Computer Intrusion Detection

Lecture 1
Introduction

Xiangyang Li
EN.650.654

Outline

Lifecycle of Information Assurance

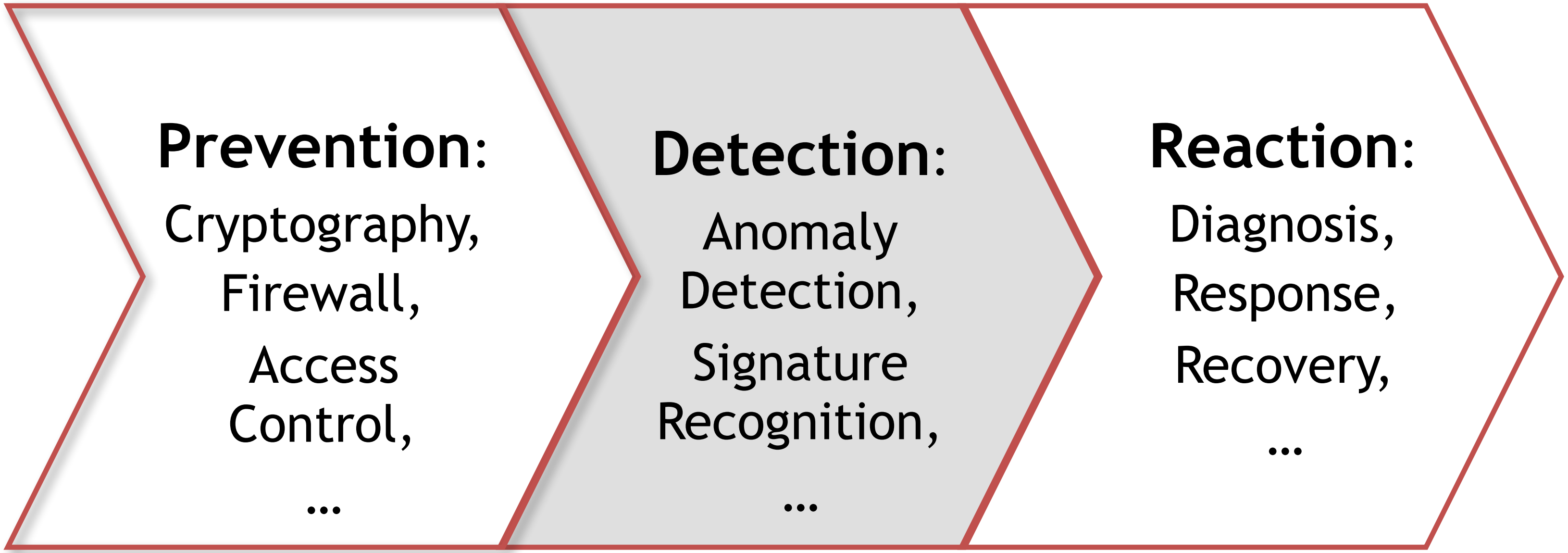
History of Intrusion Detection

IDS Architecture

Information Security

- Information security requirements have changed in recent times.
- Traditionally provided by physical and administrative mechanisms.
- Computer use requires automated tools to protect files and other stored information.
- Use of networks and communications links requires measures to protect data during transmission.

Information Assurance Lifecycle

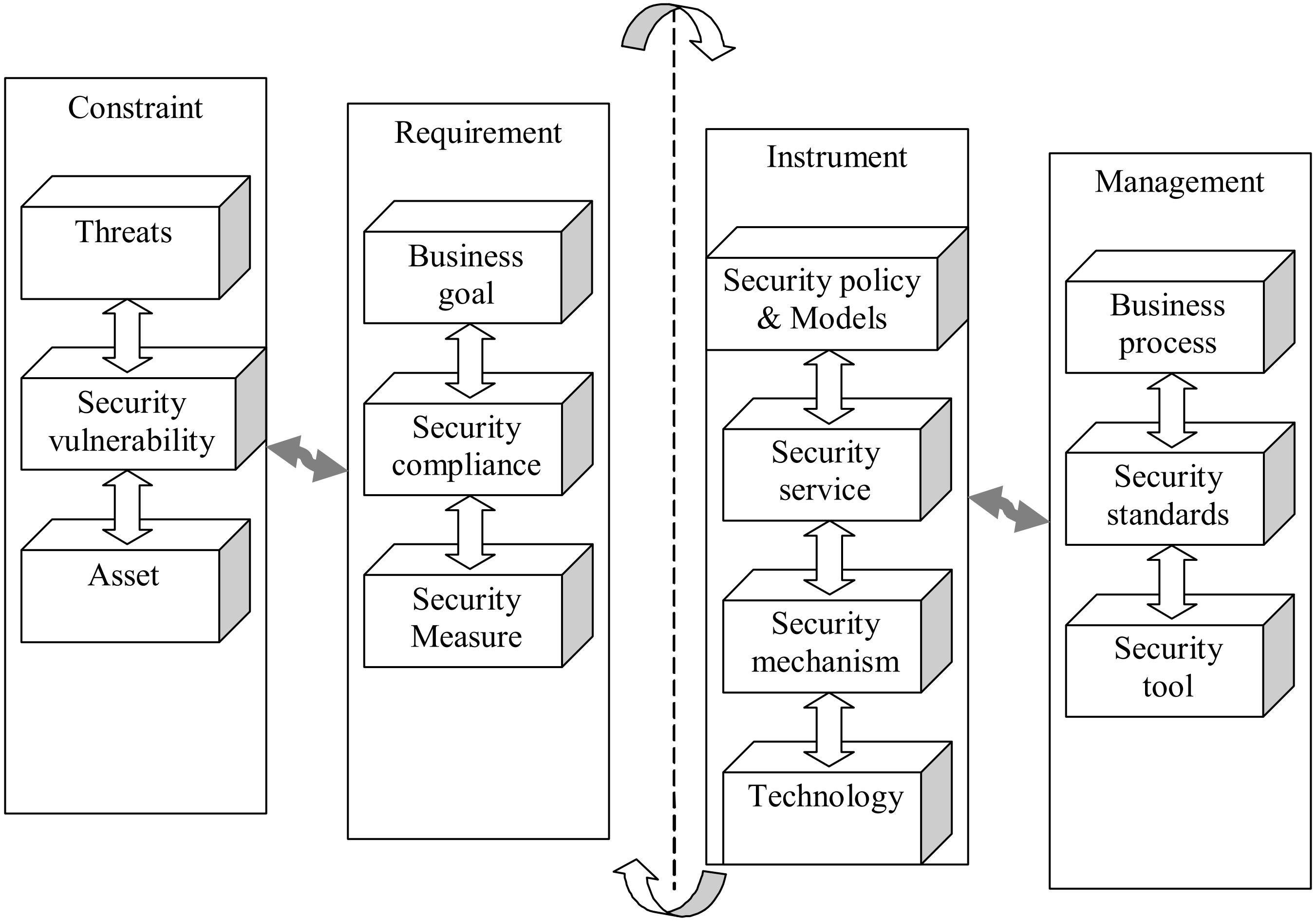


Prevention:
Cryptography,
Firewall,
Access Control,
…

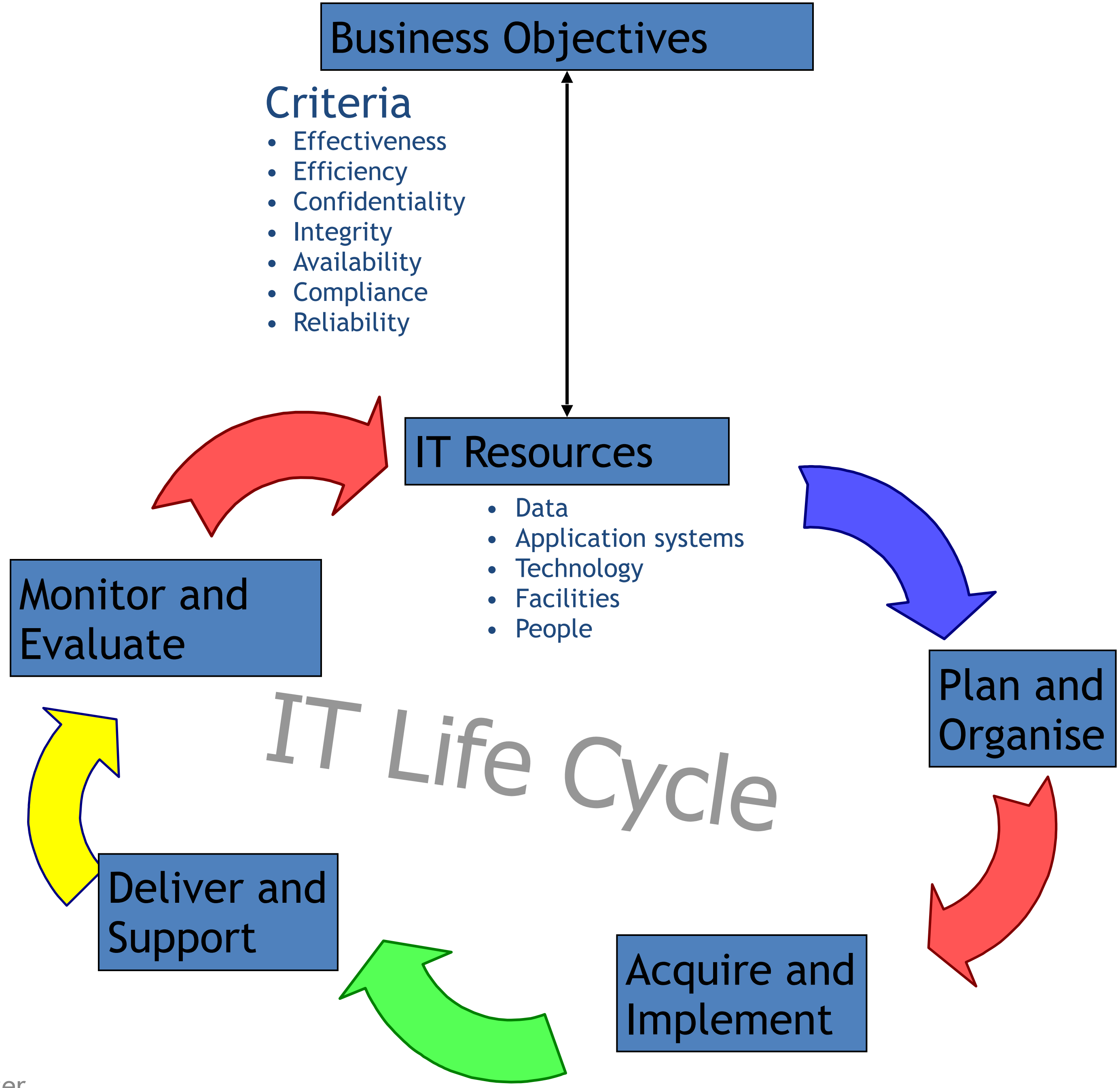
Detection:
Anomaly Detection,
Signature Recognition,
…

Reaction:
Diagnosis,
Response,
Recovery,
…

A Taxonomy


Constraint
Threats
Security vulnerability
Asset
Requirement
Business goal
Security compliance
Security Measure
Instrument
Security policy & Models
Security service
Security mechanism
Technology
Management
Business process
Security standards
Security tool

COBIT Framework



Business Objectives

Criteria

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Resources

- Data
- Application systems
- Technology
- Facilities
- People

Plan and Organise

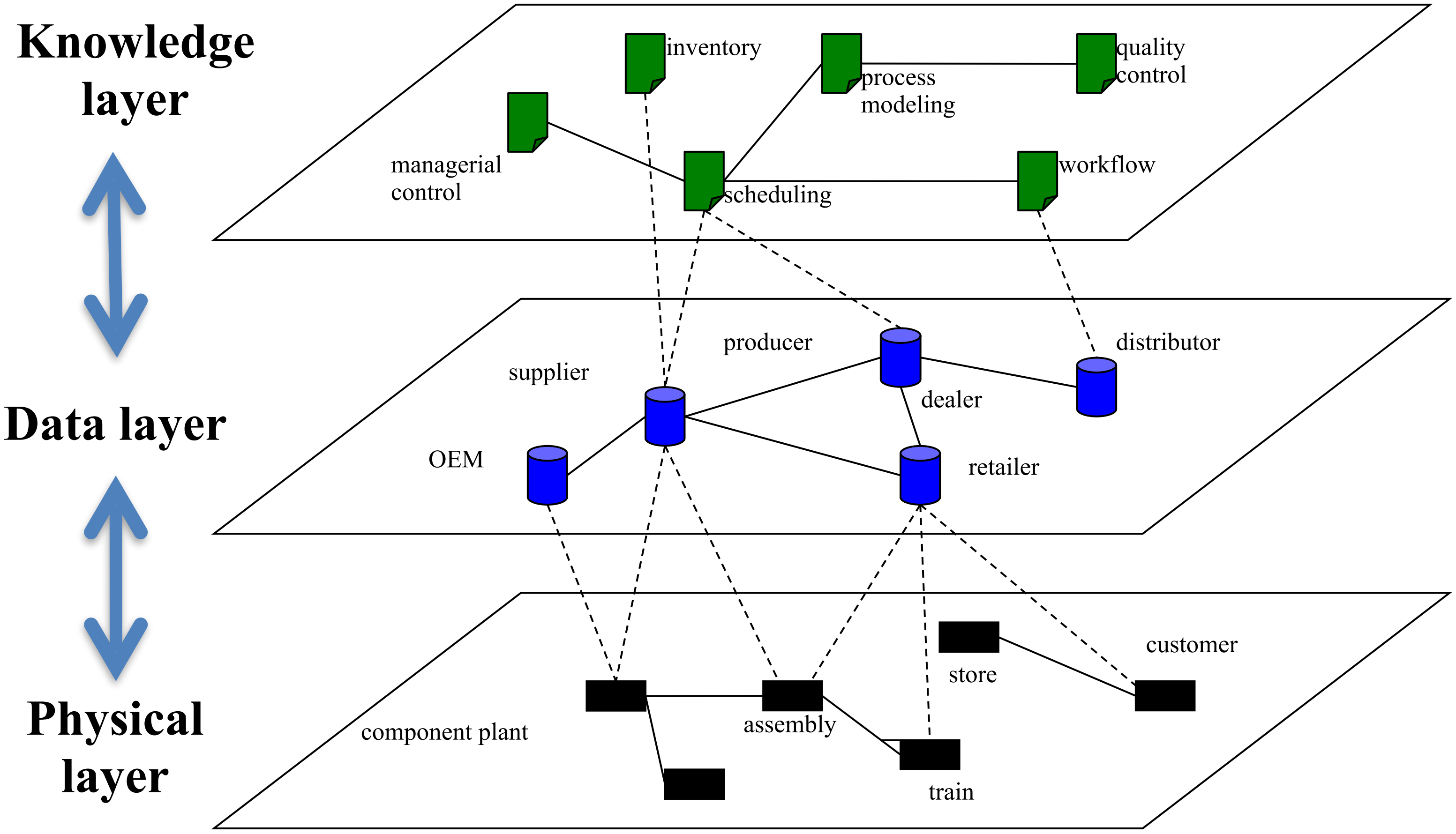
Acquire and Implement

Deliver and Support

Monitor and Evaluate

IT Life Cycle

Cyber Physical Systems



Outline

- Lifecycle of Information Assurance
- History of Intrusion Detection
- IDS Architecture

History of Intrusion Detection

1

Audit

2

Birth of Intrusion Detection

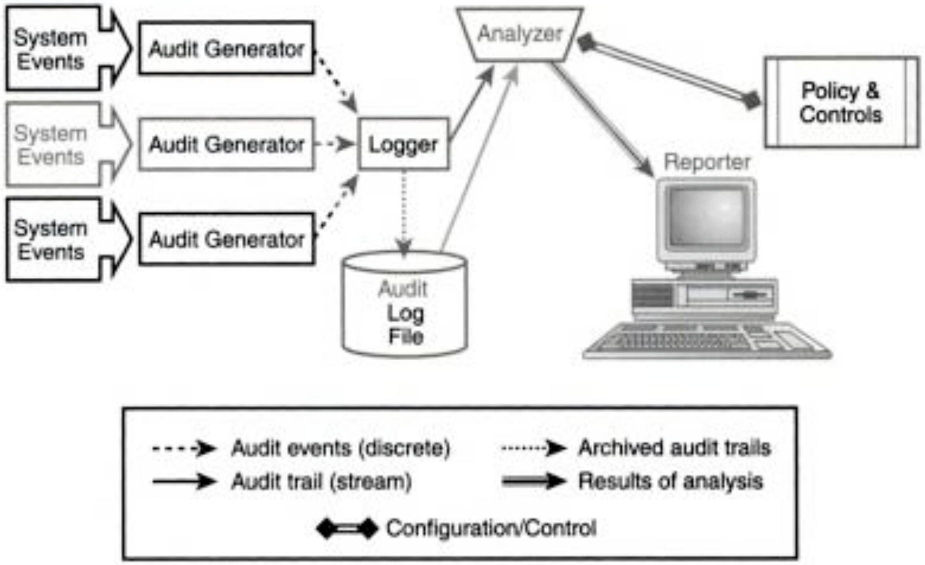
3

Intrusion Detection Systems

Audit Requirement

- “The process of generating, recording, and reviewing a chronological record of systems events.” (Bace, 2000)
  - Personal accountability
  - Reconstruct events
  - Assess damage
  - Monitor problems and control
  - Effective damage recovery
  - Deter improper behavior

Figure 1.1 Basic Audit System



(Bace, 2000)

Management and Security Audit

- Financial and management audit
  - Transaction traces to be presented in a summary
  - Deterministic
  - Chronological order
- Security audit
  - Different
  - Metrics not clearly/sufficiently defined
  - Security of security audit

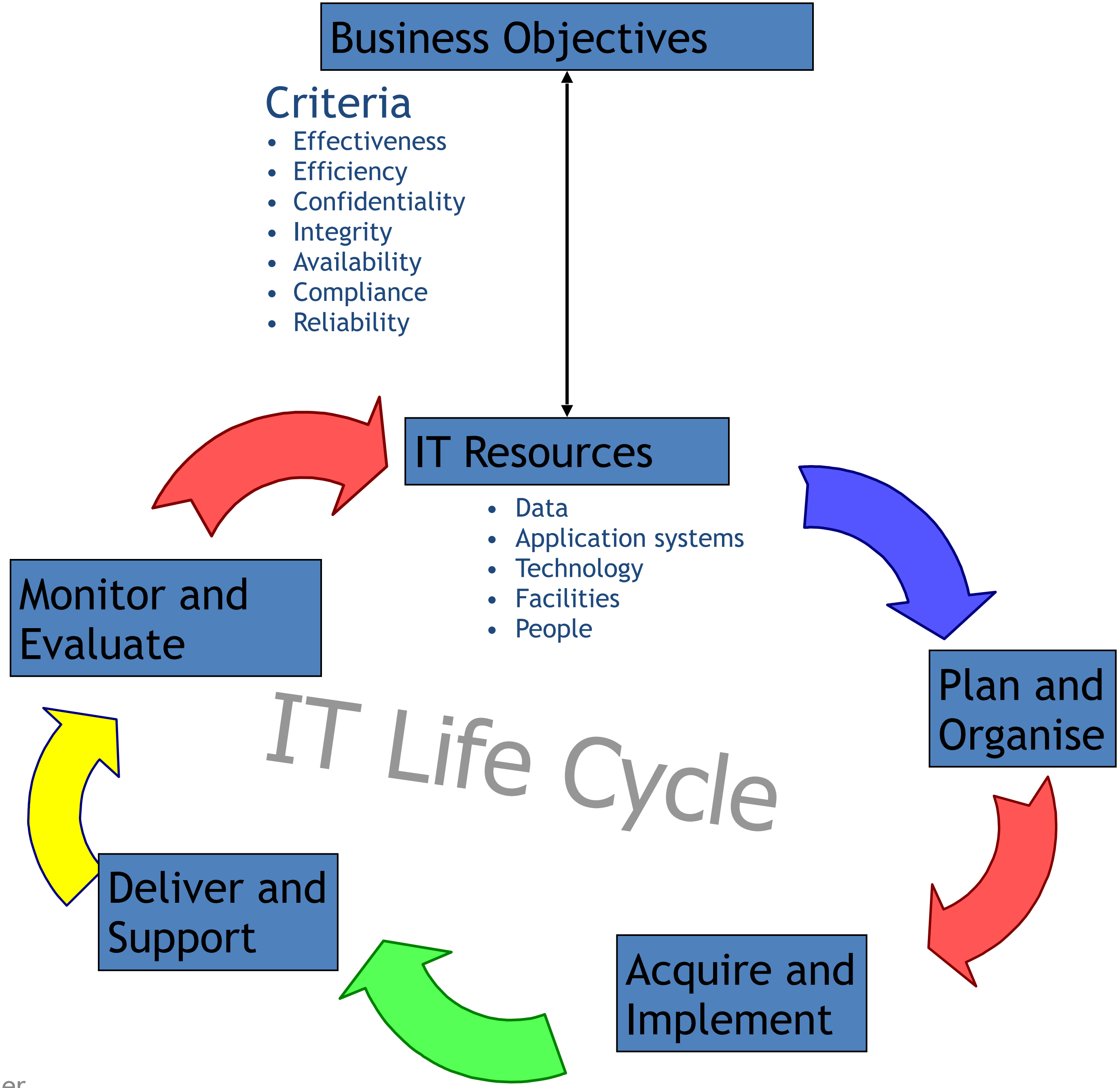
Use of Audit for Computer Management

- Manage user transactions and accounting
- Better computer usage
  - Utilization analysis
  - Resource allocation
- Security
  - Proper use
  - Sensitive information
  - Manual review

Audit and IT Governance

- Audit is an important part of IT management.
- IT compliance requirements
  - e.g., SOX act
- IT governance frameworks
  - e.g. Cobit by IT Governance Institute

COBIT Framework



Business Objectives

Criteria

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Resources

- Data
- Application systems
- Technology
- Facilities
- People

Plan and Organise

Acquire and Implement

Deliver and Support

Monitor and Evaluate

IT Life Cycle

EDP and Early Computer Security

- The first study at Bell Telephone System for audit need in future use of computers in telephone business in mid-1950s.
- Concern of audit “around the machine” not “through the machine.”
- Need of better audit capability for computer security.

Security Audit in Military and Government

- Study for security policies, guidelines, and controls for operating “trusted systems” in 1970s
  - Audit mechanism included for level C2 and above in the Trusted Computer System Evaluation Criteria
  - Five security goals in A Guide to Understanding Audit in Trusted Systems

Need for Audit Reduction

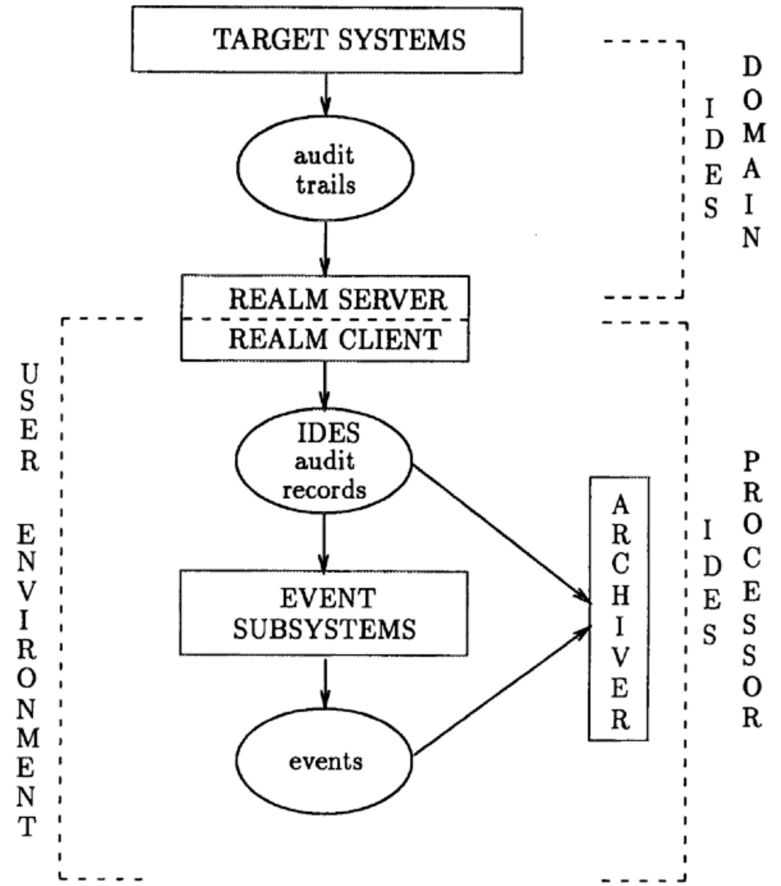
- As the speed, size, and number of computers grow, it is impossible to implement manual review of audit trails.
  - In addition, missing and superfluous information
- Anderson’s report in 1980 presented a classification of risks and threats to computer systems, and goals for security audit.
  - Internal/external user
  - Authorization of access to resources

Anderson’s Threat Matrix

	Not authorized to use data/program	Authorized to use data/program
Not authorized to use computer	Case A: External	
Authorized to use computer	Case B: Internal	Case C: Misfeasance

Real-time IDS

- IN 1987, D. Denning published the seminal work “An Intrusion Detection Model.”
  - “Profile”-based model
  - Statistical metrics to evaluate user behavior
- IDES by Denning and Neumann
  - The first prototype developed by SRI
  - Together with a rule-based expert system


TARGET SYSTEMS
audit trails
REALM SERVER
REALM CLIENT
IDES audit records
EVENT SUBSYSTEMS
events
ARCHIVER
IDES DOMAIN
IDES PROCESSOR
USER ENVIRONMENT

More IDSs

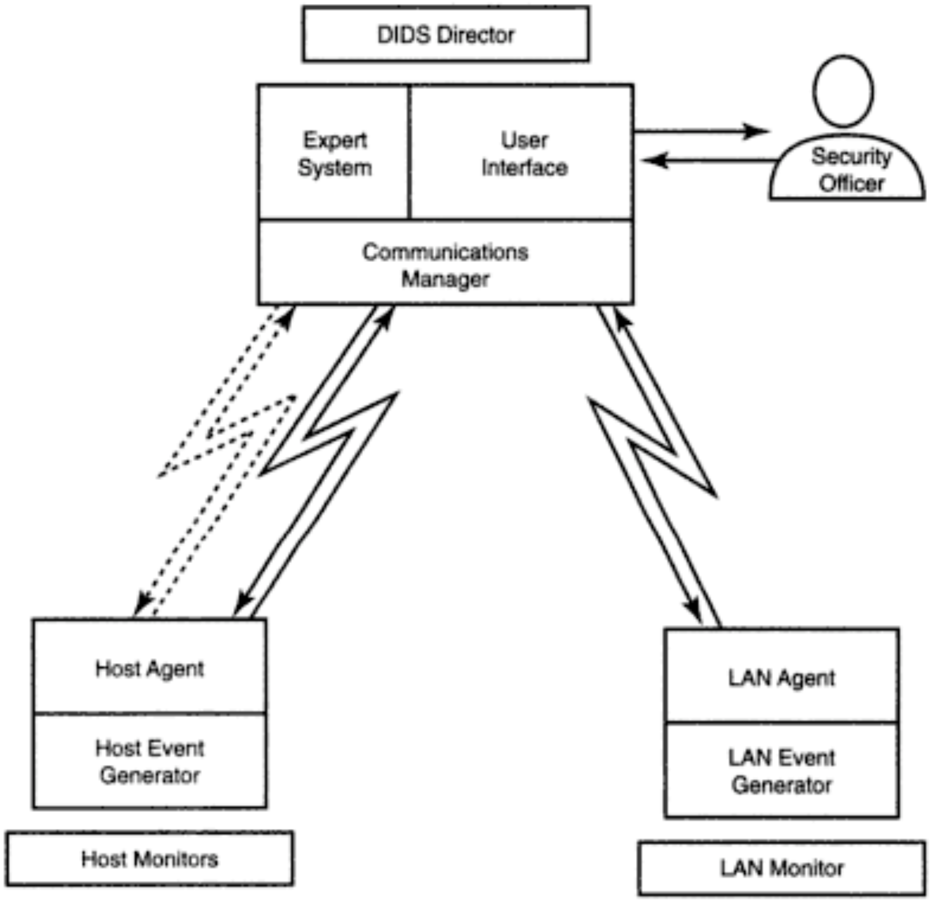
- Audit Analysis Project – database analysis of abnormal use
- Discovery – database-targeted analysis
- Haystack –anomaly detection in batch mode
- MIDAS (Multics Intrusion Detection and Alerting System) – anomaly detection and rule-based expert system
- Wisdom and Sense – statistical learning to generate rules

Network-based IDSs

- NADIR (Network Anomaly Detection and Intrusion Reporter) – combination of rule-based analysis and statistical analysis
- NSM (Network Security Monitor) – anomaly detection on network traffic
- Bro – packet analysis of libpcap data
- GrIDS (Graph-Based Intrusion Detection System) – intrusion detection helped by activity graphs of network hosts and activities

Integration of Host and Network-Based IDS

DIDS Architecture

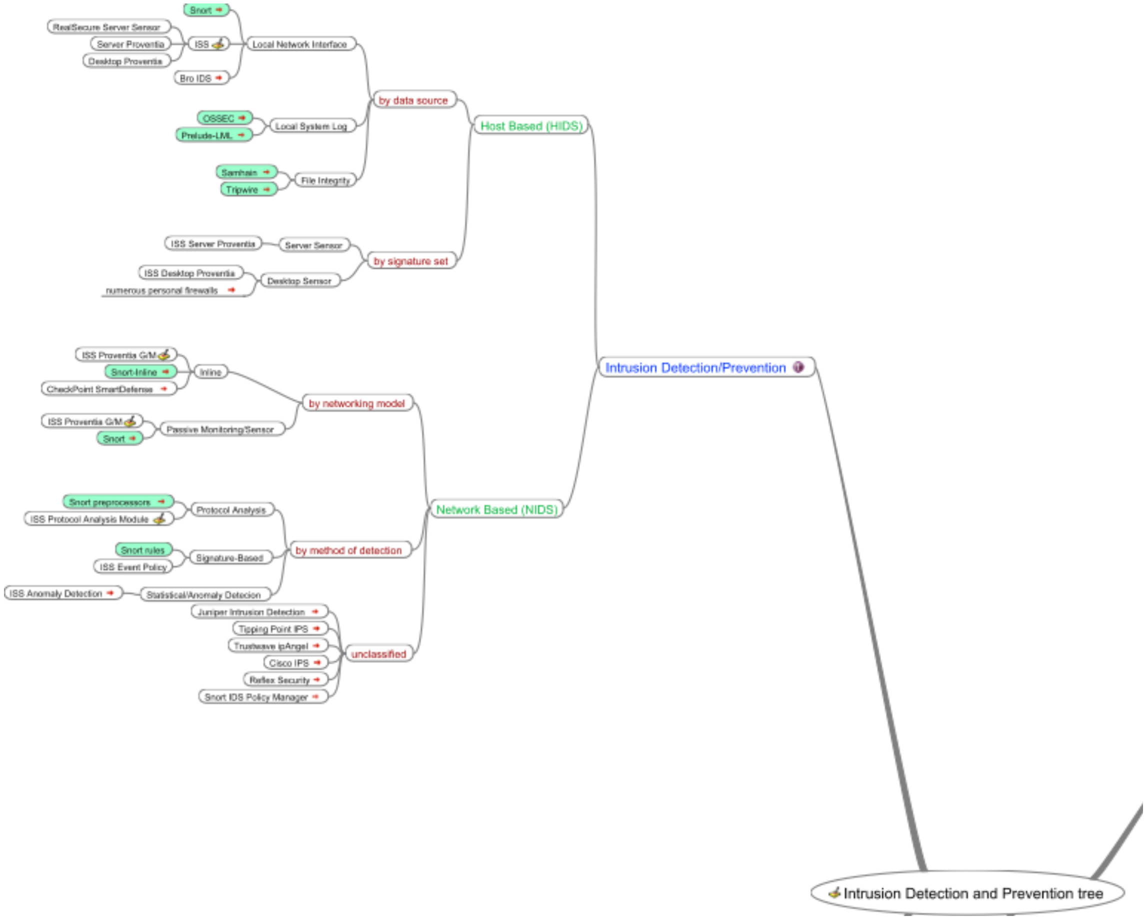


Commercial Systems

- ComputerWatch by AT&T
- ISOA by PRC, Inc.
- Clyde VAX Audit by Clyde Digital (Axent bought by Symantec)
- Symantec Intruder Alert (ITA) is the host-based IDS part of security suite that also includes network IDS (NetProwler), vulnerability assessment (NetRecon), and security policy auditing and enforcement (Enterprise Security Manager). (*Terminated in 2008*)

ID Resources and IDS Lists

- Michael Sobirey's Intrusion Detection Page (list of 92 IDSs)
- Open Directory for IDS
- Top 5 Intrusion Detection Systems (a 2006 survey Insecure.Org)
- Many online resources



Adapted from http://ipsec.pl/intrusion-detection/prevention-systems-classification-tree.html

A Definition

- NIST describes intrusion detection as "*the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network.*" *(Bace and Mell, 2001)*

Outline

Lifecycle of Information Assurance

History of Intrusion Detection

IDS Architecture

Common Intrusion Detection Procedures

1. Set-up and Training
2. System Monitoring and Data Collection
3. Analysis
4. Alarm/Report
5. Response

IDS Architecture

- Basically, a sophisticated audit system
  - *Agent* like logger; it gathers data for analysis
  - *Director* like analyzer; it analyzes data obtained from the agents according to its internal rules
  - *Notifier* obtains results from director, and takes some action
    - May simply notify security officer
    - May reconfigure agents, director to alter collection, analysis methods
    - May activate response mechanism

Agents

- Obtains information and sends to director
- May put information into another form
  - Preprocessing of records to extract relevant parts
- May delete unneeded information
- Director may request agent send other information

Example

- IDS uses failed login attempts in its analysis
- Agent scans login log every 5 minutes, sends director for each new login attempt:
  - Time of failed login
  - Account name and entered password
- Director requests all records of login (failed or not) for particular user
  - Suspecting a brute-force cracking attempt

Host-Based Agent

- Obtain information from logs
  - May use many logs as sources
  - May be security-related or not
  - May be virtual logs if agent is part of the kernel
    - Very non-portable
- Agent generates its information
  - Scans information needed by IDS, turns it into equivalent of log record
  - Typically, check policy; may be very complex

Network-Based Agents

- Detects network-oriented attacks
  - Denial of service attack introduced by flooding a network
- Monitor traffic for a large number of hosts
- Examine the contents of the traffic itself
- Agent must have same view of traffic as destination
  - TTL tricks, fragmentation may obscure this
- End-to-end encryption defeats content monitoring
  - Not traffic analysis, though

Network Issues

- Network architecture dictates agent placement
  - Ethernet or broadcast medium: one agent per subnet
  - Point-to-point medium: one agent per connection, or agent at distribution/routing point
- Focus is usually on intruders entering network
  - If few entry points, place network agents behind them
  - Does not help if inside attacks to be monitored

Aggregation of Information

- Agents produce information at multiple layers of abstraction
  - Application-monitoring agents provide one view (usually one line) of an event
  - System-monitoring agents provide a different view (usually many lines) of an event
  - Network-monitoring agents provide yet another view (involving many network packets) of an event

Director

- Reduces information from agents
  - Eliminates unnecessary, redundant records
- Analyzes remaining information to determine if attack under way
  - Analysis engine can use a number of techniques
  - Anomaly detection vs. misuse detection
- Usually run on separate system
  - Does not impact performance of monitored systems
  - Rules, profiles not available to ordinary users

Example

- Jane logs in to perform system maintenance during the day
- She logs in at night to write reports
- One night she begins recompiling the kernel
- Agent #1 reports logins and logouts
- Agent #2 reports commands executed
  - Neither agent spots discrepancy
  - Director correlates log, spots it at once

Adaptive Directors

Modify profiles, rulesets to adapt their analysis to changes in system

Usually use machine learning or planning to determine how to do this

Example: use neural nets to analyze logs

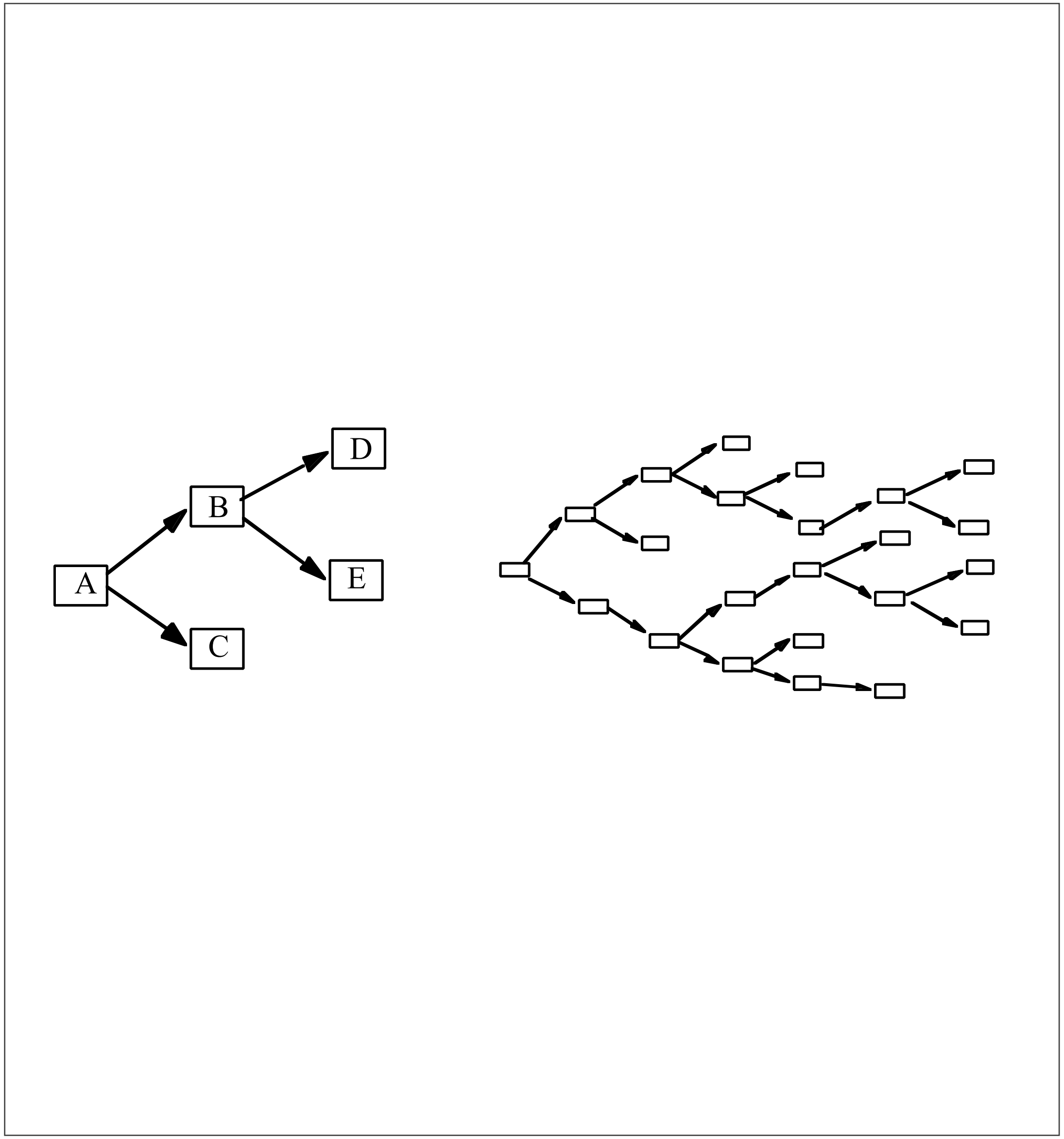
Network adapted to users’ behavior over time

Used learning techniques to improve classification of events as anomalous

- Reduced number of false alarms

Notifier

- Accepts information from director
- Takes appropriate action
  - Notify system security officer
  - Respond to attack
- Often GUIs
  - Well-designed ones use visualization to convey information



GrIDS GUI

- GrIDS interface showing the progress of a worm as it spreads through network
- Left is early in spread
- Right is later on

Other Examples

- Courtney detected SATAN attacks
  - Added notification to system log
  - Could be configured to send email or paging message to system administrator
- IDIP protocol coordinates IDSs to respond to attack
  - If an IDS detects attack over a network, notifies other IDSs on co-operative firewalls; they can then reject messages from the source