IDS
IPS
Honeypots

CS361S

FALL 2020

LECTURE NOTES

What’s The Commonality?

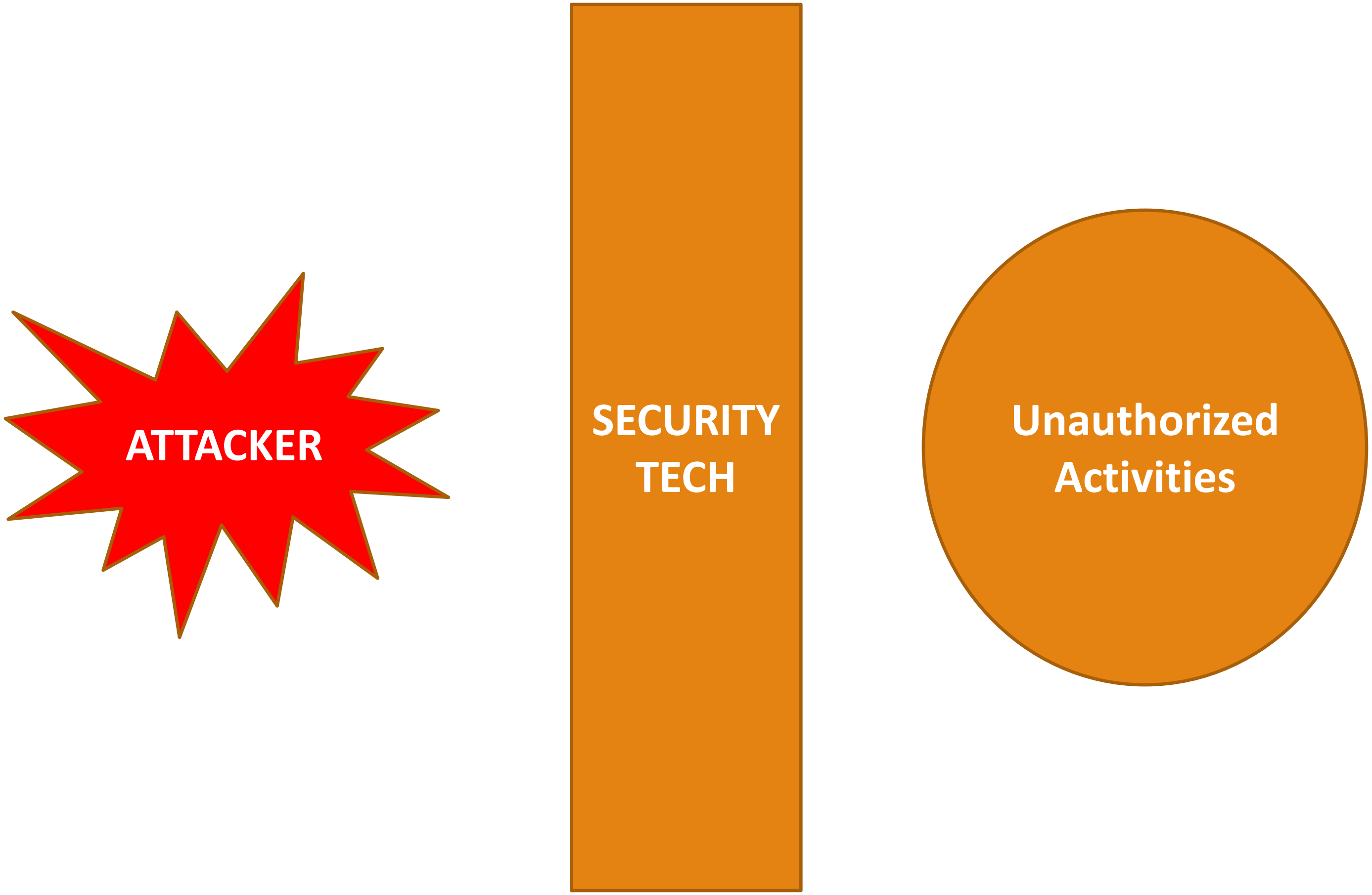
Cryptography

Access Controls

Firewalls

Filtering Inputs/Escaping Outputs

Ideal Computer Security



Security in Practice

Attackers do, in fact, get past security

Some security technology dedicated to:

- Recognizing intrusion
- Eliminating the intruder
- Mitigating the damage

These steps are independent

Intrusion Detection System

Primarily focused on ***DETECTION***

Goal is ***SPEED!*** resources

Can protect networks, systems, and other resources

Why does it Matter?

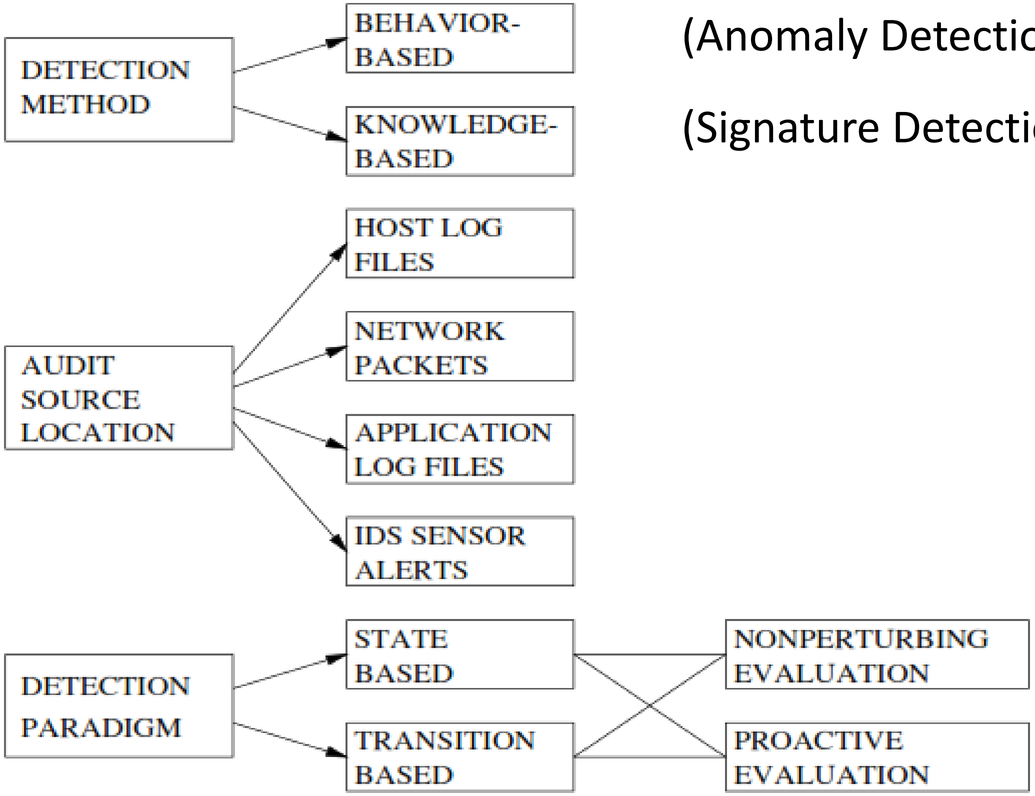
Prevent additional/worse damage

Identify holes in security

Forensic analysis of what was stolen/lost

Legal responsibilities

Taxonomy

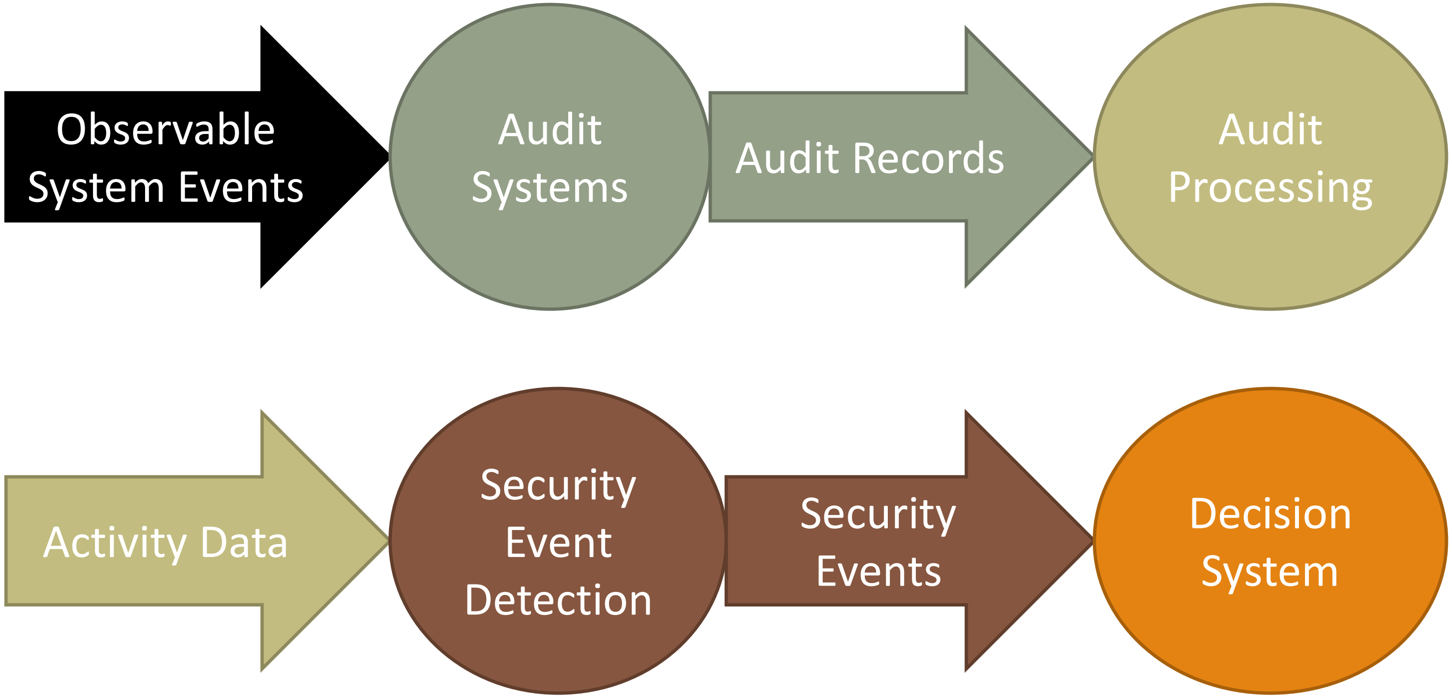


(Anomaly Detection)

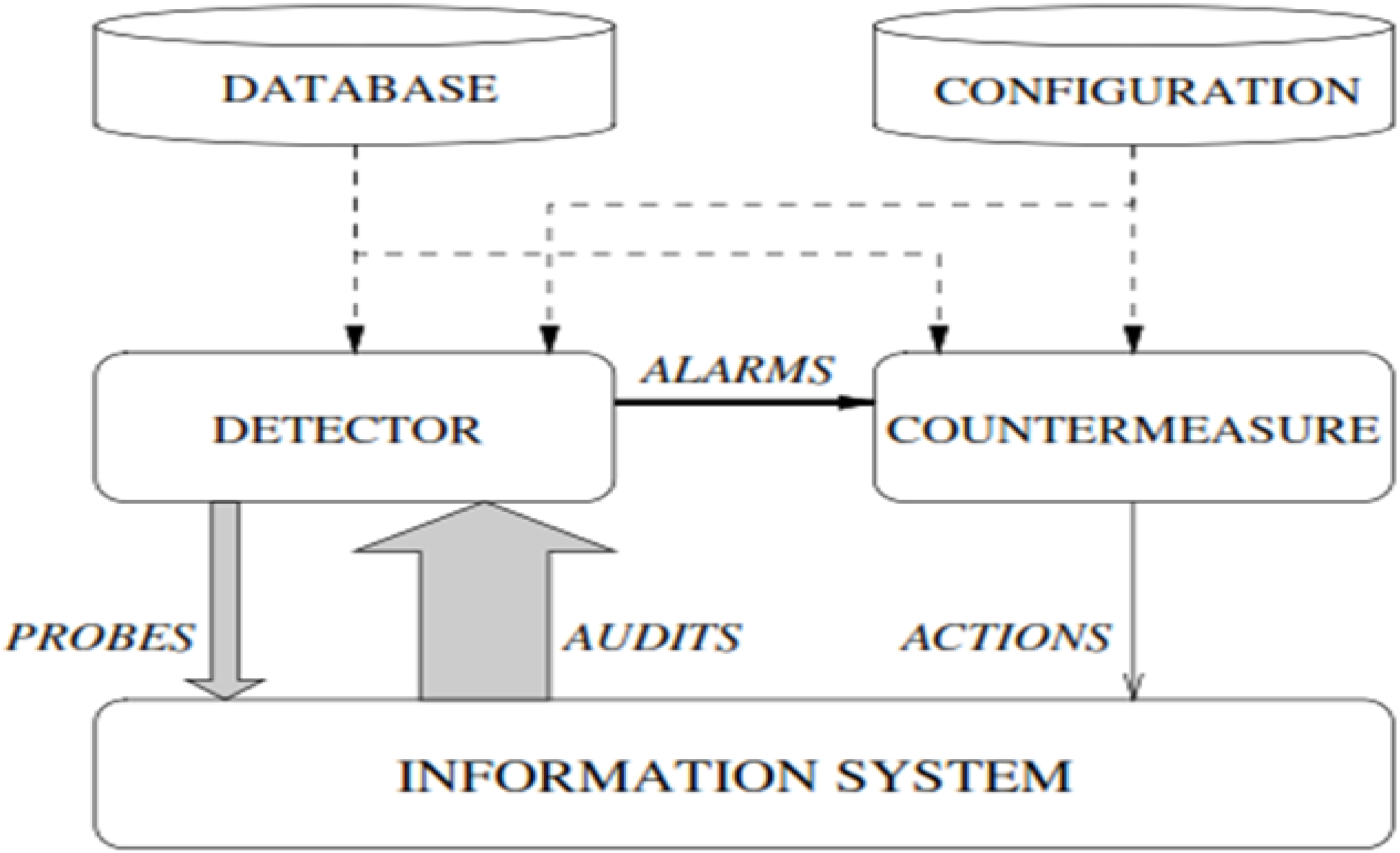
(Signature Detection)

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

Conceptual Approach



Very simple intrusion-detection system



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

Signature Approach

Library of attack ***patterns***

Can be pattern of any information

- Network packet data
- Host access
- Even Host syscall logs

Like with antivirus signatures, can’t block new attacks

Anomaly Detection

Identify “normal” activity

Trackable activity is just about anything

- File access
- User activity
- Even CPU activity!

Look for “abnormal” activity

- Can use heuristic rules
- Can use machine learning

Anomaly Problems

Always struggles with False Positives!

How often does your behavior change?

Major events like COVID completely redo the norm

Mistakes, errors, etc cause “anomalies”

Common IDS Types

NIDS – Network IDS

- For example, identifying DDOS attacks
- Scan packets, looks for bad network operations
- Can be realtime or offline

HIDS – Host-based IDS

- Monitor for unusual or unauthorized host activity
- Aggregate multiple hosts to a central system
- Host can basically become a network sensor

Protocol Analysis

At either host or network, decode the protocol

Low levels are easy! Only a few protocols

Application layer is hard! Need a decoder for each app!

Application layer also requires TLS decryption

Can use the data for signatures or anomalies

Audit Data

Even systems with real-time detection still create logs

Audit trails can be processed offline to look for intrusions

Audit data can be generated for the network or hosts

Audit data can be aggregated from many sensors

Alerts

Most IDS works by alerting a security officer

What gets alerted and how is configurable

Problem #1: Alerts from multiple systems

Problem #2: Tuning (too many, too few)

SIEM

Security Information and Event Management

Real-time analysis of alerts from multiple systems/sensors

Log and audit data normalization/aggregation

Composite alerting

Dashboards

Compliance

IPS

Intrusion Prevention System

IDS + reaction

IPS can change firewall rules in response to an attack

Some IPS can actively close an attack network connection

False positives are an even bigger problem.

Data Loss Prevention(DLP)

DLP targets malicious ***or accidental*** exfiltration

DLP has two general components

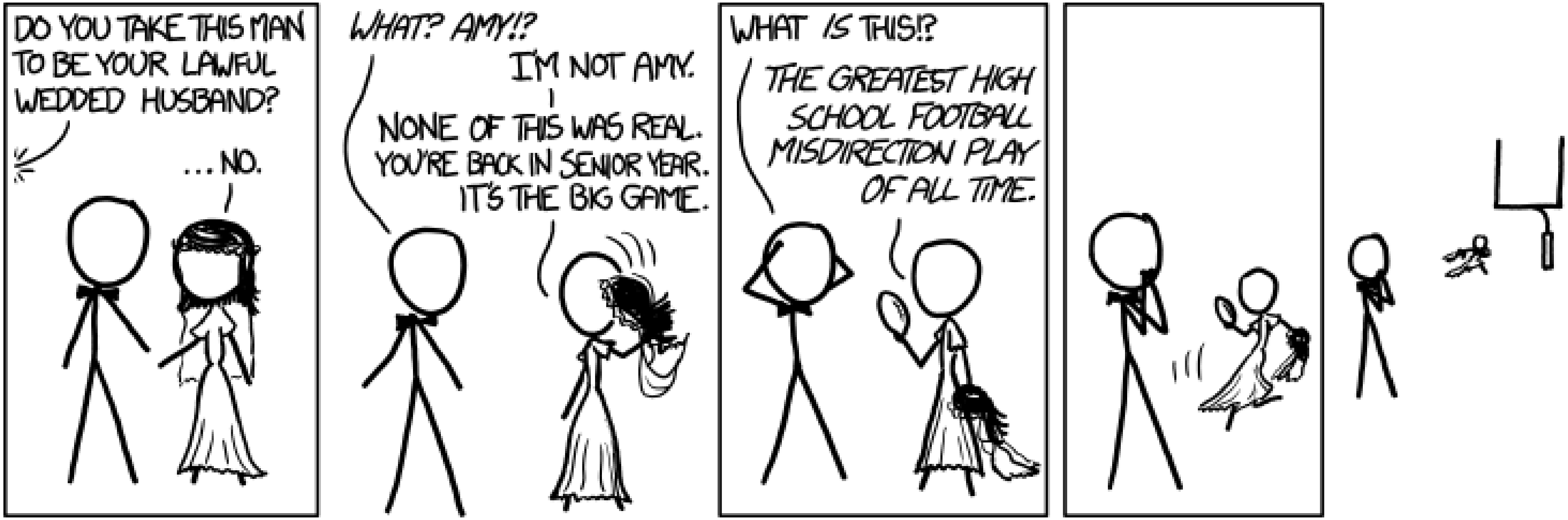
- Data preprocessing and host scanning
- Network tracking of outbound data

The first step is for finding confidential/PII

The second step partially requires the first

Almost always requires TLS visibility/interception

Deception


DO YOU TAKE THIS MAN TO BE YOUR LAWFUL WEDDED HUSBAND?
... NO.
WHAT? AMY!?
I'M NOT AMY.
NONE OF THIS WAS REAL. YOU'RE BACK IN SENIOR YEAR. IT'S THE BIG GAME.
WHAT IS THIS!?
THE GREATEST HIGH SCHOOL FOOTBALL MISDIRECTION PLAY OF ALL TIME.

https://xkcd.com/1100

Honeypots

Honeypots are any fake resource

Fake systems, fake documents, fake networks, etc

One purpose is tracking exfiltrated information

But more commonly used to detect intruders

Beyond Honeypots

Many honeypot deployments are ad hoc

Recently, better development in deception theory/practice

Better designed comprehensive honeypot system

- Fake network nodes
- Fake hosts
- Fake users/email/docs

Detect attacker, waste attacker time, etc