Module-4 Topics to be discussed:

Intrusion Detection and Prevention:

Intrusion, types of IDS,

Intrusion detection and prevention techniques,

Network-based Intrusion Detection Systems

Host-Based Intrusion Prevention Systems.

Physical Theft, Abuse of Privileges, Malware Infection.

Introduction

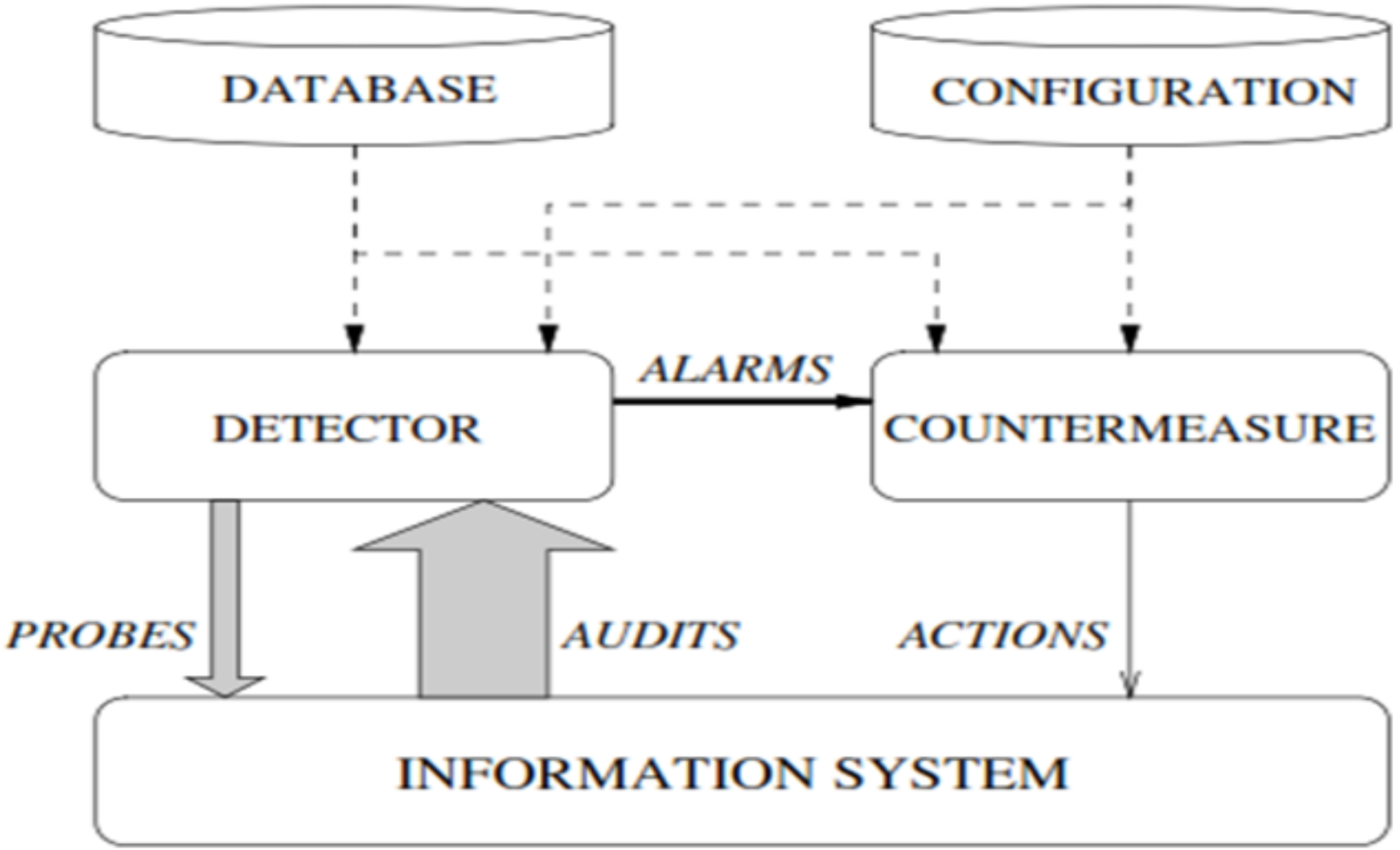
- An Intrusion Detection system (IDS)
  - Detects attacks as soon as possible and takes appropriate action.
  - Does not usually take preventive measures when an attack is detected.
  - It is a reactive rather than a pro-active agent.
  - It plays a role of informant rather than a police officer.

Introduction

- Eugene Spafford reports:
  - Information theft is up over 250% in the last 5 years.
  - 99% of all major companies report at least one major incident.
  - Telecom and computer fraud totaled $10 billion in the US alone.

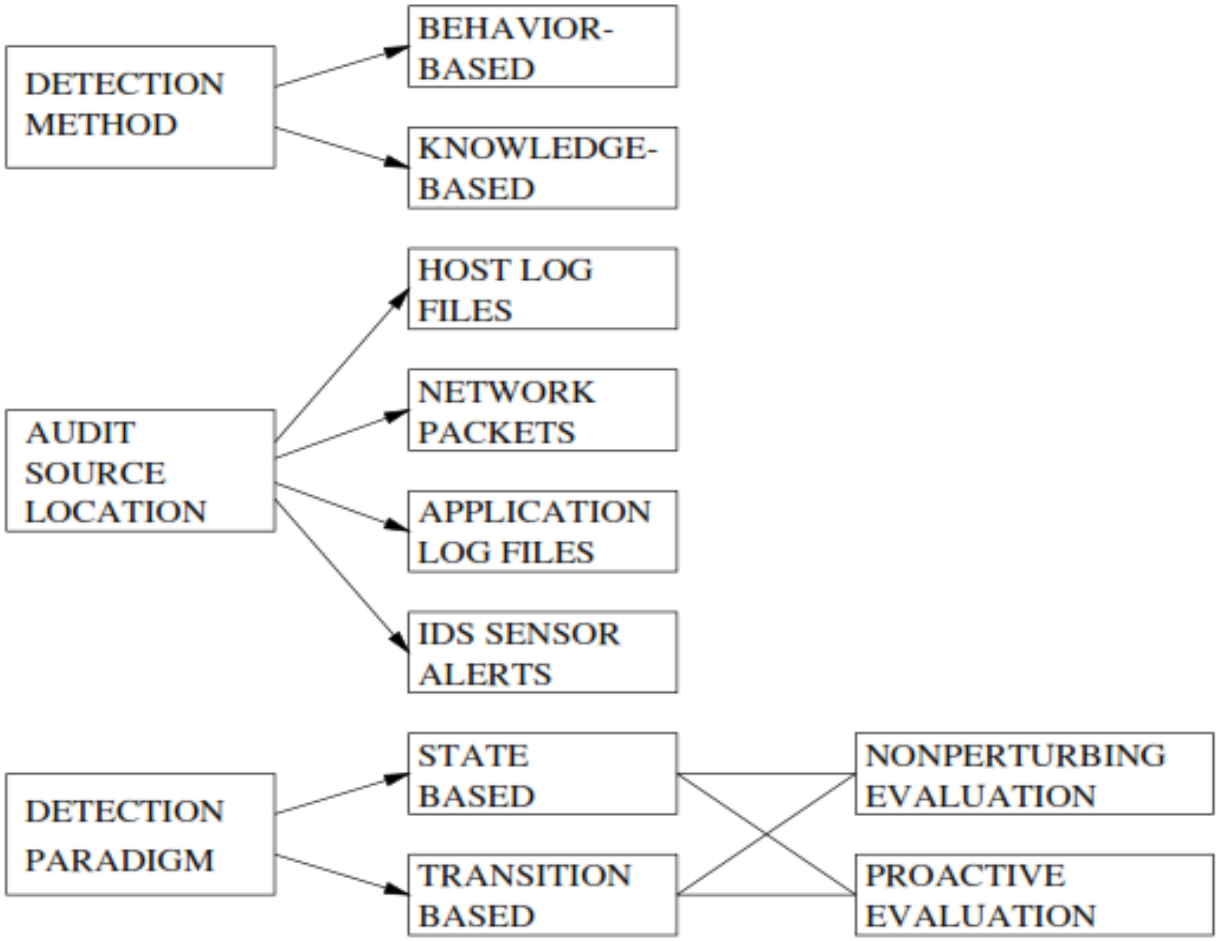
Since it seems obvious that we cannot prevent subversion, we should at least try to detect it and prevent similar attacks in future.

Very simple intrusion-detection system



Source: *H. Debar, An Introduction to Intrusion-Detection System, IBM Research, Zurich Research Lab*

Taxonomy



Source: *H. Debar, An Introduction to Intrusion-Detection System, IBM Research, Zurich Research Lab*

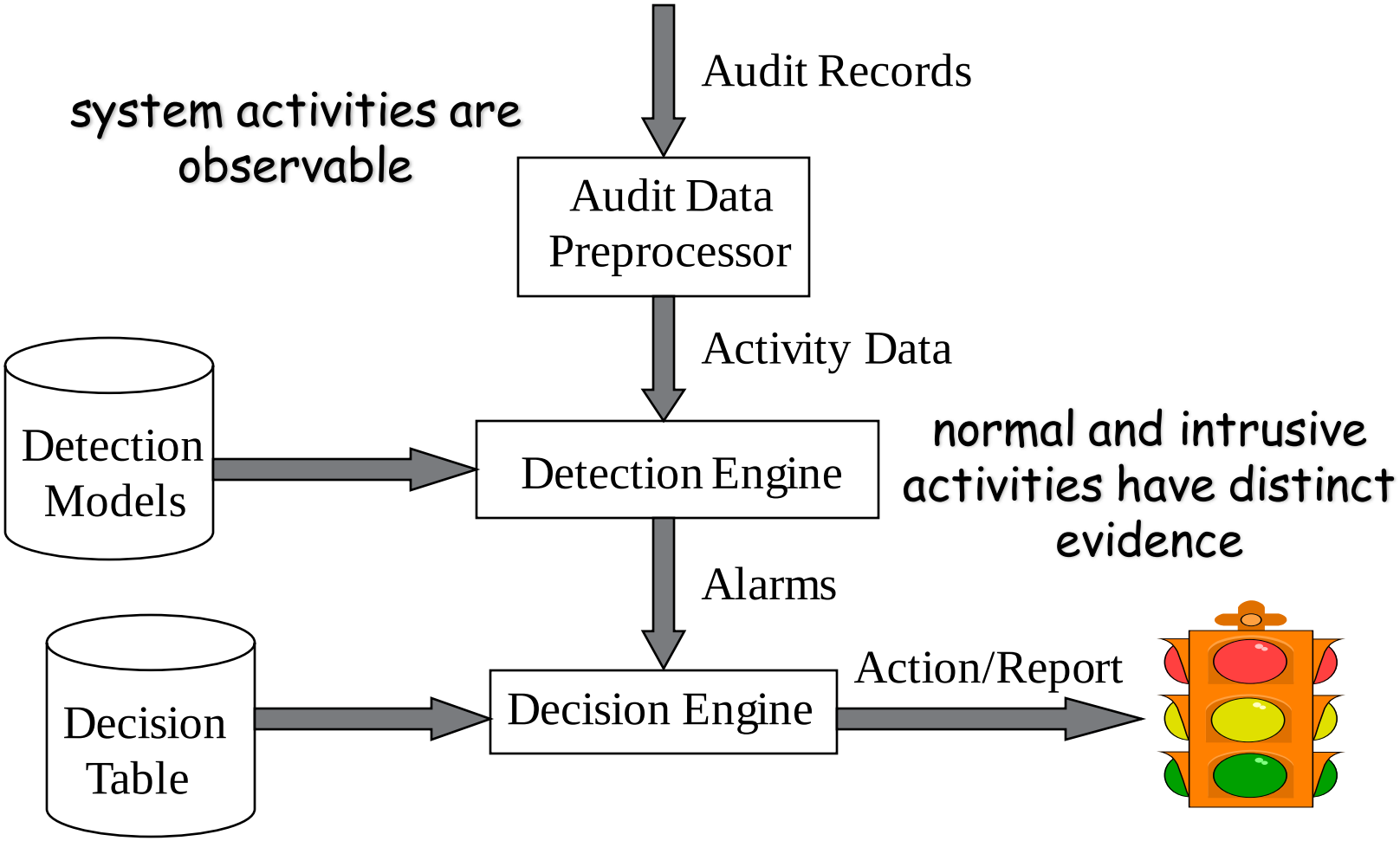
Objectives

- Understand the concept of IDS/IPS and the two major categorizations:
  - based on either signature information or
  - anomaly that generate false detections.
- Discussion on proposed hybrid IDS
- Be able to write a snort rule when given the signature and other configuration info

Elements of Intrusion Detection

- Primary assumptions:
  - System activities are observable
  - Normal and intrusive activities have distinct evidence
- Components of intrusion detection systems:
  - From an algorithmic perspective:
    - Features - capture intrusion evidences
    - Models - piece evidences together
  - From a system architecture perspective:
    - Various components: audit data processor, knowledge base, decision engine, alarm generation and responses

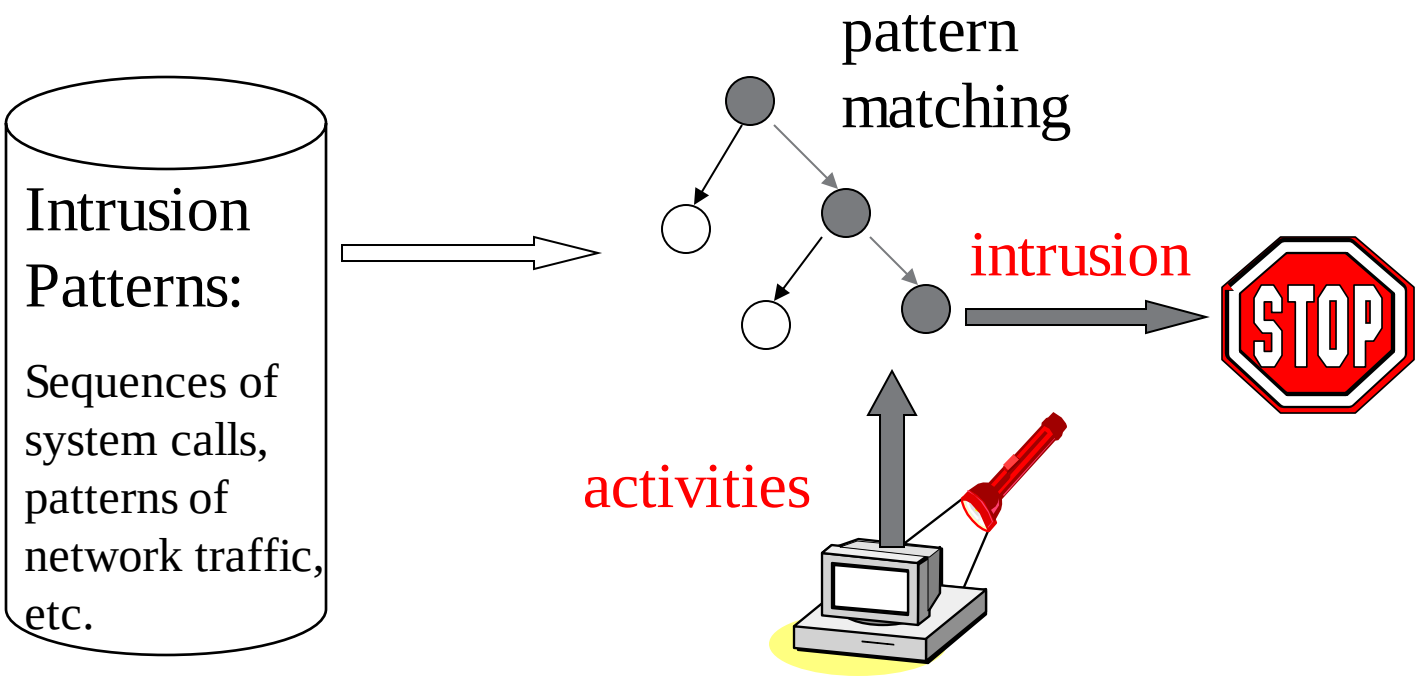
Components of Intrusion Detection System



Intrusion Detection Approaches

- Modeling
  - Features: evidences extracted from audit data
  - Analysis approach: piecing the evidences together
    - Misuse detection (signature-based)
    - Anomaly detection (statistical-based)
- Deployment: Network-based or Host-based
  - Network based: monitor network traffic
  - Host based: monitor computer processes

Misuse Detection

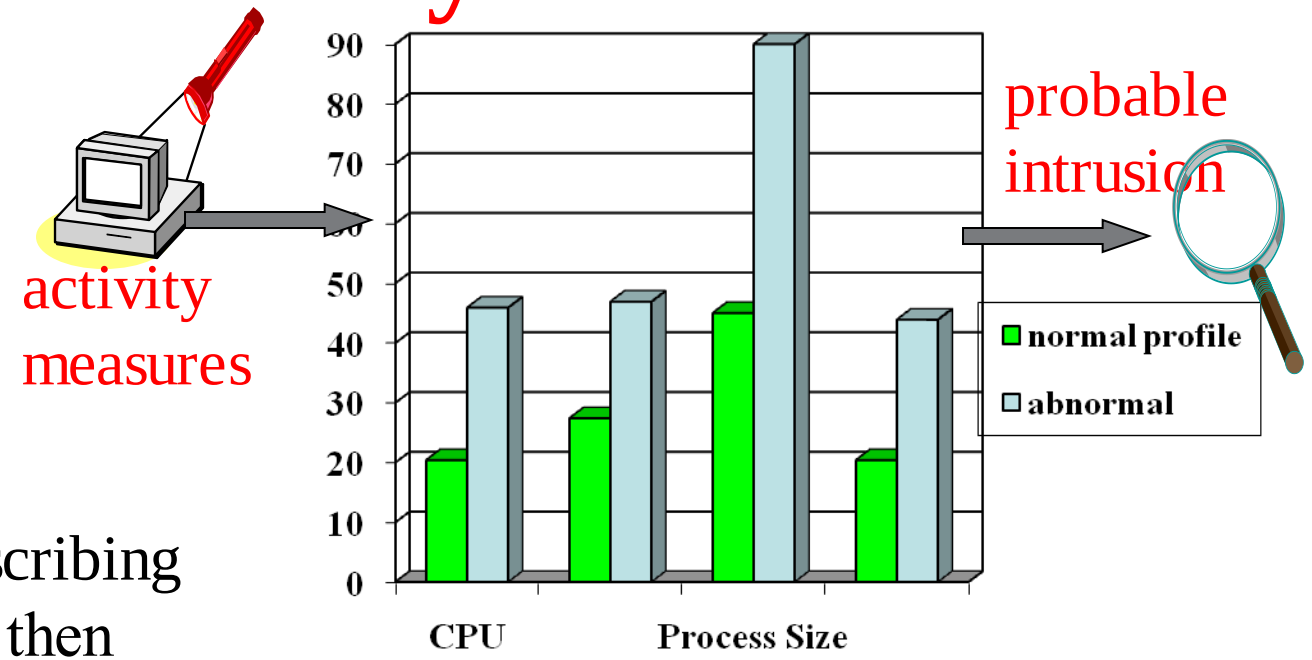


Example: ***if*** (traffic contains "x90+deZ^\r\n]{30}") ***then*** "attack detected"

Advantage: Mostly accurate. But problems?

Can't detect new attacks

Anomaly Detection



Define a profile describing "normal" behavior, then detects deviations. Thus can detect potential new attacks.

Any problem ?

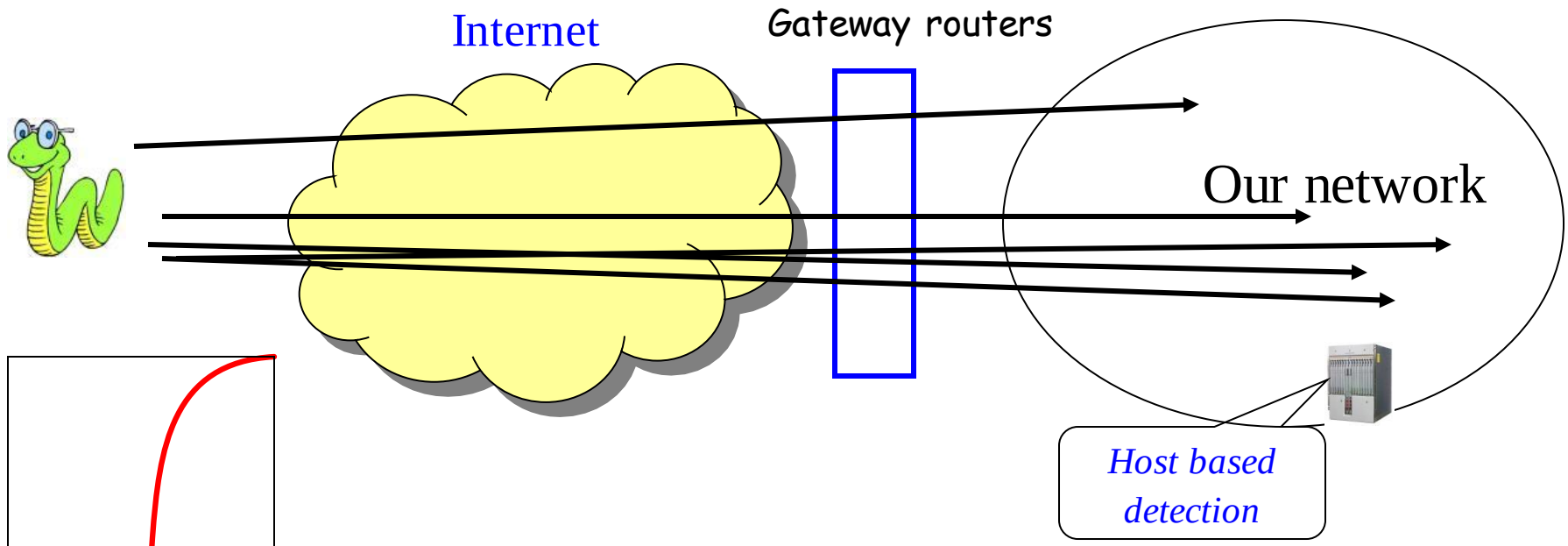
Relatively high false positive rates

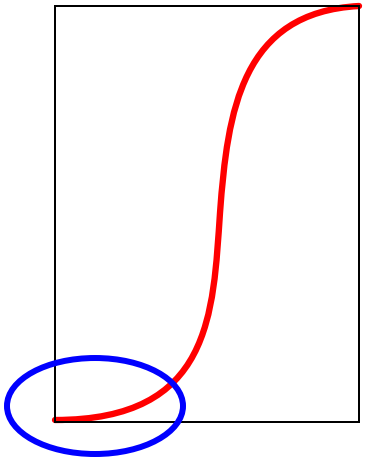
- Anomalies can just be new normal activities.
- Anomalies caused by other element faults
  - E.g., router failure or misconfiguration, P2P misconfig
- Which method will detect DDoS SYN flooding ?

Host-Based IDSs

- Use OS auditing and monitoring/analysis mechanisms to find malware
  - Can execute full static and dynamic analysis of a program
    - Monitor shell commands and system calls executed by user applications and system programs
  - Has the most comprehensive program info for detection, thus accurate
- Problems:
  - If attacker takes over machine, can tamper with IDS binaries and modify audit logs
  - User dependent: install/update IDS on all user machines!
  - Only local view of the attack

Network Based IDSs





- At the early stage of the worm, only limited worm samples.
- Host based sensors can only cover limited IP space, which has scalability issues.
  - Might not be able to detect the worm in its early stage.

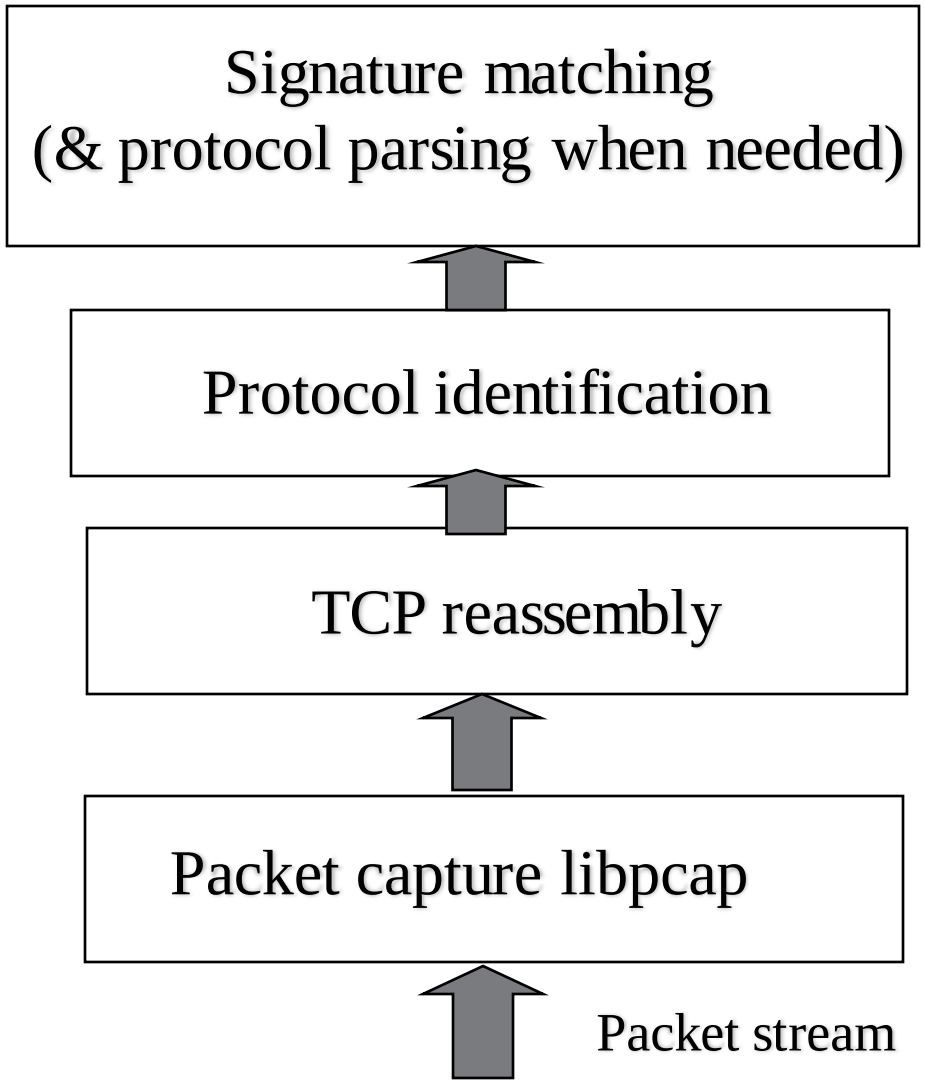
Network IDSs

- Deploying sensors at strategic locations
  - For example, Packet sniffing via *tcpdump* at routers
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
  - Look into the packet payload for malicious code
- Limitations
  - Cannot execute the payload or do any code analysis !
  - Even DPI gives limited application-level semantic information
  - Record and process huge amount of traffic
  - May be easily defeated by encryption, but can be mitigated with encryption only at the gateway/proxy

Key Metrics of IDS/IPS

- Algorithm
  - Alarm: A; Intrusion: I
  - Detection (true alarm) rate: P(A|I)
    - False negative rate P(¬A|I)
  - False alarm (aka, false positive) rate: P(A|¬I)
    - True negative rate P(¬A|¬I)
- Architecture
  - Throughput of NIDS, targeting 10s of Gbps
    - E.g., 32 nsec for 40 byte TCP SYN packet
  - Resilient to attacks

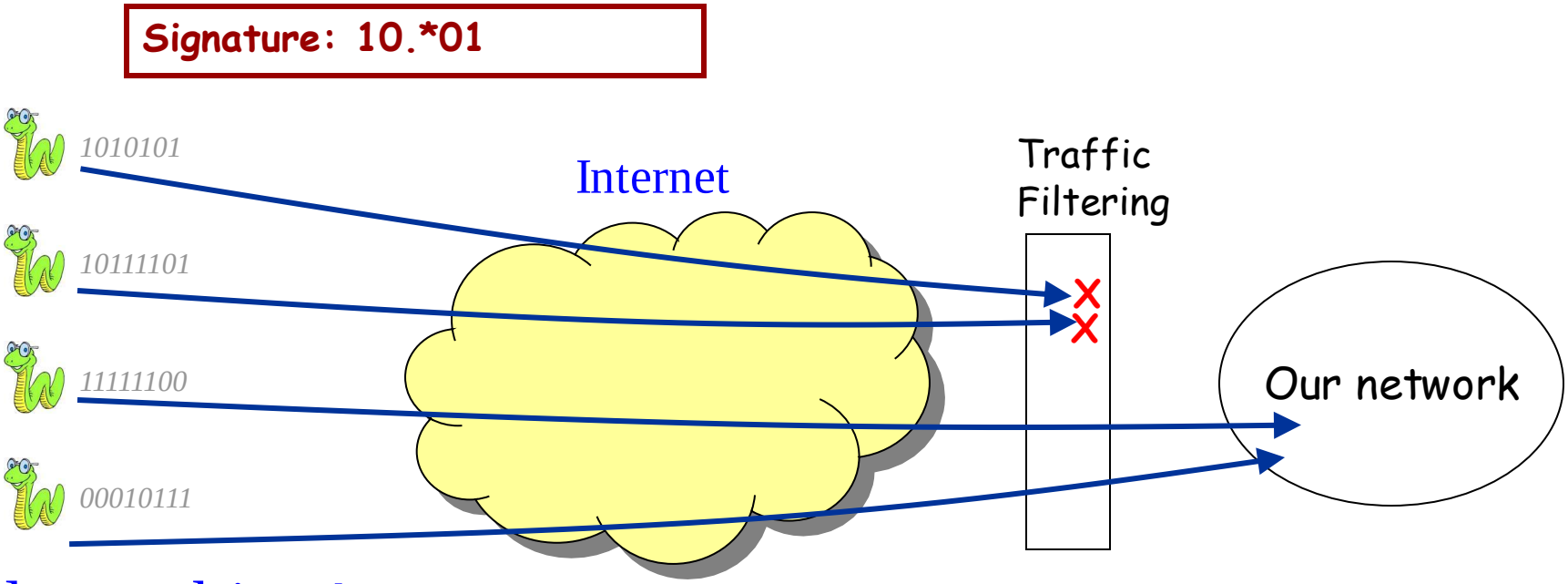
Architecture of Network IDS



Problems with Current IDSs

- Inaccuracy for exploit based signatures
- Cannot recognize unknown anomalies/intrusions
- Cannot provide quality info for forensics or situational-aware analysis
  - Hard to differentiate malicious events with unintentional anomalies
    - Anomalies can be caused by network element faults, e.g., router misconfiguration, link failures, etc., or application (such as P2P) misconfiguration
  - Cannot tell the situational-aware info: attack scope/target/strategy, attacker (botnet) size, etc.

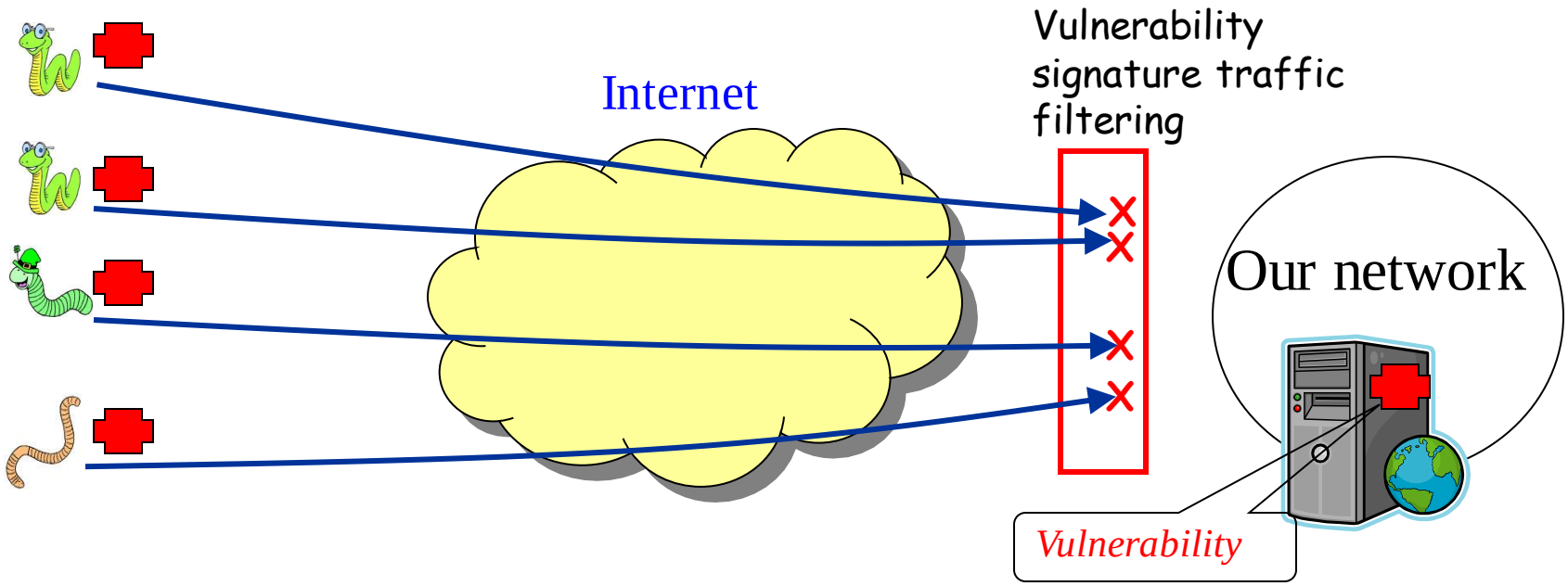
Limitations of Exploit Based Signature



Polymorphism!

Polymorphic worm might not have exact exploit based signature

Vulnerability Signature

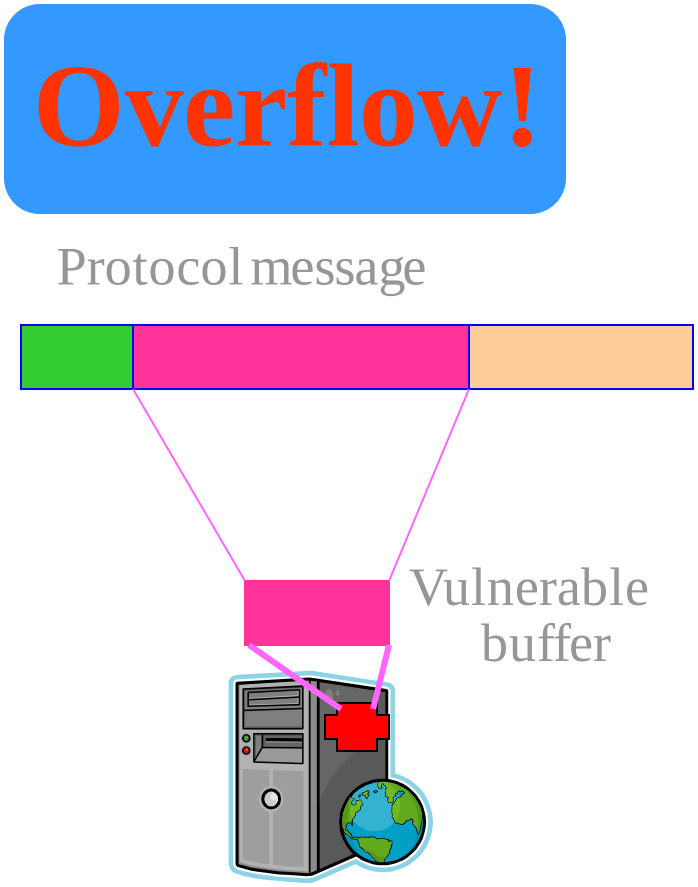


Work for polymorphic worms

Work for all the worms which target the same vulnerability

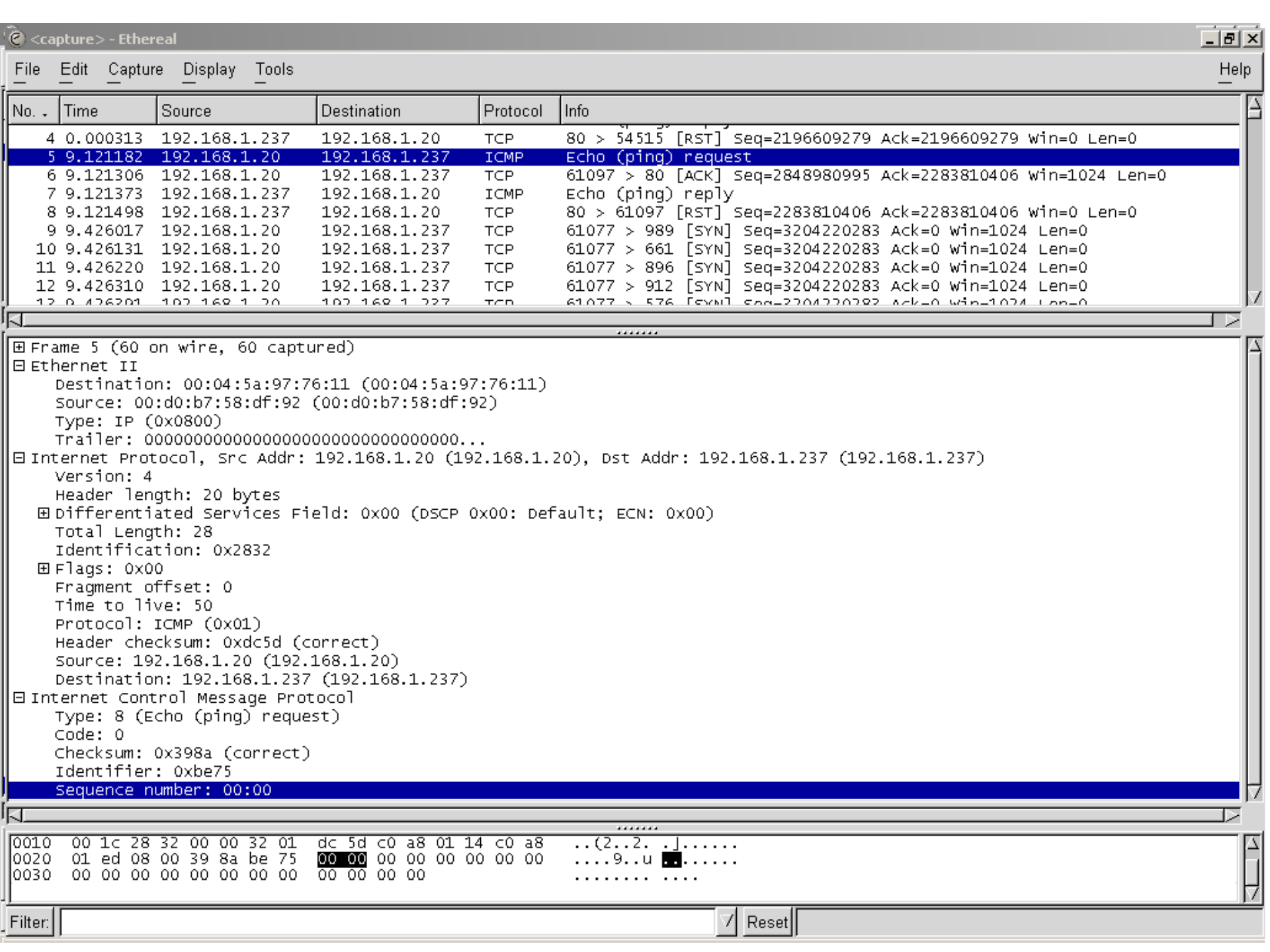
Example of Vulnerability Signatures

- At least 75% vulnerabilities are due to buffer overflow
- Sample vulnerability signature
- Field length corresponding to vulnerable buffer > certain threshold
- Intrinsic to buffer overflow vulnerability and hard to evade



Related Tools for Network IDS (I)

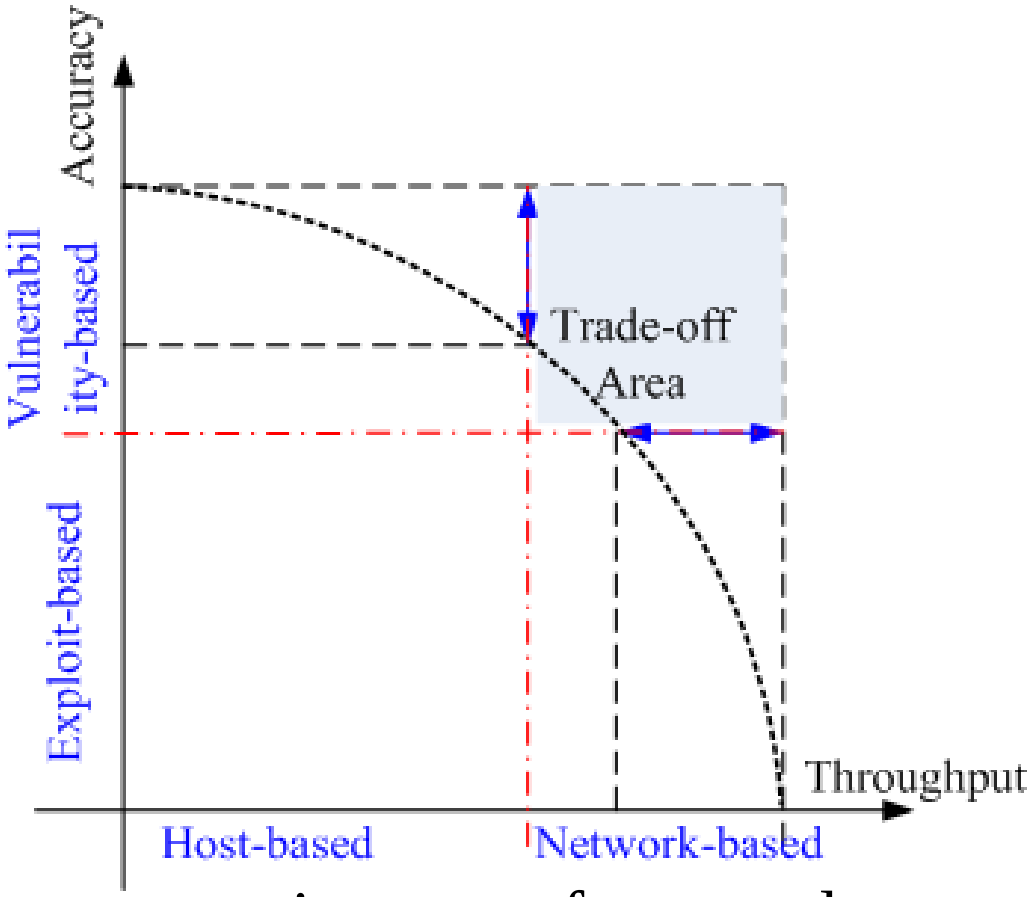
- While not an element of Snort, wireshark (used to called Ethereal) is the best open source GUI-based packet viewer
- www.wireshark.org offers:
  - Support for various OS: windows, Mac OS.
- Included in standard packages of many different versions of Linux and UNIX
- For both wired and wireless networks


<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
4 0.000313 192.168.1.237 192.168.1.20 TCP 80 > 54515 [RST] Seq=2196609279 Ack=2196609279 Win=0 Len=0
5 9.121182 192.168.1.20 192.168.1.237 ICMP Echo (ping) request
6 9.121306 192.168.1.20 192.168.1.237 TCP 61097 > 80 [ACK] Seq=2848980995 Ack=2283810406 Win=1024 Len=0
7 9.121373 192.168.1.237 192.168.1.20 ICMP Echo (ping) reply
8 9.121498 192.168.1.237 192.168.1.20 TCP 80 > 61097 [RST] Seq=2283810406 Ack=2283810406 Win=0 Len=0
9 9.426017 192.168.1.20 192.168.1.237 TCP 61077 > 989 [SYN] Seq=3204220283 Ack=0 Win=1024 Len=0
10 9.426131 192.168.1.20 192.168.1.237 TCP 61077 > 661 [SYN] Seq=3204220283 Ack=0 Win=1024 Len=0
11 9.426220 192.168.1.20 192.168.1.237 TCP 61077 > 896 [SYN] Seq=3204220283 Ack=0 Win=1024 Len=0
12 9.426310 192.168.1.20 192.168.1.237 TCP 61077 > 912 [SYN] Seq=3204220283 Ack=0 Win=1024 Len=0
Frame 5 (60 on wire, 60 captured)
Ethernet II
Destination: 00:04:5a:97:76:11 (00:04:5a:97:76:11)
Source: 00:d0:b7:58:df:92 (00:d0:b7:58:df:92)
Type: IP (0x0800)
Trailer: 00000000000000000000000000000000...
Internet Protocol, Src Addr: 192.168.1.20 (192.168.1.20), Dst Addr: 192.168.1.237 (192.168.1.237)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 28
Identification: 0x2832
Flags: 0x00
Fragment offset: 0
Time to live: 50
Protocol: ICMP (0x01)
Header checksum: 0xdc5d (correct)
Source: 192.168.1.20 (192.168.1.20)
Destination: 192.168.1.237 (192.168.1.237)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x398a (correct)
Identifier: 0xbe75
Sequence number: 00:00
0010 00 1c 28 32 00 00 32 01 dc 5d c0 a8 01 14 c0 a8 ..(2..2. .]......
0020 01 ed 08 00 39 8a be 75 00 00 00 00 00 00 00 00 ....9..u ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
Filter:
Reset

Related Tools for Network IDS (II)

- Also not an element of Snort, tcpdump is a well-established Command Line Interface (CLI) packet capture tool
  - www.tcpdump.org offers UNIX source
  - http://www.winpcap.org/windump/ offers windump, a Windows port of tcpdump

Next Generation IDSs



- Vulnerability-based
- Adaptive
  - Automatically detect & generate signatures for zero-day attacks
- Scenario-based for forensics and being situational-aware
  - Correlate (multiple sources of) audit data and attack information

Physical Theft

An adversary gains physical access to a system or device through theft of the item. Possession of a system or device enables a number of unique attacks to be executed and often provides the adversary with an extended timeframe for which to perform an attack.

What is an example of physical theft?

The theft of magnetic storage media (tapes, hard drives), optical storage media such as CDs (Compact Discs), DVDs (Digital Versatile Discs) or electronics such as USB sticks (Universal Serial Bus), used for security copies, main storage or backups, is very common and enables the theft of large quantities of data.

What is the relationship between physical security and cybersecurity?

Together, **cyber and physical assets represent a significant amount of risk to physical security and cybersecurity** – each can be targeted, separately or simultaneously, to result in compromised systems and/or infrastructure.

How can we prevent physical theft?

- Do **not** leave your devices unattended in public areas.
- Store devices in secure areas such as a locked desk or office.
- Lock publicly-accessible non-portable devices to solid fixtures such as walls or tables to prevent theft.
- Do not leave physical documents containing sensitive University information in public areas.

Abuse of Privileges

Privilege abuse is **the fraudulent practice of using an account with additional privileges, also known as a privileged account, to access, exploit, or damage confidential business entities.**

Abuse of privileged information- This involves the use, by a public servant ofprivileged information and knowledge that a public servant possesses as a result of his/ her office to provide unfair advantage to another person or entity to obtain a benefit.

Negative impacts on privilege abuse by employees: Without a security protocol in place, **employees can easily gain access to sensitive information and increase the risk of data being leaked**. This can happen by accident, because of sloppy or lacking privileged access management (PAM) or through the interference of a cyber adversary.

Examples of privileged access used by humans:

The phrase "Keys to the IT Kingdom" is often used when referring to the privileged nature of some administrator accounts and systems. Local administrative account: This account is located on an endpoint or workstation and uses a combination of a username and password.

Understanding Privilege Escalation

Privilege escalation is a type of network attack used to gain unauthorized access to systems within a security perimeter.

Attackers start by finding weak points in an organization's defenses and gaining access to a system. In many cases that first point of penetration will not grant attackers with the level of access or data they need. They will then attempt privilege escalation to gain more permissions or obtain access to additional, more sensitive systems.

Malware Infection:

Malware can use known software vulnerabilities to infect your PC. A vulnerability is like a hole in your software that can give malware access to your PC. When you go to a website, it can try to use vulnerabilities in your web browser to infect your PC with malware.

What causes malware infection?

Malware can get onto your device when you open or download attachments or files, or visit a scammy website. Your device might get infected with malware through: downloading free stuff like illegal downloads of popular movies, TV shows, or games. downloading content available on file-sharing sites.

How do you know if you have a malware infection?

If you notice your homepage changed or you have new toolbars, extensions, or plugins installed, then you might have some sort of malware infection. Causes vary, but this usually means you clicked on that "congratulations" pop-up, which downloaded some unwanted software.

References

- Dr. K. V. Arya, Multimedia & Information Security Research Group, ABV-Indian Institute of Information Technology & Management Gwalior, India,
- https://www.malwarebytes.com/malware#:~:text=If%20you%20notice%20your%20homepage,which%20downloaded%20some%20unwanted%20software.
- https://www.google.com/search?rlz=1C1OKWM_enIN930IN930&q=What+causes+malware+infection%3F&sa=X&ved=2ahUKEwi9gPf35qr9AhUDCLcAHcDRD-0Qzmd6BAgXEAU
- https://support.microsoft.com/en-us/windows/how-malware-can-infect-your-pc-872bf025-623d-735d-1033-ea4d456fb76b#:~:text=Malware%20can%20use%20known%20software,infect%20your%20PC%20with%20malware.