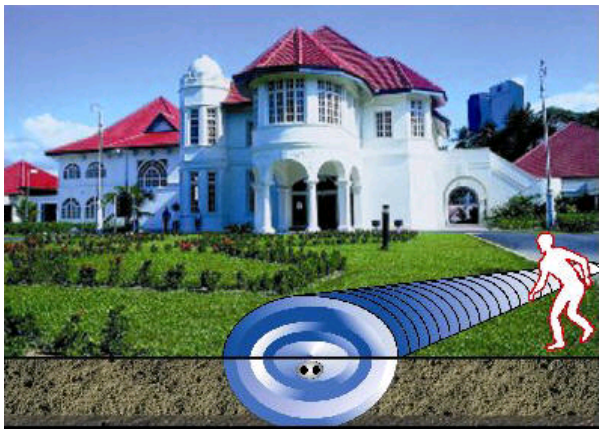
CSCE 465 Computer & Network Security

Instructor: Sungmin Kevin Hong

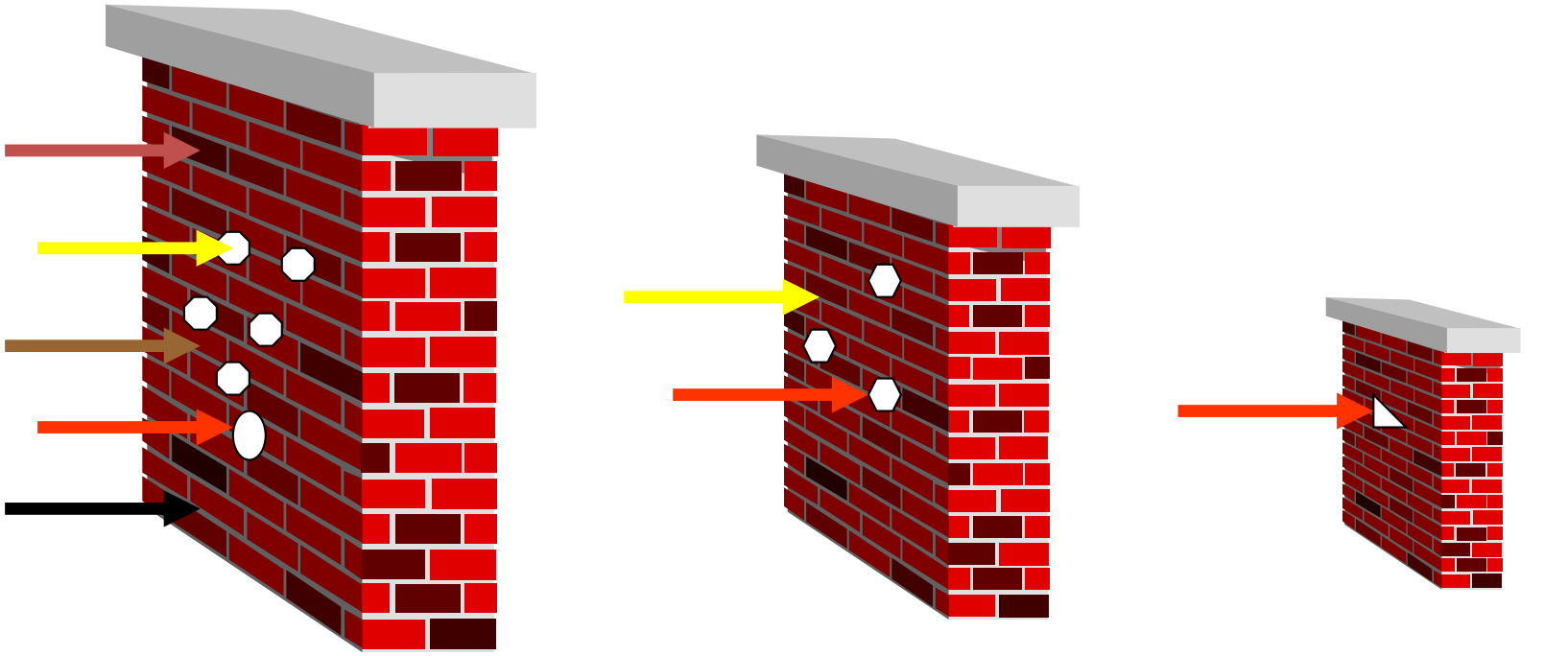
Intrusion Detection System

Definitions

- Intrusion
  - A set of actions aimed to compromise the security goals, namely
    - Confidentiality, Integrity, or Availability, of a computing and networking resource
- Intrusion detection
  - The process of identifying and responding to intrusion activities



Why Is Intrusion Detection Necessary?



Prevent

Detect

React/
Survive

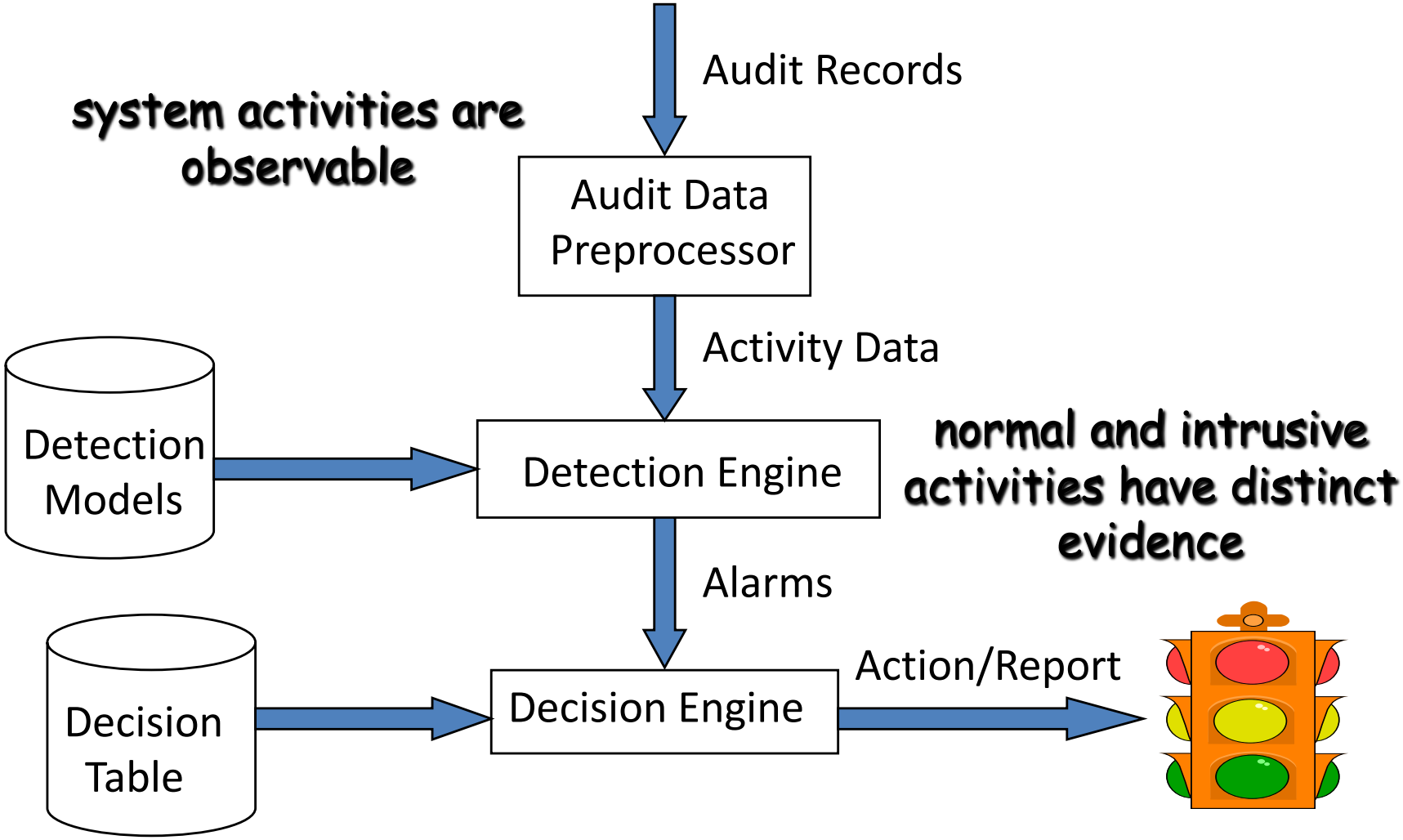
Security principles: layered mechanisms

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:
    - Audit data processor, knowledge base, decision engine, alarm generation and responses

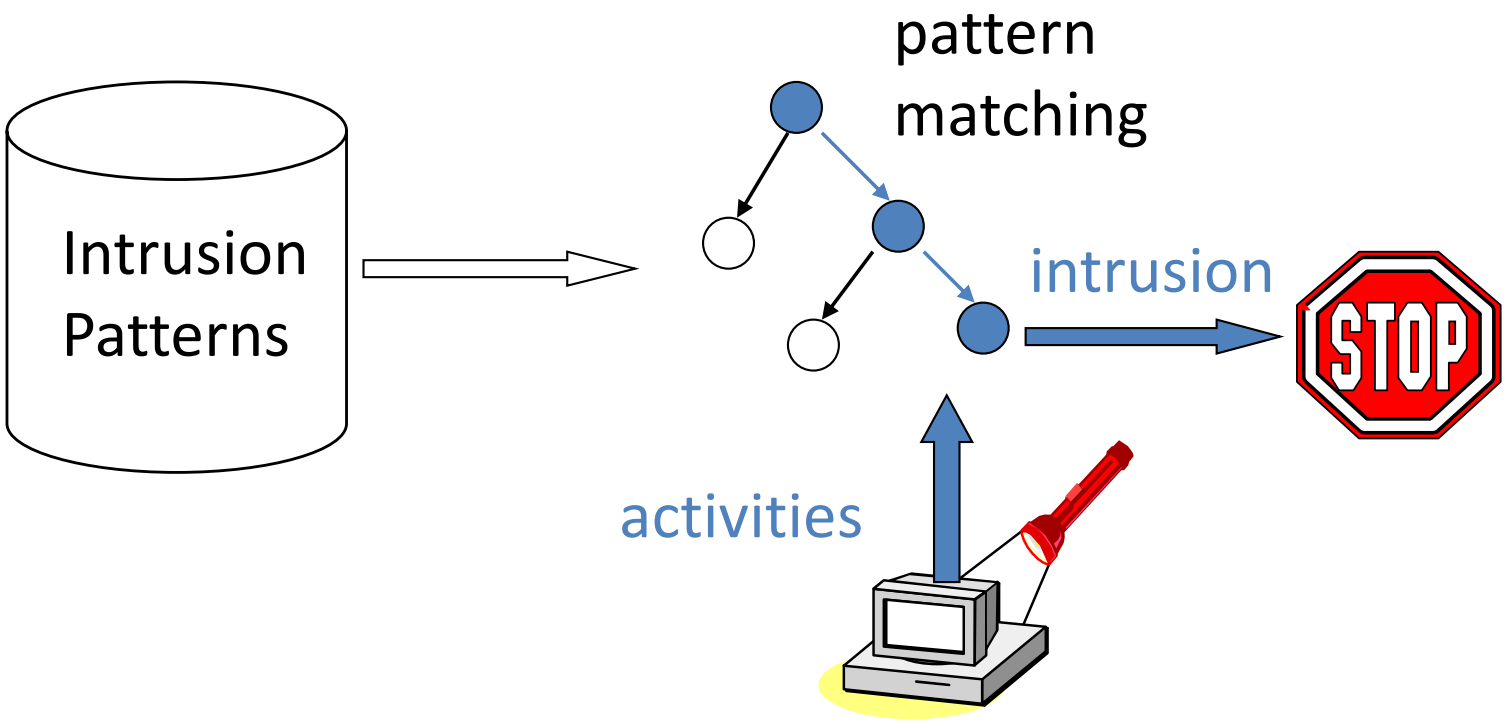
Components of Intrusion Detection System



Intrusion Detection Approaches

- Modeling
  - Features: evidences extracted from audit data
  - Analysis approach: piecing the evidences together
    - Misuse detection (signature-based, e.g., Snort, Bro)
    - Anomaly detection (e.g., statistical-based)
- Deployment: Network-based or Host-based
- Development and maintenance
  - Hand-coding of “expert knowledge”
  - Learning based on audit data

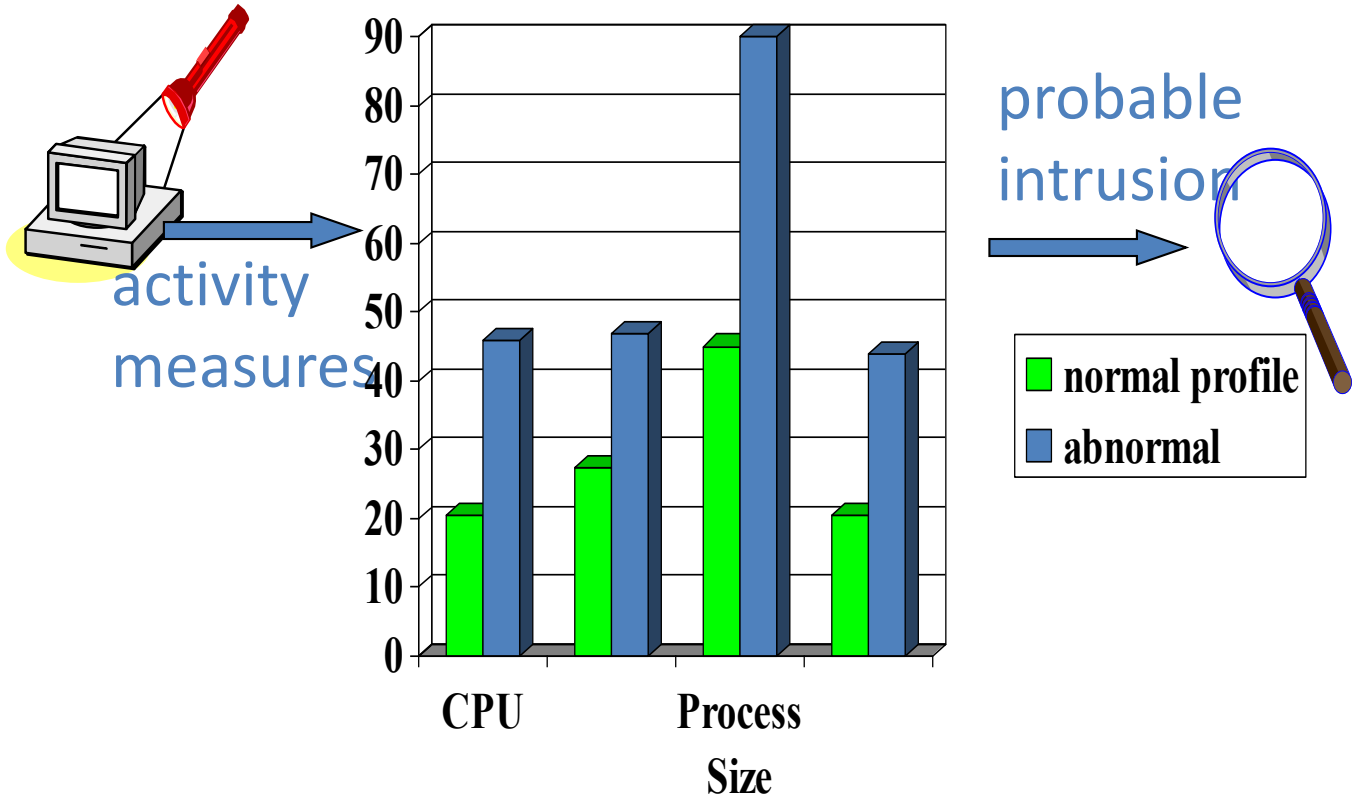
Misuse Detection



Example: ***if*** (src_ip == dst_ip) ***then*** "land attack"

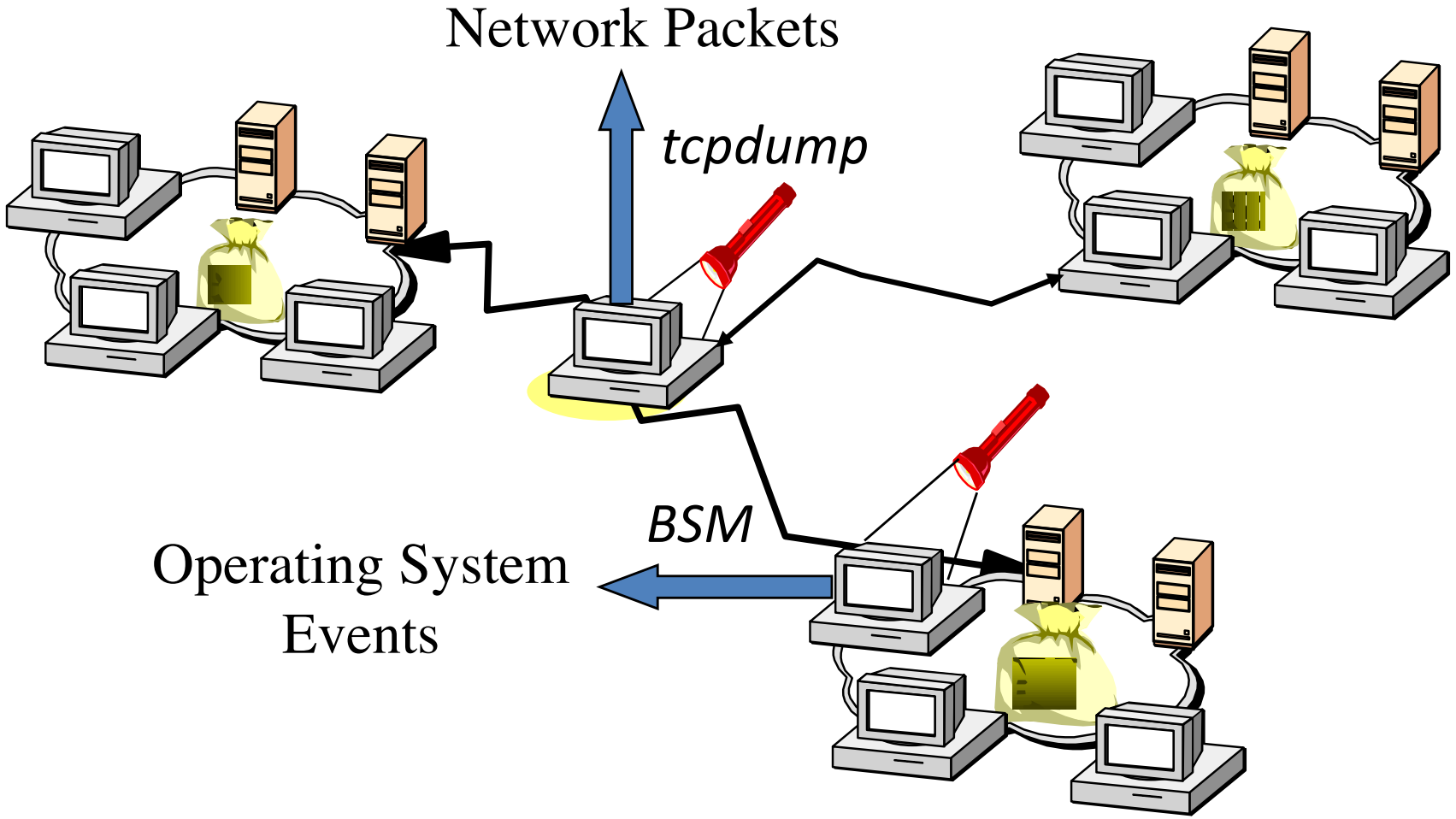
Can't detect new attacks

Anomaly Detection



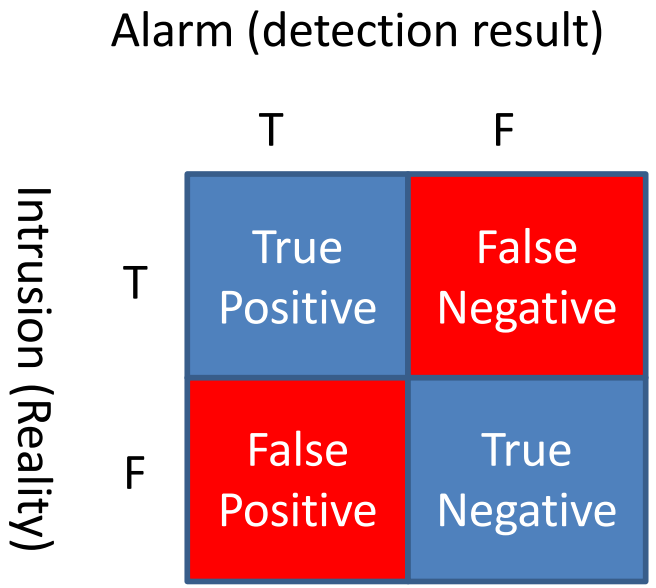
Relatively high false positive rate -
anomalies can just be new normal activities.

Monitoring Networks and Hosts



Key Performance Metrics

- Algorithm
  - Alarm: A; Intrusion: I
  - Detection (true positive) rate: P(A|I)
    - False negative rate P(¬A|I)
  - False positive (alarm) rate: P(A|¬I)
    - True negative rate P(¬A|¬I)
  - Bayesian detection rate: P(I|A)
- Architecture
  - Scalable
  - Resilient to attacks

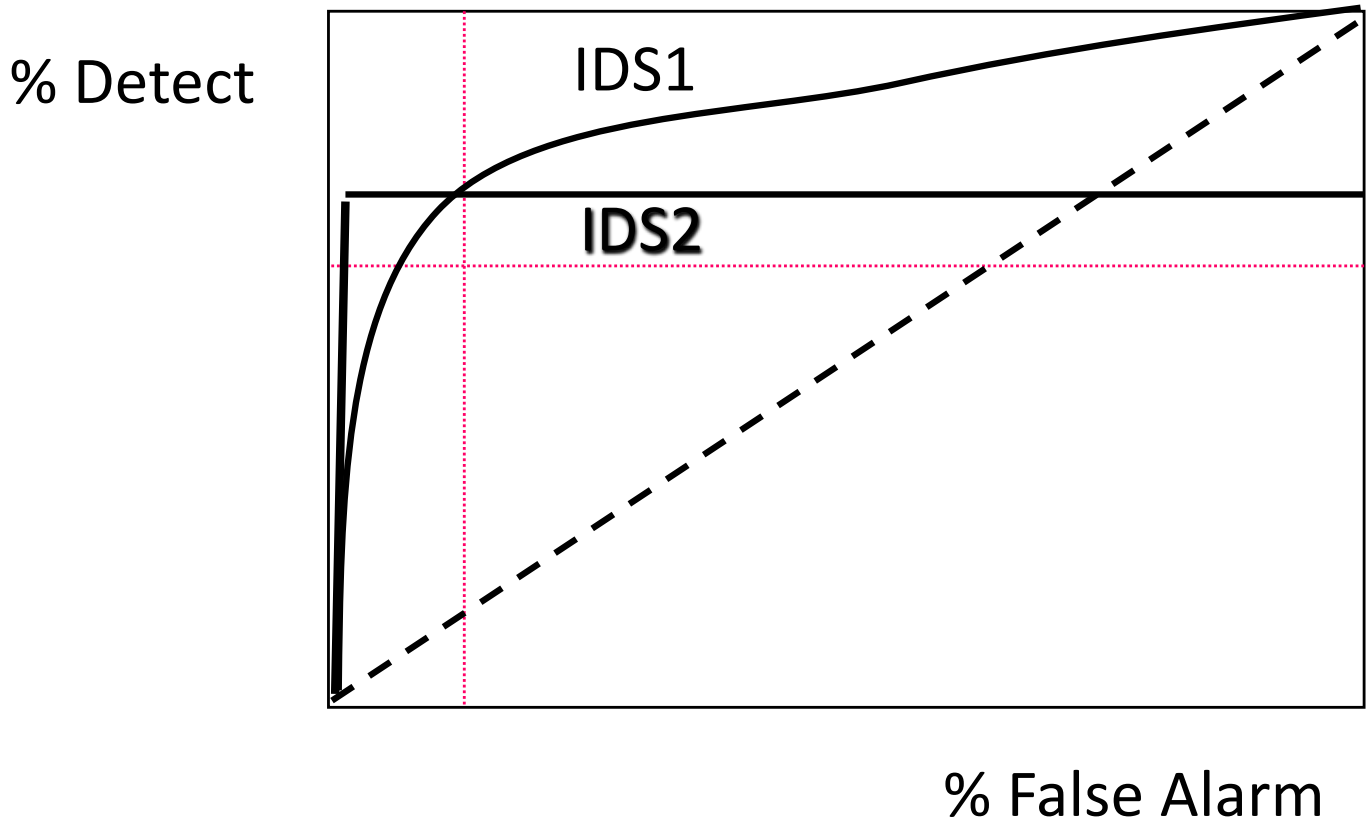


Bayesian Detection Rate

$$P(I \mid A) = \frac{P(I)P(A \mid I)}{P(I)P(A \mid I) + P(\neg I)P(A \mid \neg I)}$$

- Base-rate fallacy
  - Even if false alarm rate $P(A|\neg I)$ is very low, Bayesian detection rate $P(I|A)$ is still low if base-rate $P(I)$ is low
  - E.g. if $P(A|I) = 1$, $P(A|\neg I) = 10^{-5}$, $P(I) = 2\times10^{-5}$, $P(I|A) =$ 66%
- Implications to IDS
  - Design algorithms to reduce **false alarm rate**
  - Deploy IDS to appropriate point/layer with sufficiently **high base rate**

Example ROC Curve



- Ideal system should have 100% detection rate with 0% false alarm

Host-Based IDSs (HIDS)

- Using OS auditing mechanisms
  - E.G., BSM on Solaris: logs all direct or indirect events generated by a user
  - *strace* for system calls made by a program
- Monitoring user activities
  - E.G., Analyze shell commands
- Monitoring executions of system programs
  - E.G., Analyze system calls made by *sendmail*

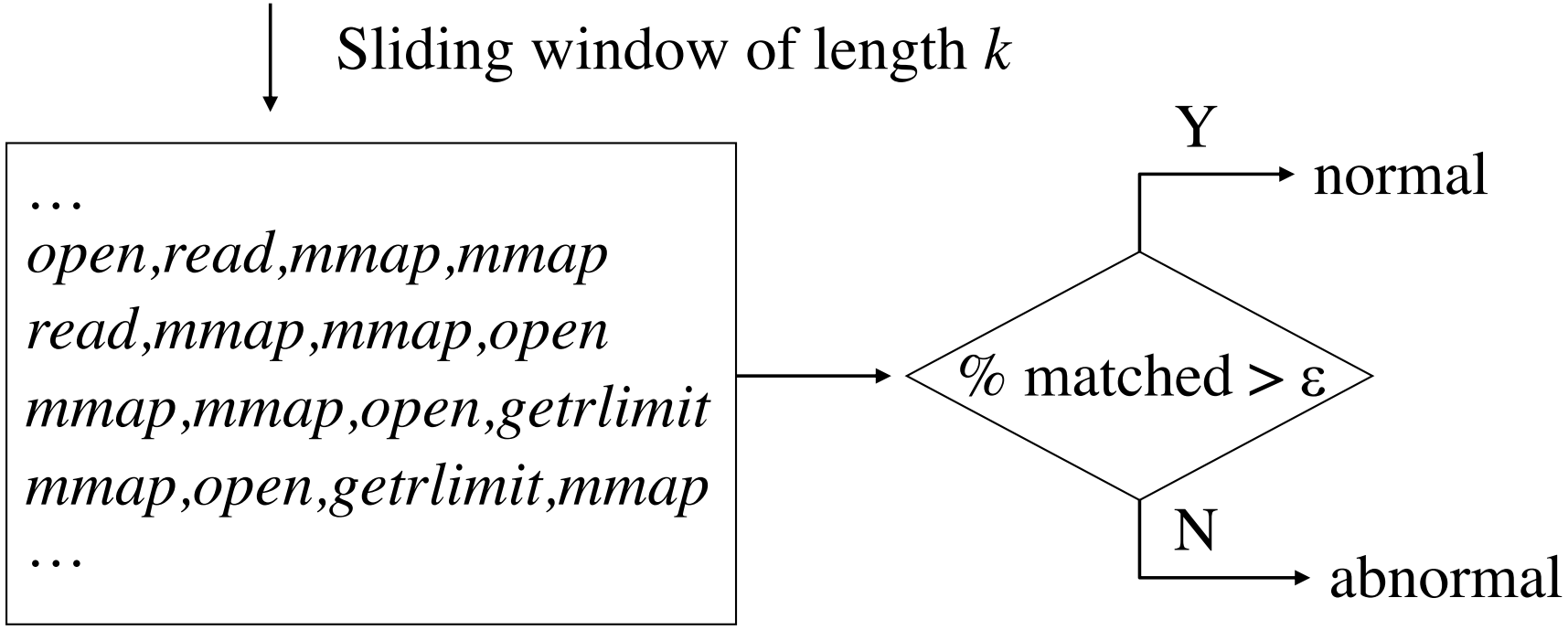
Example HIDS:
A Sense of Self - Immunology Approach

- Prof. Forrest at University of New Mexico
  - Anomaly detection
  - Simple and short sequences of events to distinguish “self” from not
  - Currently looking at system calls (strace)
  - Apply to detection of *lpr* and *sendmail*

Some Details

- Anomaly detection for Unix processes
  - "Short sequences" of system calls as normal profile (Forrest et al. UNM)

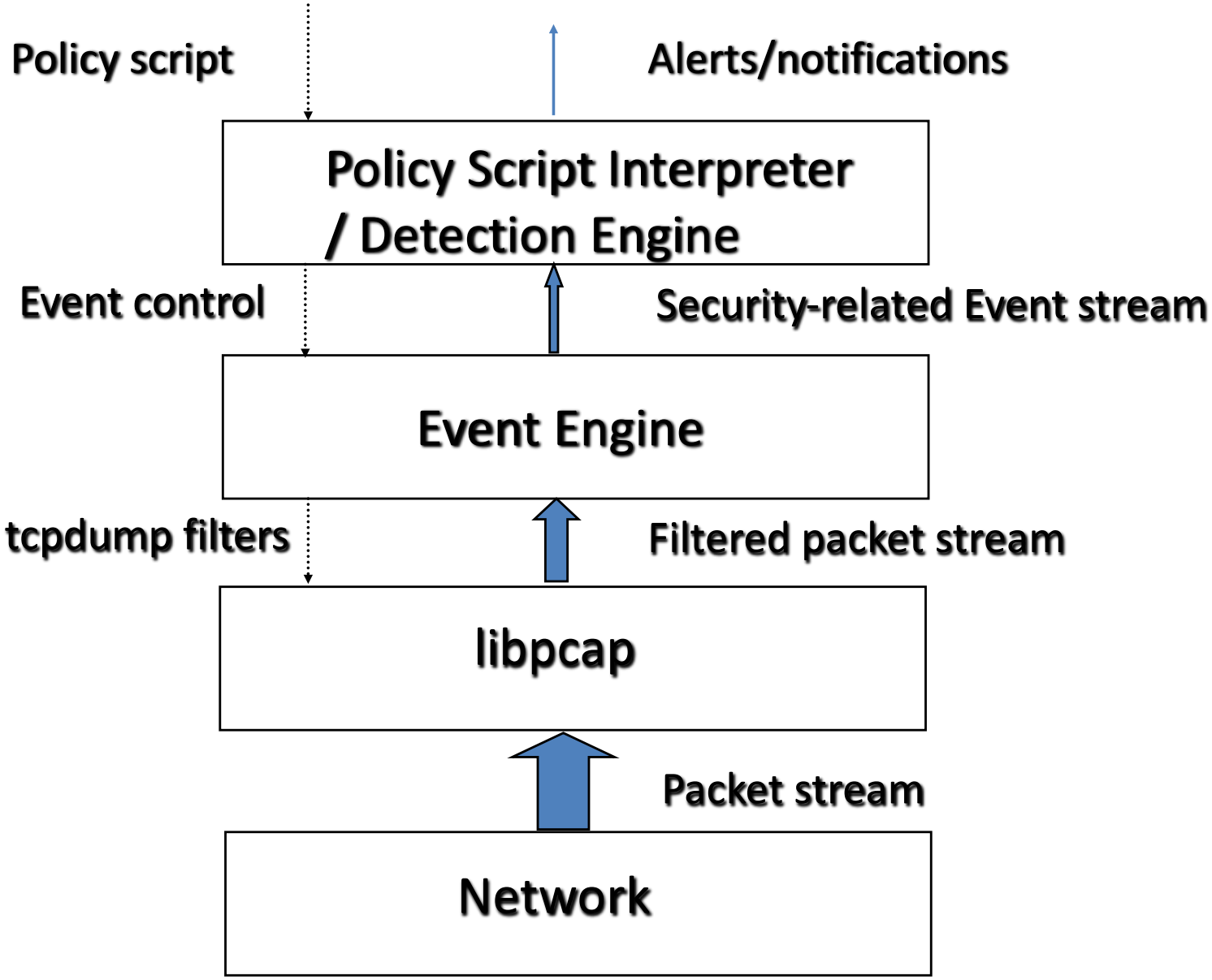
…,*open*,*read*,*mmap*,*mmap*,*open*,*getrlimit*,*mmap*,*close*,…



Network IDSs (NIDS)

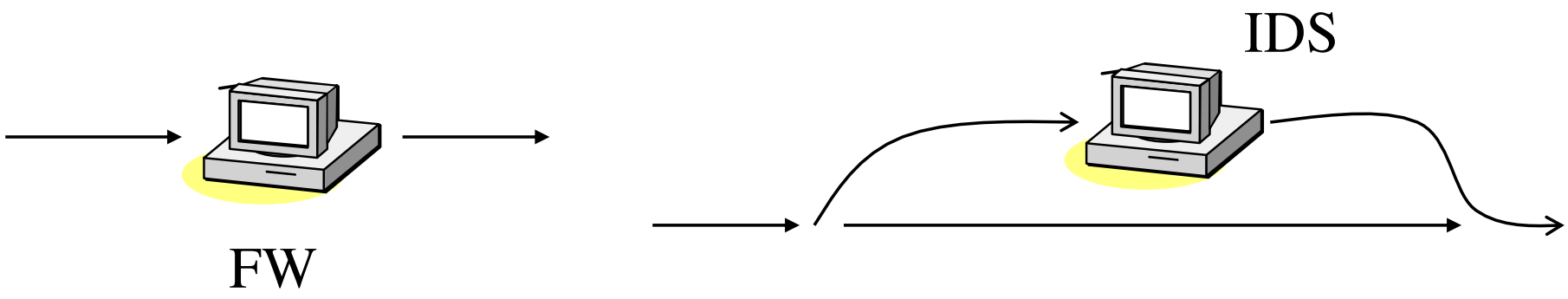
- Deploying sensors at strategic locations
  - E.G., Packet sniffing via *tcpdump* at routers
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
- Monitoring user activities
  - Look into the data portions of the packets for malicious command sequences
- May be easily defeated by encryption
  - Data portions and some header information can be encrypted
- Other problems …

Architecture of Network IDS



Firewall Versus Network IDS

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



Requirements of Network IDS

- High-speed, large volume monitoring
  - No packet filter drops
- Real-time notification
- Extensible
- Broad detection coverage
- Economy in resource usage
- Resilience to stress
- Resilience to attacks upon the IDS itself!

Eluding Network IDS

- What the IDS sees may not be what the end system gets.
  - Insertion and evasion attacks.
    - IDS needs to perform full reassembly of packets.
  - But there are still ambiguities in protocols and operating systems:
    - E.G. TTL, fragments.
    - Need to “normalize” the packets.

Insertion Attack