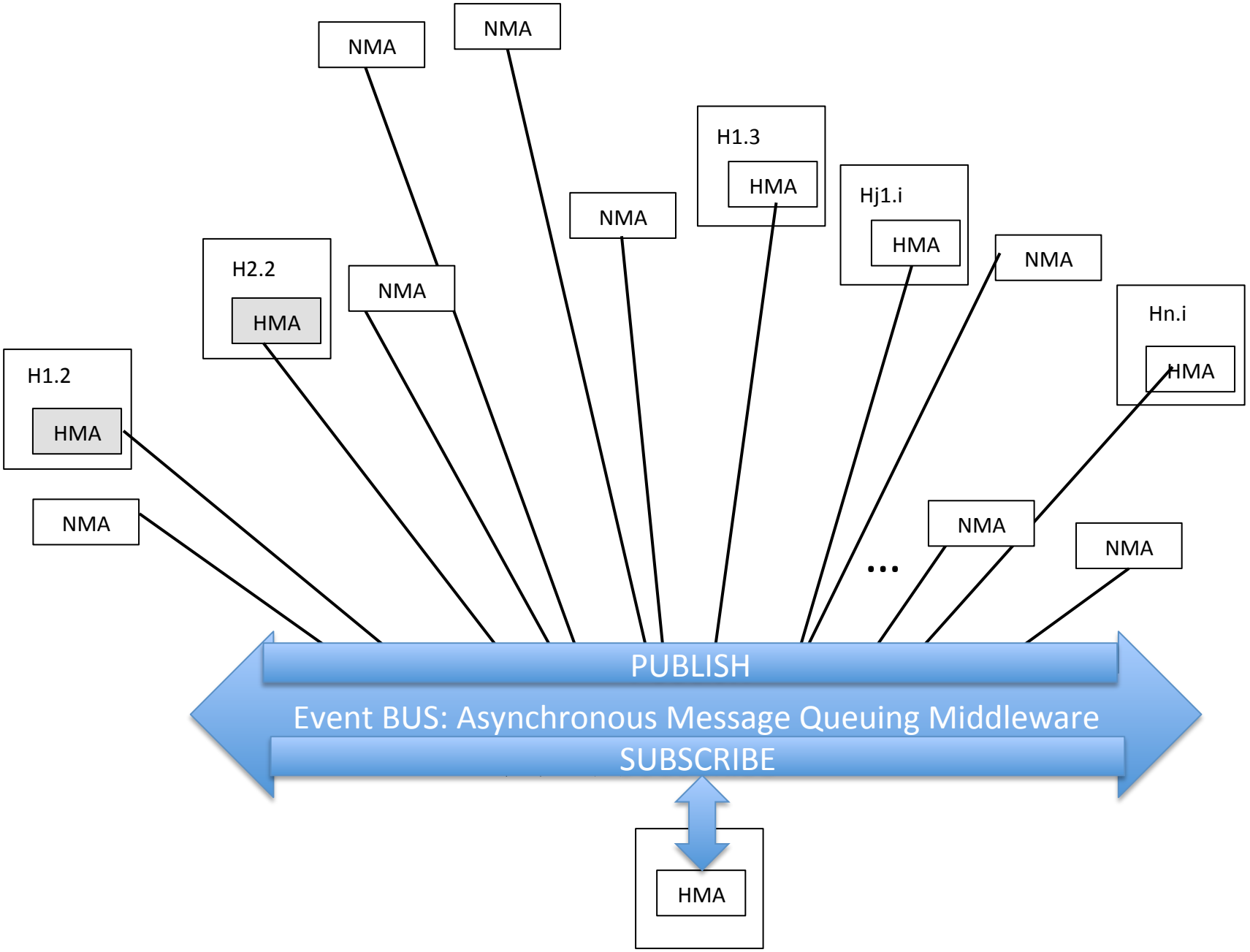
Instantiation of the Generic Internetworking Infrastructure (as introduced in Chap. 1) S2

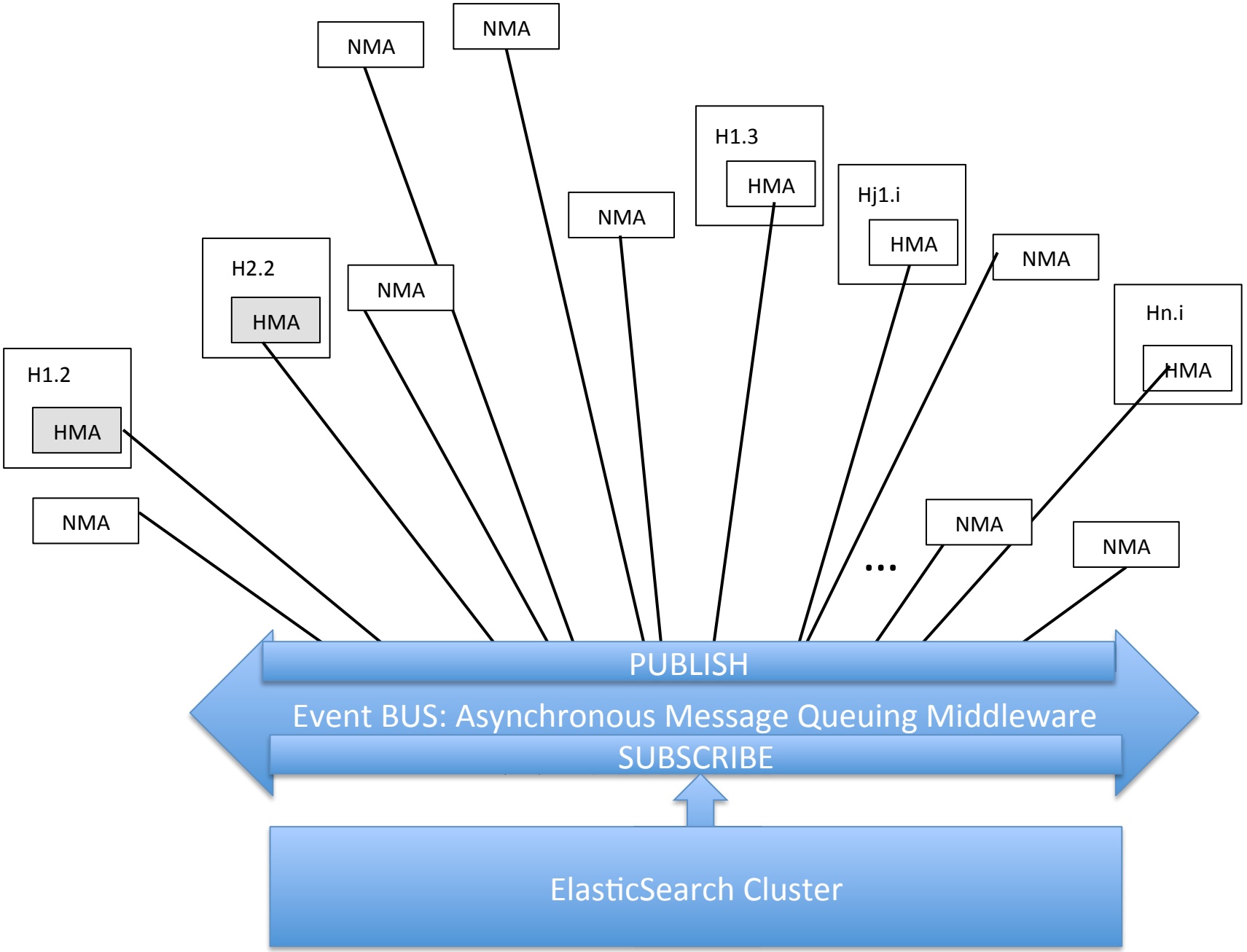



NMA
NMA
NMA
H1.3
HMA
Hj1.i
HMA
NMA
H2.2
HMA
NMA
Hn.i
HMA
H1.2
HMA
NMA
NMA
NMA
...
NMA
H1.n
HMA
NMA
NMA
NMA
NMA
Hi.n
HMA
NMA
HMA


NMA
NMA
NMA
H1.3
HMA
Hj1.i
HMA
NMA
H2.2
HMA
NMA
Hn.i
HMA
H1.2
HMA
NMA
NMA
NMA
H1.n
HMA
NMA
NMA
NMA
NMA
Hi.n
HMA
HMA


NMA
NMA
H1.3
HMA
Hj1.i
HMA
NMA
H2.2
HMA
NMA
NMA
Hn.i
HMA
H1.2
HMA
NMA
NMA
NMA
...
PUBLISH
Event BUS: Asynchronous Message Queuing Middleware
SUBSCRIBE
HMA


NMA
NMA
NMA
H1.3
HMA
Hj1.i
HMA
NMA
H2.2
HMA
NMA
Hn.i
HMA
H1.2
HMA
NMA
NMA
NMA
...
PUBLISH
Event BUS: Asynchronous Message Queuing Middleware
SUBSCRIBE
HMA


NMA
NMA
NMA
H1.3
HMA
Hj1.i
HMA
NMA
H2.2
HMA
NMA
Hn.i
HMA
H1.2
HMA
NMA
NMA
NMA
...
PUBLISH
Event BUS: Asynchronous Message Queuing Middleware
SUBSCRIBE
ElasticSearch Cluster

DHIDS Probing Environment

Pervasive Intrusion Event-Detectors using:

- Specific Probes
- Leveraged Probes (using Event-Capturing and Filtering Management), leveraged by corresponding components in existent solutions
- Providing, Heterogeneity and Diversity in a Scalable Pervasive Probing Environment
- Probes as “appliances” built on top of dedicated HW/SW Appliances
    - In the case we use Raspberry PI and ODROID nodes in the implementation

IDS	Data Source	Detection Method	Cooperation /Extensibility	Detection Time	Reaction
Snort	Network (NIDS)	Rule/Signature based	Prepared for the addition of Plug-ins	Real-time	Passive alert
Suricata	Network (NIDS)	Rule/Signature based	Prepared for the addition of Plug-ins	Real-time	Passive alert
OSSEC	Host (HIDS)	Rule/Signature based	Agent-Manager archit. / not extendible	Real-time	Passive alert / Active response
AIDE	Host (HIDS)	Rule/Signature based	Insufficient documentation	Delayed Detection	Produces an integrity report

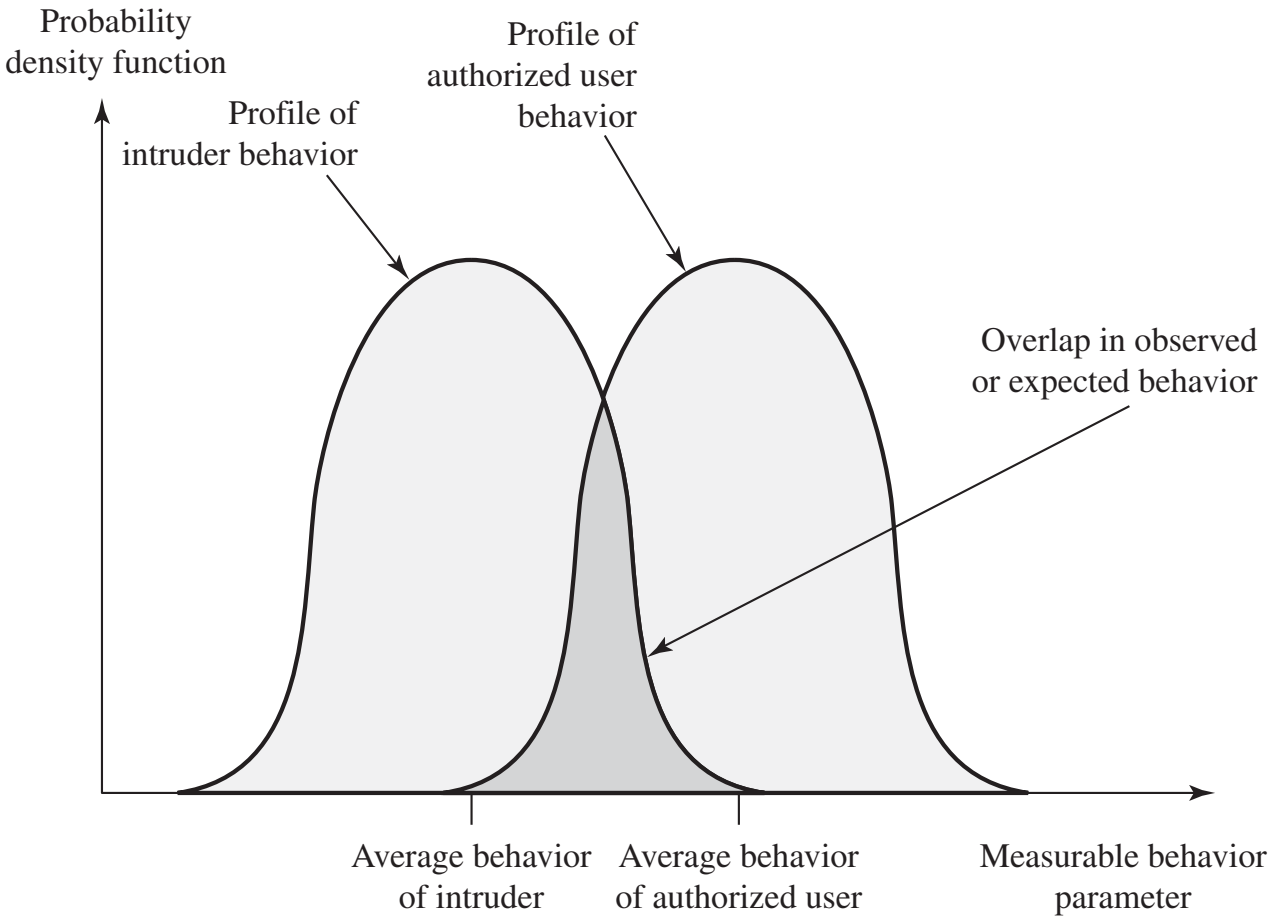
Intrusion Detection Systems: IDS types

- **HIDS (Host-based Intrusion Detection Systems)**
  - Monitors a single host (events occurring within a single host)
- **NIDS (Network Intrusion Detection Systems)**
  - Monitors network traffic for specific network segments or from/to devices
  - Can be focused on a single protocol (specific stack layer), as well as, correlated events from different protocol layers, to identify suspicious activity
- **Distributed or Hybrid IDS**
  - Combines events from different probes (HIDS-based sensors and NIDS-based sensors), typically in a centralized component (central analyzer), that is able to better identify and respond to intrusion activity
  - Central analyzers, usually managed in the context of SOCs (Security Operation Centers), ex., in the context of SIEM (Security and Intrusion Event Management) monitoring and analytics platforms

IDS approach principle

- Base assumption: the behavior of an intruder (intrusion effects) differs from the behavior of the legitimate user (legitimate effects)
- Is the assumption expected in the “real life” ?
  - We must expect overlaps !
  - Consequences ?
  - => IDS false positives (or false alarms)
    - If correct users are identified as intruders
  - => IDS false negatives
    - Intruders not detected as intruders
    - increase if we consider a very “tight” interpretation of the intrusion behavior

Behavior Profiles in a IDS



BRF - Base Rate Falacy

- To be of practical use:
  - An IDS should detect a substantial percentage of intrusions – if not the system will provide a false sense of security
  - … while keeping the false positive rate low
    - if not, system managers will begin to ignore the detected events (considering that they are false alarms, or much time will be wasted analyzing false alarms
- Base Rate Fallacy: if actual numbers of intrusions is low compared with legitimate uses, false positives are high… unless the test is extremely discriminating

IDS properties

- Run continuously, no human supervision
- Fault-Tolerant / Intrusion Tolerant , able to recover from failures and intrusions
  - Crash or Byzantine failures (or attacks)
- Subversion-tolerance: able to monitor itself and detect self-failures, attacks against itself
- Impose minimal overhead on systems where it is running
- Configuration security policies (enforcements) of monitored systems
- Able to dynamic adaptations (user behavior, changes in monitored systems, changes in operational environments, etc)
- Ready to address scale conditions
- Graceful degradation when some of its specific components stop working
- Allow dynamic reconfigurations, without stopping the ID operation (always available)

Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

IDS analysis approach

- Two base approaches
  - Anomaly Detection approach
    - Start from the collection of data characteristic from a correct behavior (correct users/correct usage) over an observation in a period of time
    - During the learning phase, the system is strongly monitored or restricted in its operation, to improve the confidence on the "correct behavior"
  - Signature-Based (or Heuristic-Based) approach (or misused detection approach)
    - Start by setting (explicitly) what is an incorrect behavior (or malicious patterns (formally known as "signatures") or attack rules ("heuristics")
    - Approach only detects attacks already "well-known"

Anomaly Detection

- Aim to define normal, correct or expected behavior
- Preferred approach: allows to address "unknown" or "zero day" attacks
  - But the "learning" or "training" phase can be problematic
  - Can induce a lot of "false positives": ex., in heterogeneous operation environments
  - Solution: learning in different moments and evolve continuously the model of legitimate operation behavior

Anomaly Detection Techniques

- Statistical
  - Based in the analysis of observed behavior using univariate, multivariate or time-series models of observed metrics
- Knowledge-base
  - Use of an expert-system to classify the observed behavior according to a set of modelling rules describing the correct behavior
- Machine-learning
  - Automatic determination of a suitable classification model from the training data, using data-mining techniques
  - Good for flexibility, adaptability, and dynamic ability to capture interdependencies between observed metrics
  - Disadvantages:
    - A "wrong" base model for the correct behavior implies on high false positives: approach only considers "known-correct behavior".
    - Complexity, high-resource requirements and processing cost

Anomaly Detection with a Machine Learning Approach

- Can use a variety of specific techniques
  - **Bayesian Networks**: graphs encoding probabilistic relationships among observed metrics
  - **Markov models**: a model based on sets of states, some of them hidden, interconnected by transition probabilities
  - **Neural networks**: base on human-brain operation with neurons and synapses between neurons, that classify observed data
  - **Fuzzy Logic**: usage of fuzzy sets where reasoning is approximate and can accommodate degrees of uncertainty
  - **Clustering and outlier detection**: observed data are grouped according to similarity functions (distance functions), subsequent data are grouped belonging to other groups (when valid) or outliers (when not valid)
  - **Genetic algorithms**: algorithms implementing simulation of evolutionary biology (computing inheritance, mutations, selection, recombination), to build classification rules

Signature-Based Approach

- Explicit descriptions (configuration rules) mixing what is right (normal, correct behavior) and what is wrong (incorrect, malicious behavior)
  - Large-collections of well-known patterns of malicious data (in the network traffic, or against data-stored on a system)
  - Large means large enough to minimize false positives
  - The same approach is taken in anti-virus software network traffic shapers/scanners, or NIDS
  - **Advantages**: low cost in time ans resources used – fast detection, wide-practical acceptance
  - **Drawbacks**: effort in the permanent identification of new signatures (ex., new malware patterns), inability to be used for zero-day attacks – resulting from previously undisclosured vulnerabilities (for which no signatures exist yet when the correspondent flaw becomes known)

Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

HIDS
Host Based Intrusion Detection Systems

- Data sources and sensing information:
  - **System call traces** (Interceptors on Unix/Limux System Calls, … more difficult with Windows DLLs)
  - **Audit log file records**
    - Using the available information … problem when attackers modify/ delete records
    - Idea: events sent immediately to remote secure loggers
  - **File integrity checksums**
    - Tested against initial integrity references, on non-volatile read only memory, cdroms, or read-only disk partitions, …. or in HW TPMs (see more about this later in the course)
  - **Windows registry access**
    - Many information… but "windows specific"
- Events passed to a local IDS analyzer, or to a remote IDS analyzer

Anomalous-Detection based HIDS

- Ex., in Ubuntu Linux Distributions: system call traces can be easily gathered by the BSM audit module, with relevant information about process-activities that can be classified as correct or incorrect, by a decision engine
- See Creech 2013, Developing a High Accuracy Cross Platform Host-based IDS capable of Reliably Detecting Zero Day Attacks, PhD thesis, Univ of New South Wales, 2013
  - Intrusion detection rates in the interval 95 to 99 % effectiveness, on the experimental observation of such approach
  - Effectiveness of previous approiaches using audit log records: ~80%

Windows DLLs for IDS Monitoring

- See bibliography
  - Reference Linux System Calls
  - Windows DLLs

HIDS File integrity checksums

- Another relevant source of probing information
- Secure cryptographic hashes of:
  - Program binaries
  - Scripts
  - Critical configuration files
  - …
- Ex., use by the Tripwire system
- Also base approach to verifications "at boot time and load-time" (or TPM approaches)
- but … how can we detect changes made to processes once they are running on the system…

Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

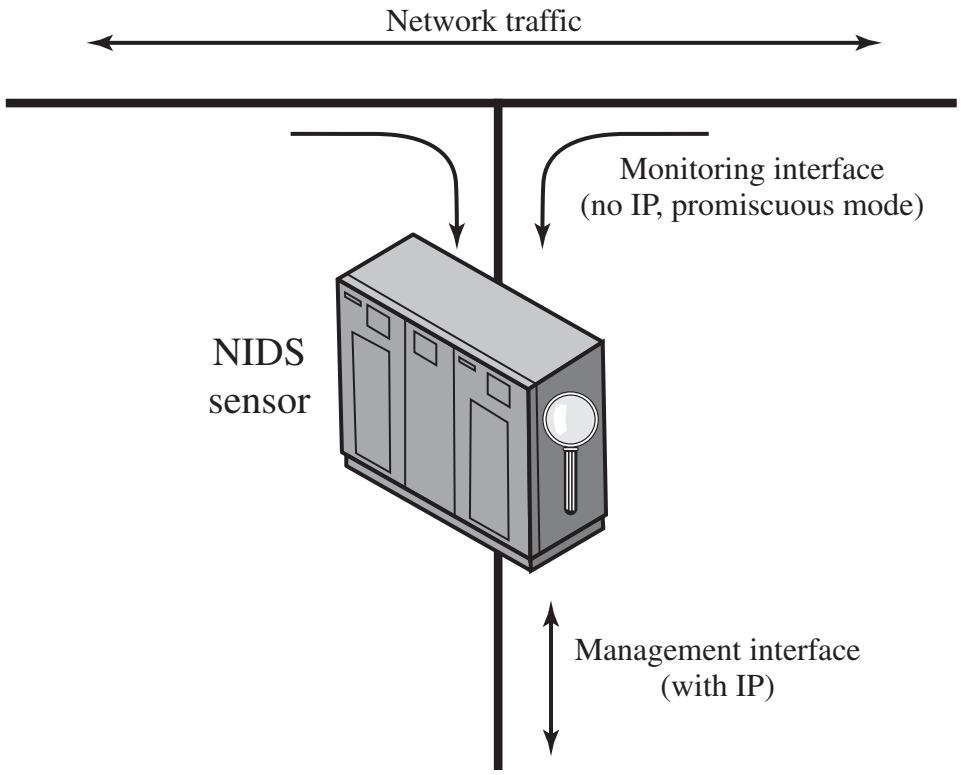
NIDS
Network Intrusion Detection Systems

- Monitors network traffic at selected points of the network or interconnected networks
- A NIDS Captures, examines, filters, packet by packet (in real time), focusing on a specific layer, or the layers of protocol stack (ex., TCP/IP stack) to attempt to detect intrusion patterns
- Location of NIDS: in the perimeter defense
- Can be incorporated as a component in a Firewall (FW) system, implemented by a dedicated HS/SW appliance associated with the FW or a SW appliance running in a computer
- Analysis of traffic patterns and packet-content (payloads), to identify malicious patterns
- Only part of the IDS solution
  - Limited: problem today with the increasing use of cryptography
- A NIDS solution can include different sensors, one or more servers for management purposes and one or or more management consoles for operation

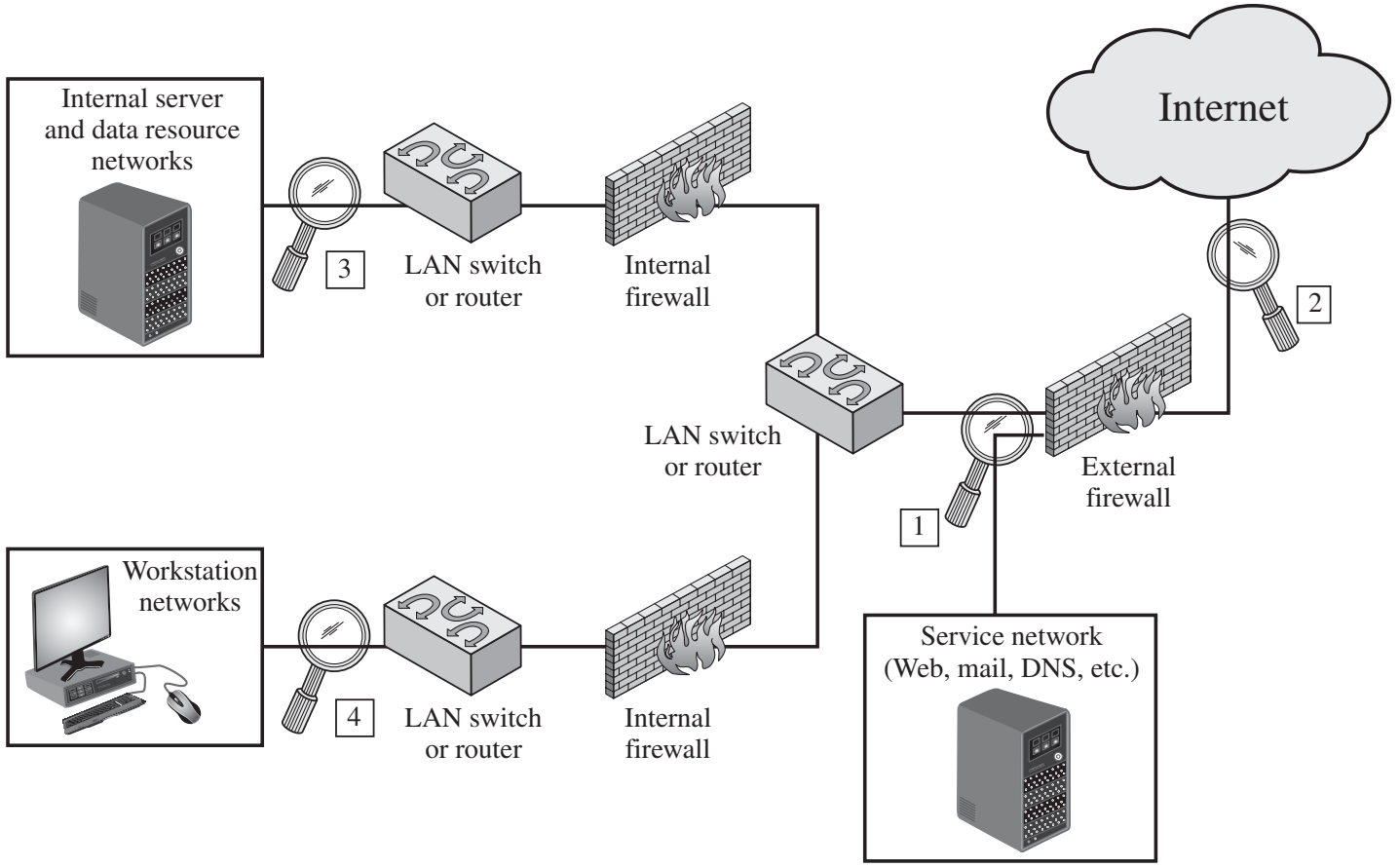
NIDS sensors

- In-Line sensors: when the NIDS materializes a component inserted in a network segment, so that the traffic pass though the sensor
  - Ex., a case of NIDS running in a NAT BOX, in a router, in a gateway or in a firewall
  - Ex., a case of NIDS running as a component of an AP (access point) in a wireless network
  - In this case, such a solution can combine intrusion detection and intrusion prevention functions, blocking an attack as a result of the attack detection
- Passive sensors
  - Use as a packet sniffer, capturing traffic in “promiscuous” mode
  - More efficient that in-line sensors, avoidance of additional packet-delays in a end-to-end perspective

Passive NIDS



Deployment of NIDS



NIDS – Detection Techniques

- Signature detection based:
  - **Application layer reconnaissance**
    - Detection of attack patterns that have been identified as targeting application protocols, namely: DHCP, DNS, finger, FTP HTTP, IMAO, IRC, NFS, POP, IMAP, rlogin/rsh, RPCs, SIP, SMB, SMTP, SNMP, TELNET, TFTP., RFC, …
    - Can also look to more specific detection (ex., Traffic Injecton, ex., SQL injection patterns, XSS Bahavior,
  - **Transport layer reconnaissance (TCP and UDP analysis)**
    - Detection of scans for vulnerable ports, unusual packet fragmentation, detection of SYN floods from DoS attacks
  - **Network layer reconnaissance**
    - IPV4, IPV6, ICMP, IGMP packet analysis. Ex., detection of Spoofed IP addresses or illegal IP header values
  - **Unexpected application detection**
    - If the activity on a transport connection is consistent with expected application protocols
    - Ex., traffic showing that a certain host is running an unauthorized application service
  - **Policy violations**
    - Identification of use of not allowed Web Sites or use of forbidden application protocols

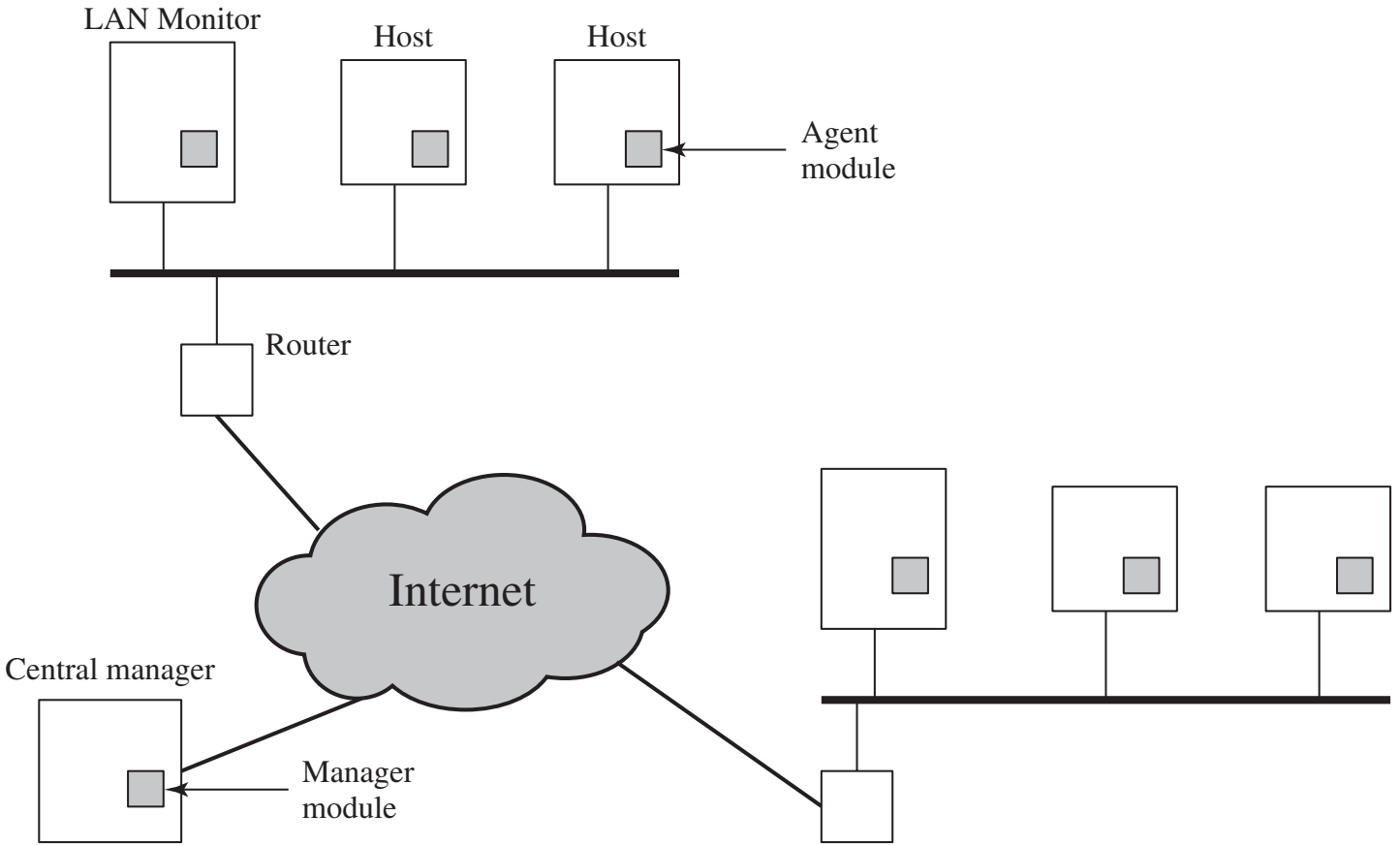
Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

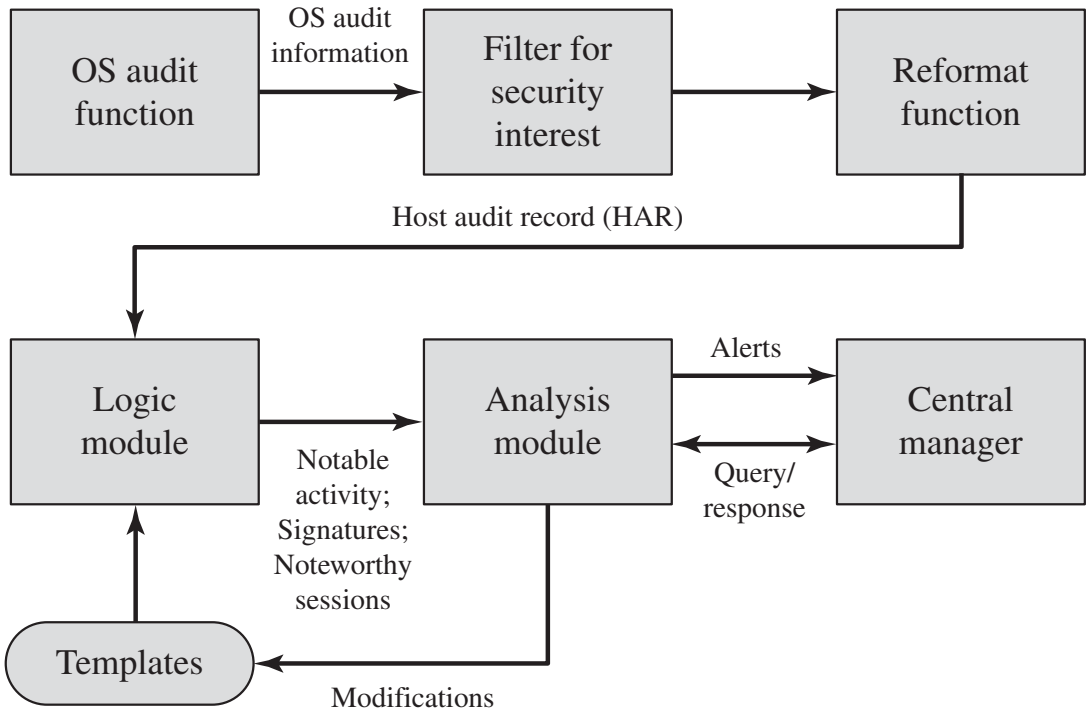
Distributed Host Intrusion Detection

- Solution to avoid a management environment with single-systems, stand-alone-operation
- More effective defense
  - Coordination and cooperation among IDS components, distributed across a large-network (ex., large-scale organization)
- Can combine different HIDS probes, possibly using diversity of technology, monitoring specific heterogeneous hosts
- Events are locally detected, filtered (possible pre-processing) and transmitted to a remote analyzer (management system), with APIs operated in a SOC by specialized personnel
  - The same idea of the SIEM Platforms

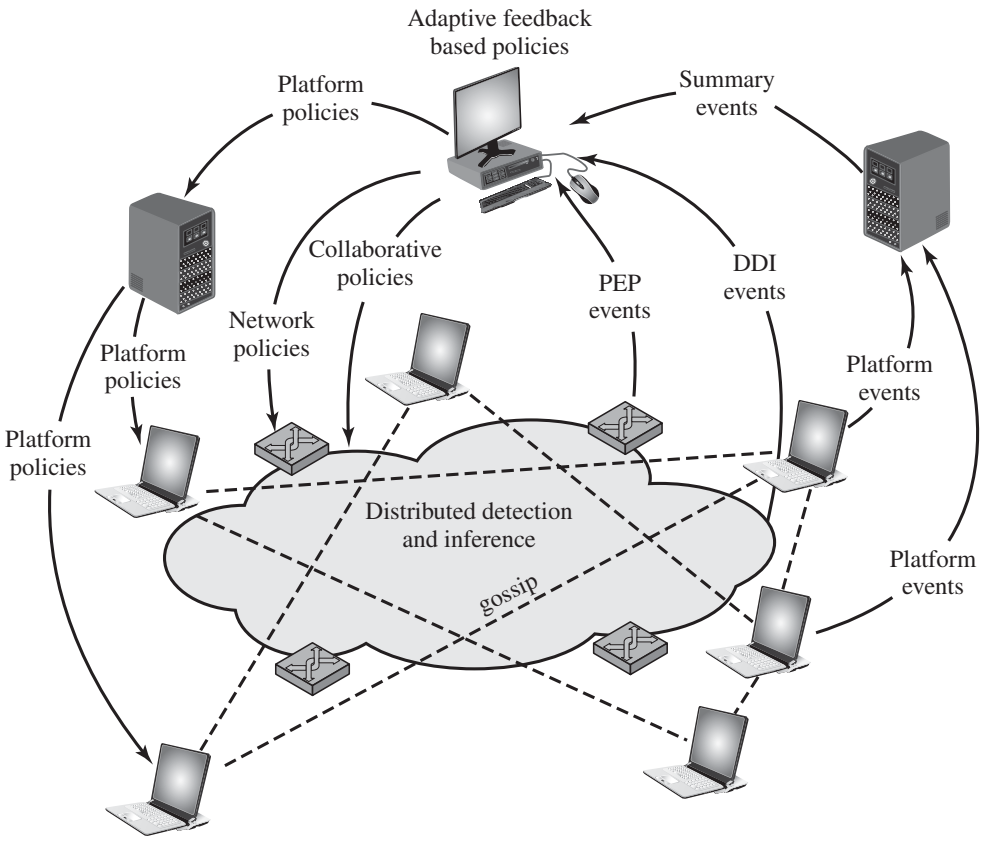
Distributed Host Intrusion Detection Architecture



Agent Modules



Distributed Adaptive Intrusion detection

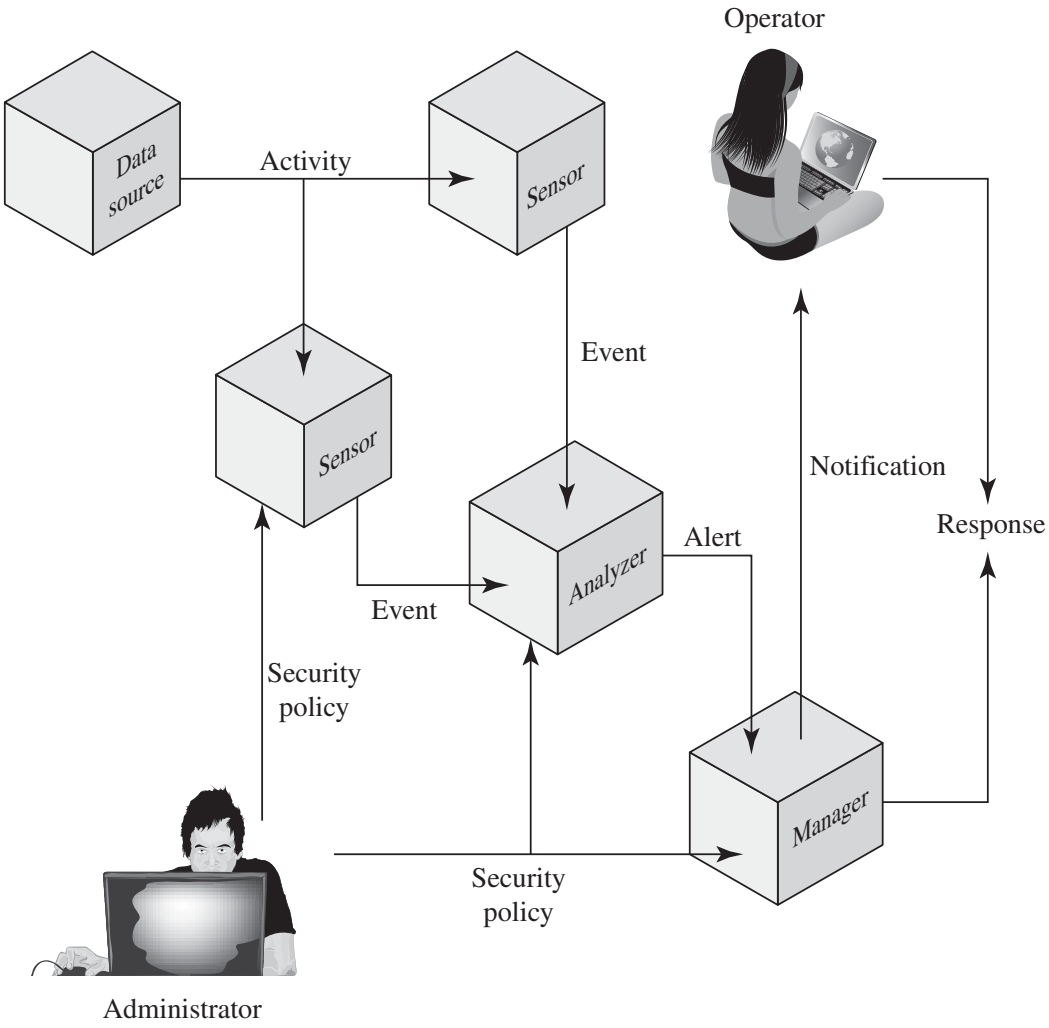


PEP = policy enforcement point
DDI = distributed detection and inference

Outline

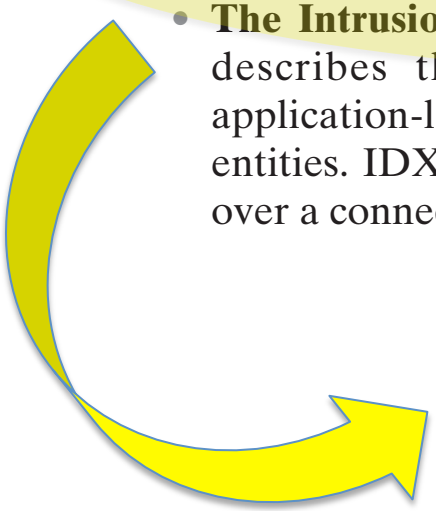
- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

Intrusion detection exchange formats



Intrusion detection exchange formats

- **Intrusion Detection Message Exchange Requirements (RFC 4766):** This document defines requirements for the Intrusion Detection Message Exchange Format (IDMEF). The document also specifies requirements for a communication protocol for communicating IDMEF.
- **The Intrusion Detection Message Exchange Format (RFC 4765):** This document describes a data model to represent information exported by intrusion detection systems and explains the rationale for using this model. An implementation of the data model in the Extensible Markup Language (XML) is presented, an XML Document Type Definition is developed, and examples are provided.
- **The Intrusion Detection Exchange Protocol (RFC 4767):** This document describes the Intrusion Detection Exchange Protocol (IDXP), an application-level protocol for exchanging data between intrusion detection entities. IDXP supports mutual-authentication, integrity, and confidentiality over a connection-oriented protocol.



Materialization in DHIDS:
Implemented as a JSON-based representation in the DHIDS Platform, JSON events aggregated and Correlated in a ELK Cluster Environment
Searched by “Attack-Signatures” expressed by a domain Specific query-language (DHIDS-QL)

Outline

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

Honeypots

- A relatively recent approach in intrusion detection technology.
- Honeypots are decoy systems, designed to lure a potential attacker away from critical systems.
- Honeypots are designed to:
  - Divert an attacker from accessing critical systems.
  - Collect information about the attacker's activity.
  - Encourage the attacker to stay on the system long enough for administrators to respond.

Honeypot development environment

- See more in the bibliography (Stallings)
  - Honeypots and Honeynets
  - Interesting research direction: Cooperative Honeynets in Large-Scale Internet Environments

- Ex., in DHIDS we use Honeypots in two different ways:
  - Complete replciated “in production” systems with “fake data”, reporting complete interactions with potential adversaries
  - Simple “diversion” Apps , just to notify that they were touched (reporting these touches as anomalous behaviors)

Outline in this lesson

- Intruders and Intrusion Attacks
- Intruder behavior
- Intrusion detection systems (IDS)
- Intrusion detection analysis approaches
- HIDS
- NIDS
- Intrusion Detection Techniques and Distributed Hybrid Intrusion Detection
- IDS and event exchange formats
- Honeypots and Honeynets

Suggested Readings

- See the suggested readings in the presentation
- W. Stallings, L. Brown, Computer Security – Principles and Practice
- Chap 8 – Intrusion Detection
  - See in the CLIP provided documentation

- For evaluation: see the questions in the end of the chapter