CSCI 22062

Introduction to Cyber Security

Intrusion Detection/Prevention Systems

Dr. Dhammika Weerasinghe

hesiri@kln.ac.lk

Department of Computer Systems Engineering
Faculty of Computing & Technology
University of Kelaniya

Objectives and Deliverable

- Understand the concept of IDS/IPS and the two major categorizations: by features/models, and by location. Understand the pros and cons of each approach
- Be able to write a snort rule when given the signature and other configuration info
- Understand the difference between exploits and vulnerabilities

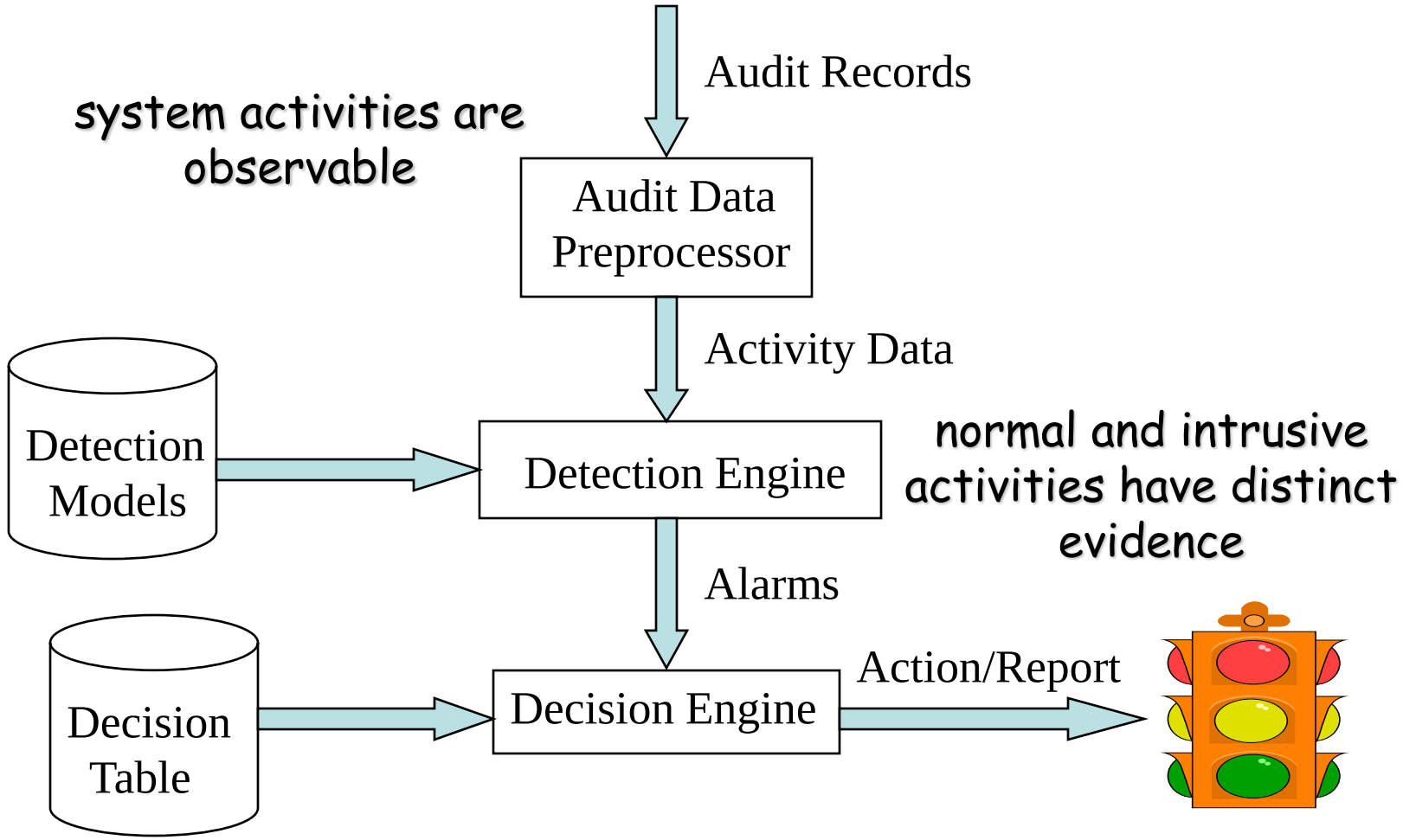
Definitions

- Intrusion
  - A set of actions aimed to compromise the security goals, namely
    - Integrity, confidentiality, or availability, of a computing and networking resource
- Intrusion detection
  - The process of identifying and responding to intrusion activities
- Intrusion prevention
  - Extension of ID with exercises of access control to protect computers from exploitation

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

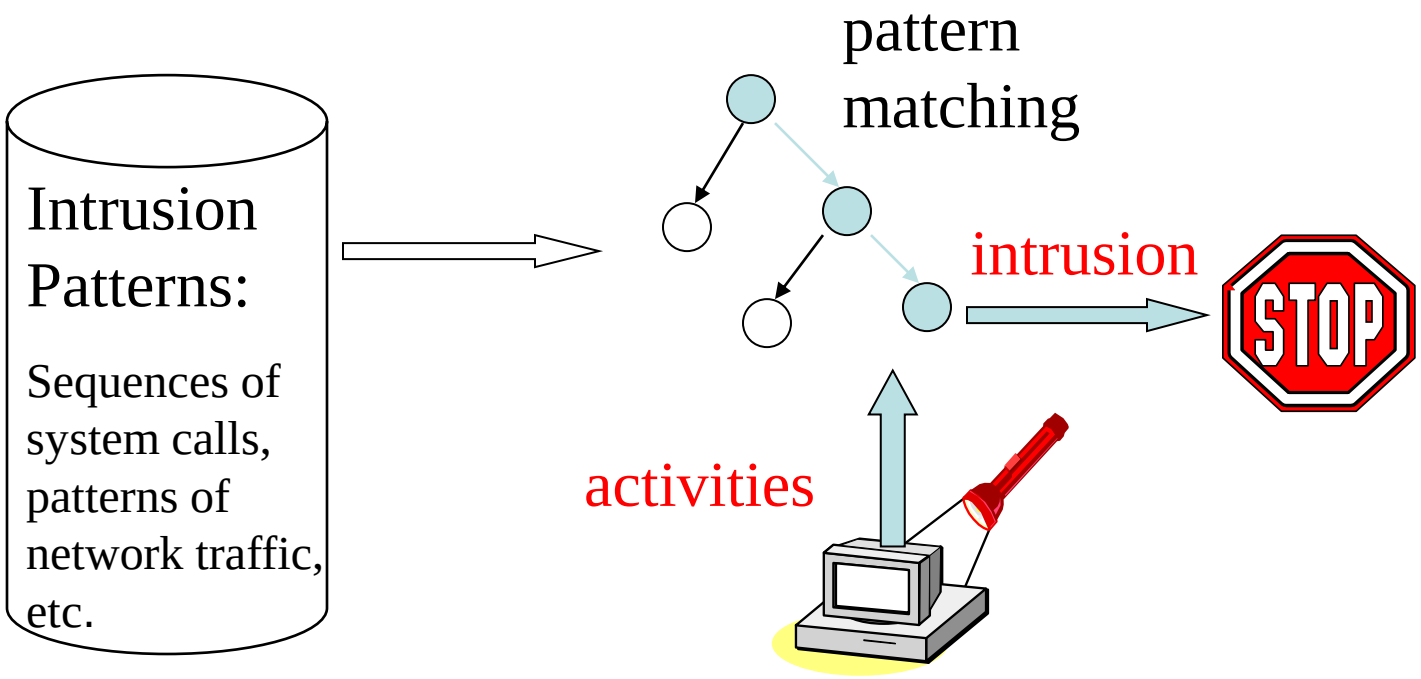
Components of Intrusion Detection System



Intrusion Detection Approaches

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

Misuse Detection

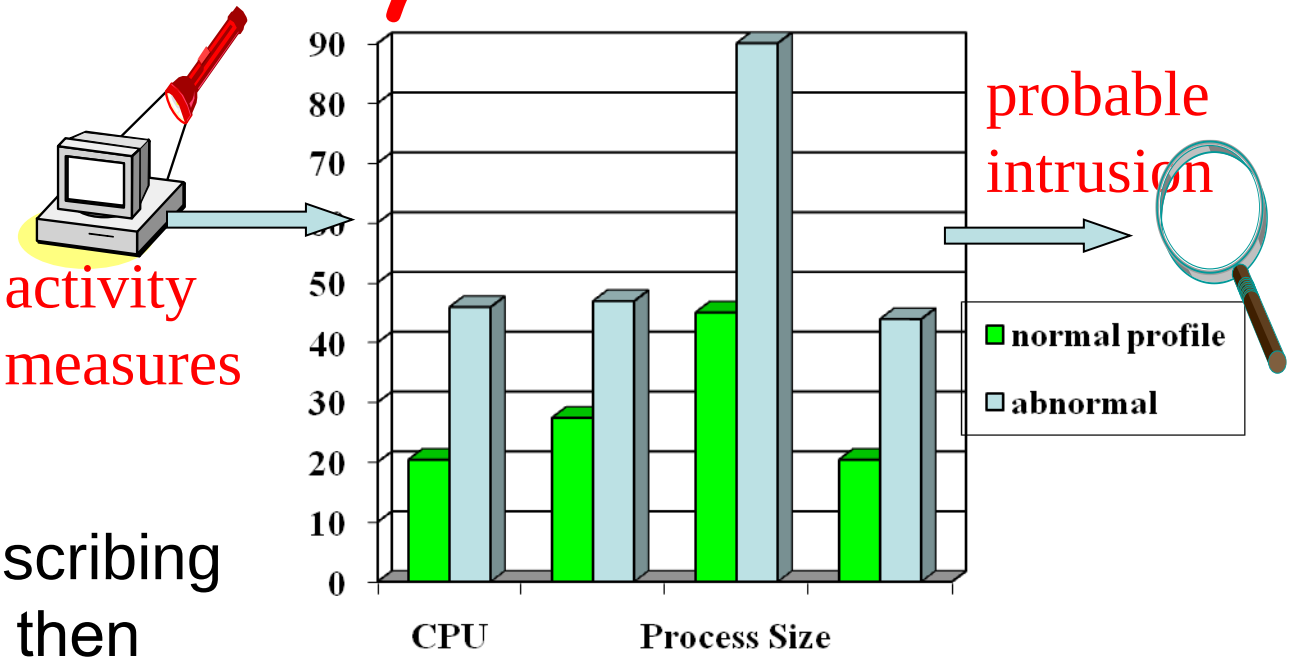


Example: ***if*** (traffic contains "x90+de[^\r\n]{30}") ***then*** "attack detected"

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 ?

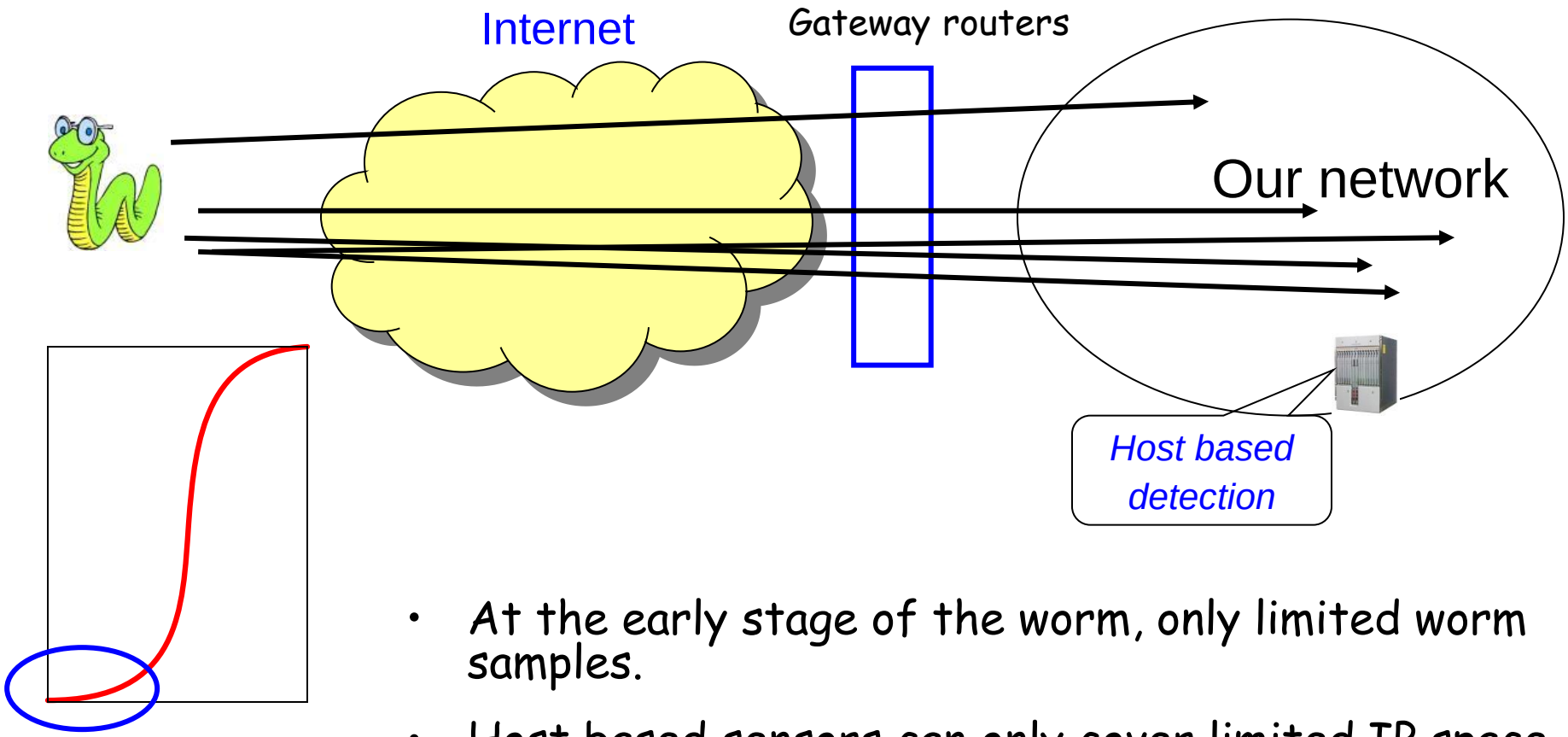
Relatively high false positive rates

- 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:
  - User dependent: install/update IDS on all user machines!
  - If attacker takes over machine, can tamper with IDS binaries and modify audit logs
  - 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. Thus they 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

Host-based vs. Network-based IDS

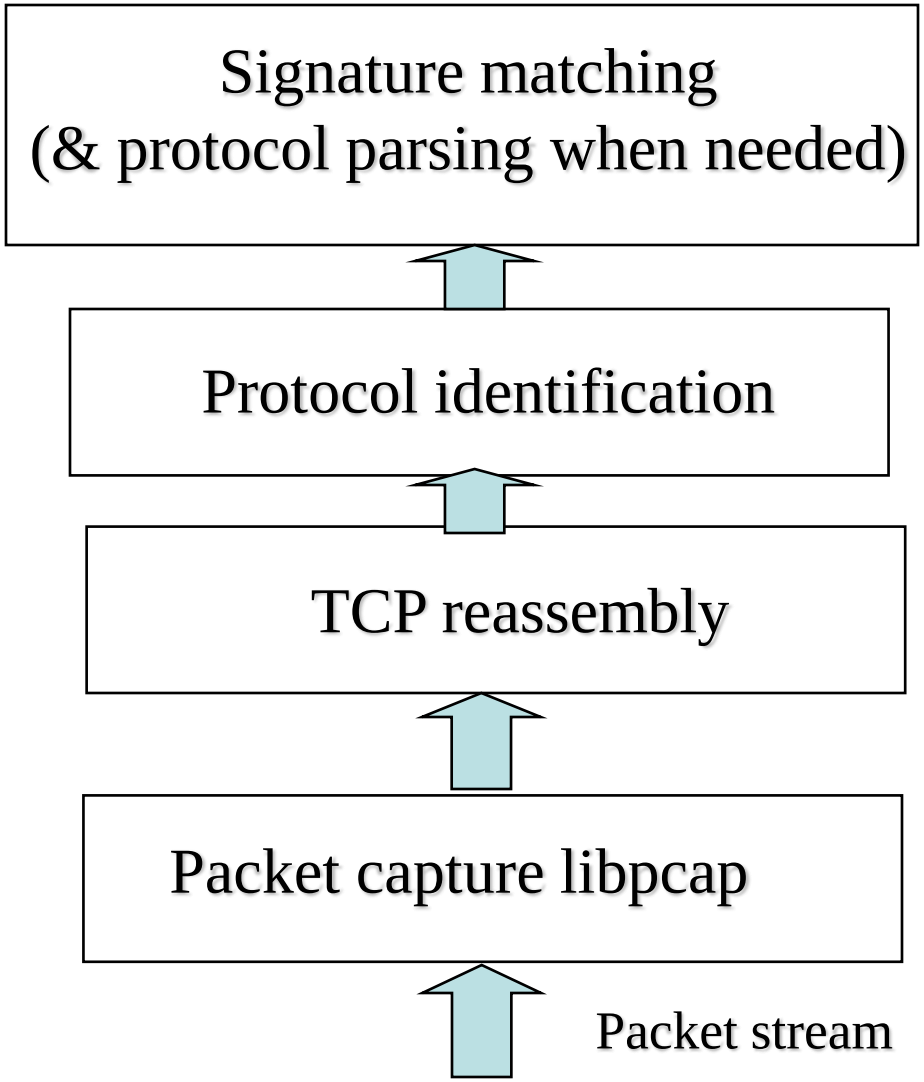
- Give an attack that can only be detected by host-based IDS but not network-based IDS

- Can you give an example only be detected by network-based IDS but not host-based IDS ?

Key Metrics of IDS/IPS

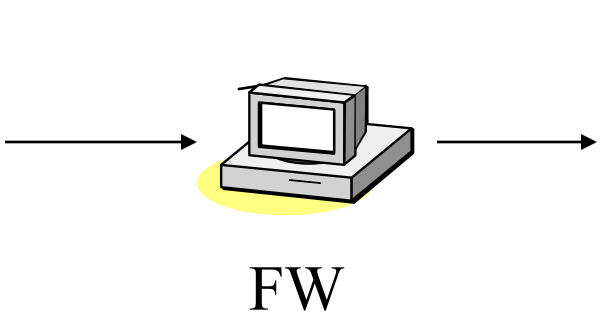
- Algorithm
  - Alarm: A; Intrusion: I
  - Detection (true alarm) rate: P(A|I)
    - False negative rate P(¬A|I)
  - False alarm (aka, false positive) rate: P(A|¬I)
    - True negative rate P(¬A|¬I)
- Architecture
  - Throughput of NIDS, targeting 10s of Gbps
    - E.g., 32 nsec for 40 byte TCP SYN packet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

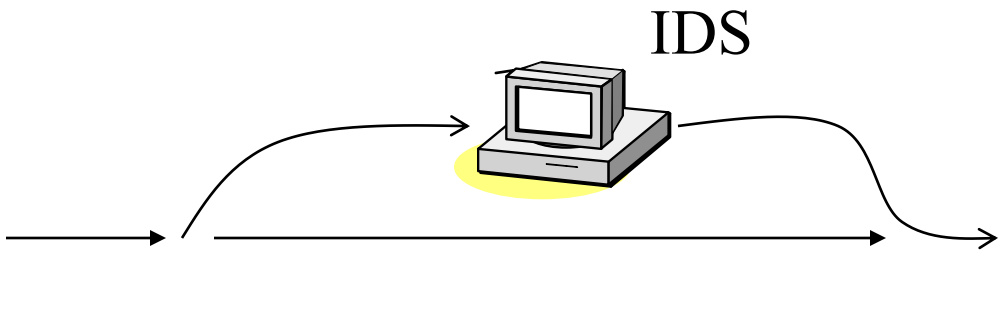
Architecture of Network IDS



Firewall/Net IPS VS Net IDS

- Firewall/IPS
  - Active filtering
  - Fail-close
- Network IDS
  - Passive monitoring
  - Fail-open





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.