

Computer and Network Security

©Copyright 2000 R. E. Newman

Computer & Information Sciences & Engineering
University Of Florida
Gainesville, Florida 32611-6120
nemo@cise.ufl.edu

Network Security
(Pfleeger Ch. 9, KPS Ch. 12, 13, 17)

1 Network Basics

1.1 Network Types

1.1.1 LANs

- Bus
- Tree
- Star
- Ring
- Dual Bus

1.1.2 CWANs

1.1.3 MANs

1.1.4 WANs

- Circuit-Switched
- Virtual Circuit Packet-Switched
- Datagram Packet-Switched

1.1.5 internets

1.1.6 VPNs

1.1.7 Wireless

1.1.8 Satellite

1.2 ISO OSI Reference Network Architecture

1.2.1 General

- Reference Architecture
- Layered - Layer i only gets service from layer $i - 1$
- Peer layers
- International standard

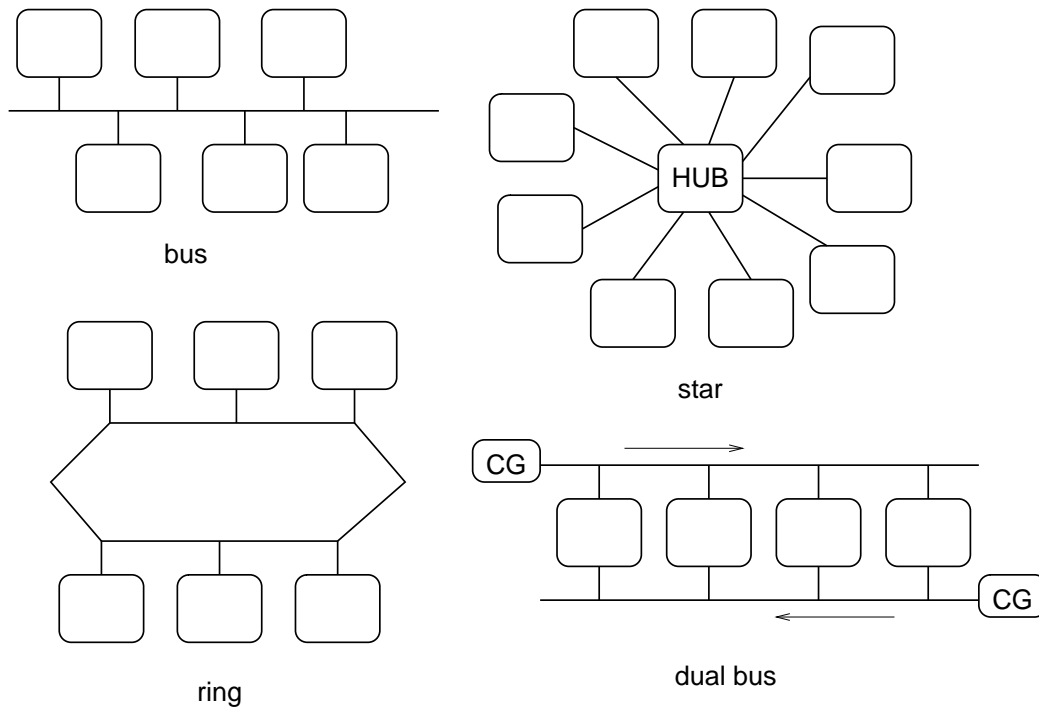


Figure 1: LAN topologies

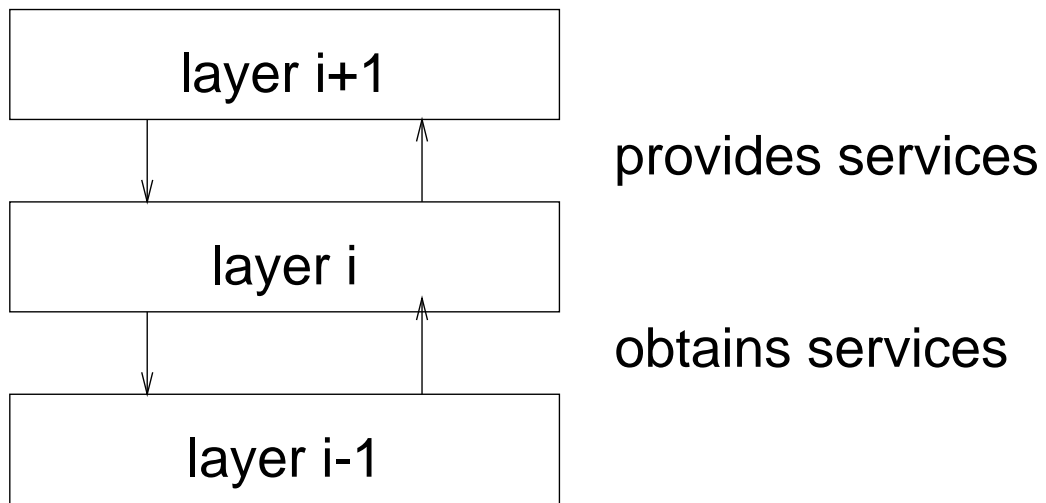


Figure 2: Layered architecture

1.2.2 Layers

1. Physical
2. DataLink
3. Network
4. Transport

5. Session
6. Presentation
7. Application
8. Financial
9. Political
10. Religious

OSI Reference Architecture Layers

7 - Application	- underlying OS security - interoperation - multiple applications
6- Presentation	- common formatting, utilities
5 - Session	- session management
4 - Transport	- end-to-end, process-to-process
3 - Network	- host identification only - per-packet OH if datagram service - higher level entities are treated same
2 - Link	- only useful for immediate neighbors
1 - Physical	- electrical, mechanical modulation/detection

Figure 3: OSI layers

- Chained layers
- End-to-end layers
- PDUs
- encapsulation

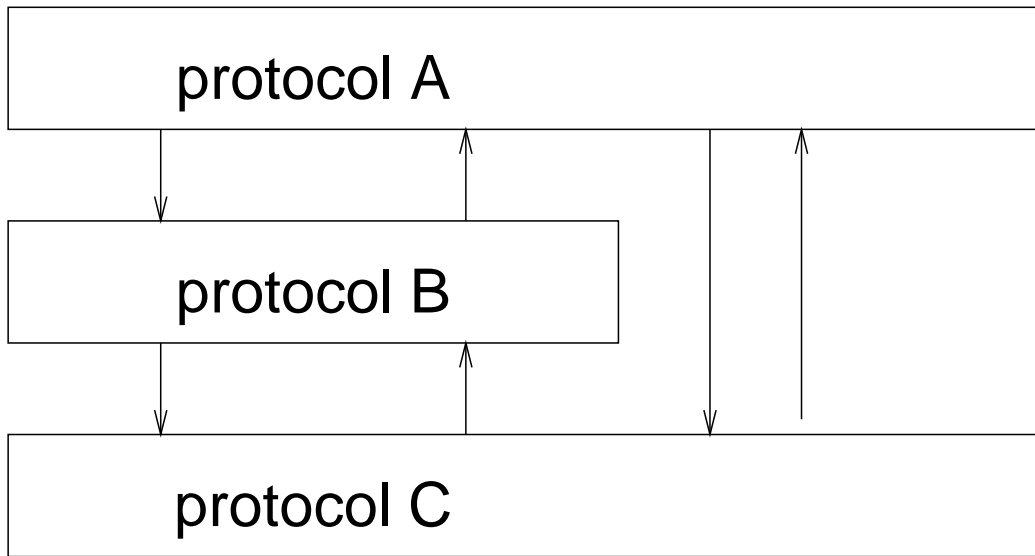


Figure 4: Hierarchical architecture

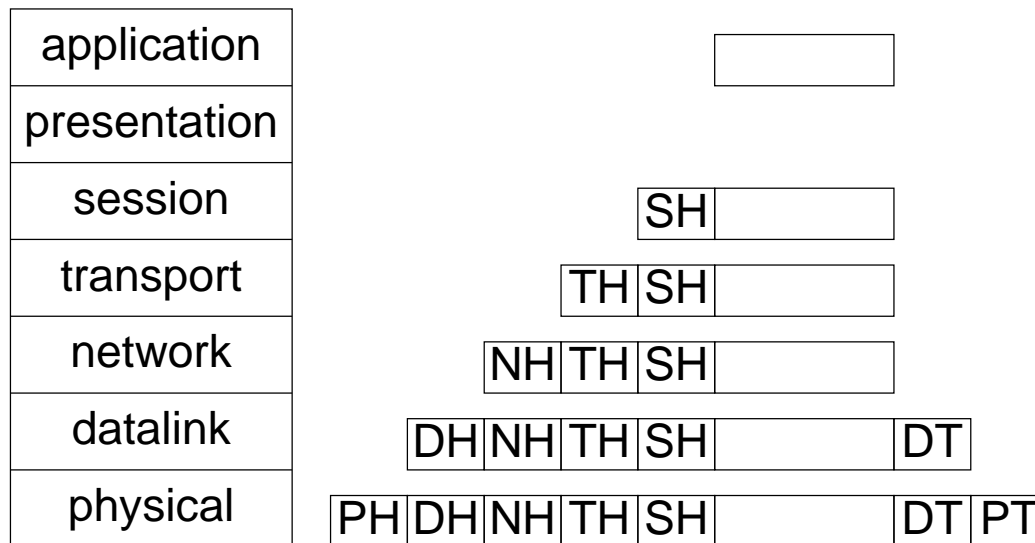


Figure 5: Encapsulation

1.3 TCP/IP

1.3.1 IP

1.3.2 ICMP

1.3.3 Routing

1.3.4 UDP

1.3.5 TCP

1.4 Addressing

1.4.1 Types of addressing

1. TSAPs

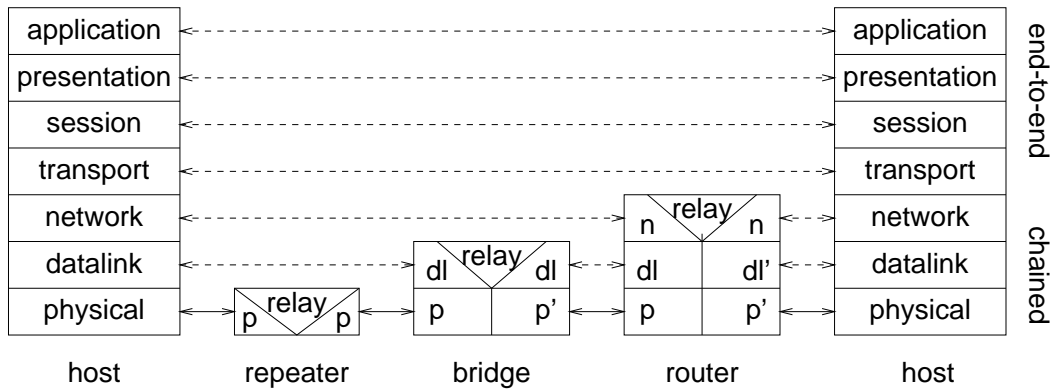


Figure 6: OSI network

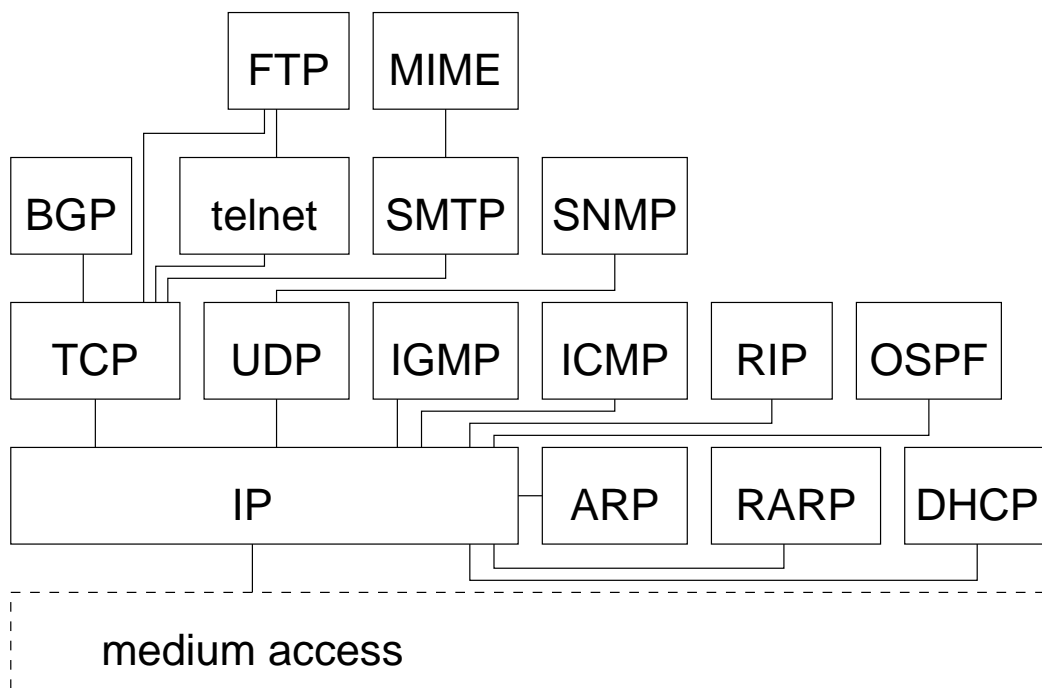


Figure 7: TCP/IP

2. NSAPs
3. LSAPs
4. PSAPs
5. Logical names

1.5 Network Devices

1.5.1 Repeater

1.5.2 Bridge

1.5.3 Router

1.5.4 Protocol Translator

1.5.5 Gateway

1.5.6 Address translation

1. ARP

2. RARP

3. DNS

4. portmapper

2 Network Security Issues

2.1 Sharing

2.2 Complexity

2.3 Perimeter

2.4 Points of Attack

2.5 Anonymity

2.6 Unknown Path

3 Network Threats

3.1 Eavesdropping

3.1.1 Cable

3.1.2 Microwave

3.1.3 Satellite

3.1.4 Optic Fiber

3.2 Other Message Confidentiality Violations

3.2.1 Misdelivery

3.2.2 Transient Exposure

3.2.3 Traffic Analysis

Source and Destination

- port
- host
- network interface
- network

Quantities

- load
- load changes
- window issues

- 3.3 Message Integrity Violations
 - 3.3.1 Noise
 - 3.3.2 Fabrication
 - 3.3.3 Replay
 - 3.3.4 Cut & Paste
 - 3.3.5 Modification
 - 3.3.6 Replacement
 - 3.3.7 Redirection
 - 3.3.8 Delay
 - 3.3.9 Destruction
- 3.4 Spoofing
 - 3.4.1 no authentication (lunacy)
 - 3.4.2 authentication by source address (trust relationships)
 - 3.4.3 guessed authentication information (weak passwords)
 - 3.4.4 sniffed authentication information (weak authentication)
 - 3.4.5 well-known authentication (trapdoor)
- 3.5 Other Message Authenticity Violations
 - 3.5.1 repudiation
 - 3.5.2 denial of receipt
- 3.6 Mobile Code
 - 3.6.1 Java
 - 3.6.2 Active-X
 - 3.6.3 web browsers
 - 3.6.4 AOL
- 3.7 Denial of Service
 - 3.7.1 connectivity
 - 3.7.2 network flooding
 - 3.7.3 spamming
 - 3.7.4 redirection
 - 3.7.5 port hammering
 - 3.7.6 syn attack
 - 3.7.7 memory exhaustion
 - 3.7.8 disk exhaustion
 - 3.7.9 service exhaustion
 - 3.7.10 winnuke
 - 3.7.11 buffer overflow/crash
- 4 Network Controls
 - 4.1 Encryption
 - 4.1.1 Protocol Layer
 1. application
 2. transport/network

3. link

4.2 Access Control

4.2.1 policy routing

4.2.2 port protection

4.2.3 auto callback

4.2.4 differential access rights

4.2.5 group membership

4.2.6 CORBA

4.3 Authentication

4.3.1 DEC authentication architecture

4.3.2 Kerberos

4.3.3 DCE

4.3.4 Sesame

4.3.5 CORBA

4.4 Traffic Control

4.4.1 Routing

1. Policy routing
2. Dynamic routing
3. Rerouting
4. Onion routing
5. Chaum mixes

4.4.2 Padding

4.4.3 Delay

4.5 Data Integrity

4.5.1 Protocols

4.5.2 Error Handling

1. Forward Error Correction
2. Error Correction Codes
3. Backward Error Correction
4. Error Detection Codes
5. MACs and MICs
6. Notarization

4.6 Intrusion Detection

4.6.1 Detector Source Information

1. Packets
2. Host events
3. N/W state
4. Host state

4.6.2 Anomaly Detection

1. Statistical
2. AI
3. Neural Nets
4. Formal Languages

4.6.3 Misuse Detection

1. signatures
2. expert systems

4.6.4 Response

1. notify security team
2. log events
3. reconfigure controls
4. reconfigure system

5 Multilevel Networks

5.1 Trusted Network Interpretation (Red Book)

Interprets TCSEC for networks

5.2 Trusted Network Interface

5.2.1 Trusted Hosts (MLS)

5.2.2 Untrusted Hosts (MSL)

5.2.3 Labeled output

5.2.4 classification check before release

5.2.5 data integrity

5.2.6 label integrity

5.2.7 confinement

5.2.8 protection from link compromise

5.3 Secure Communication

5.3.1 write down for ACKs

5.3.2 Waller - TNI + Trusted host

5.3.3 NRL pump

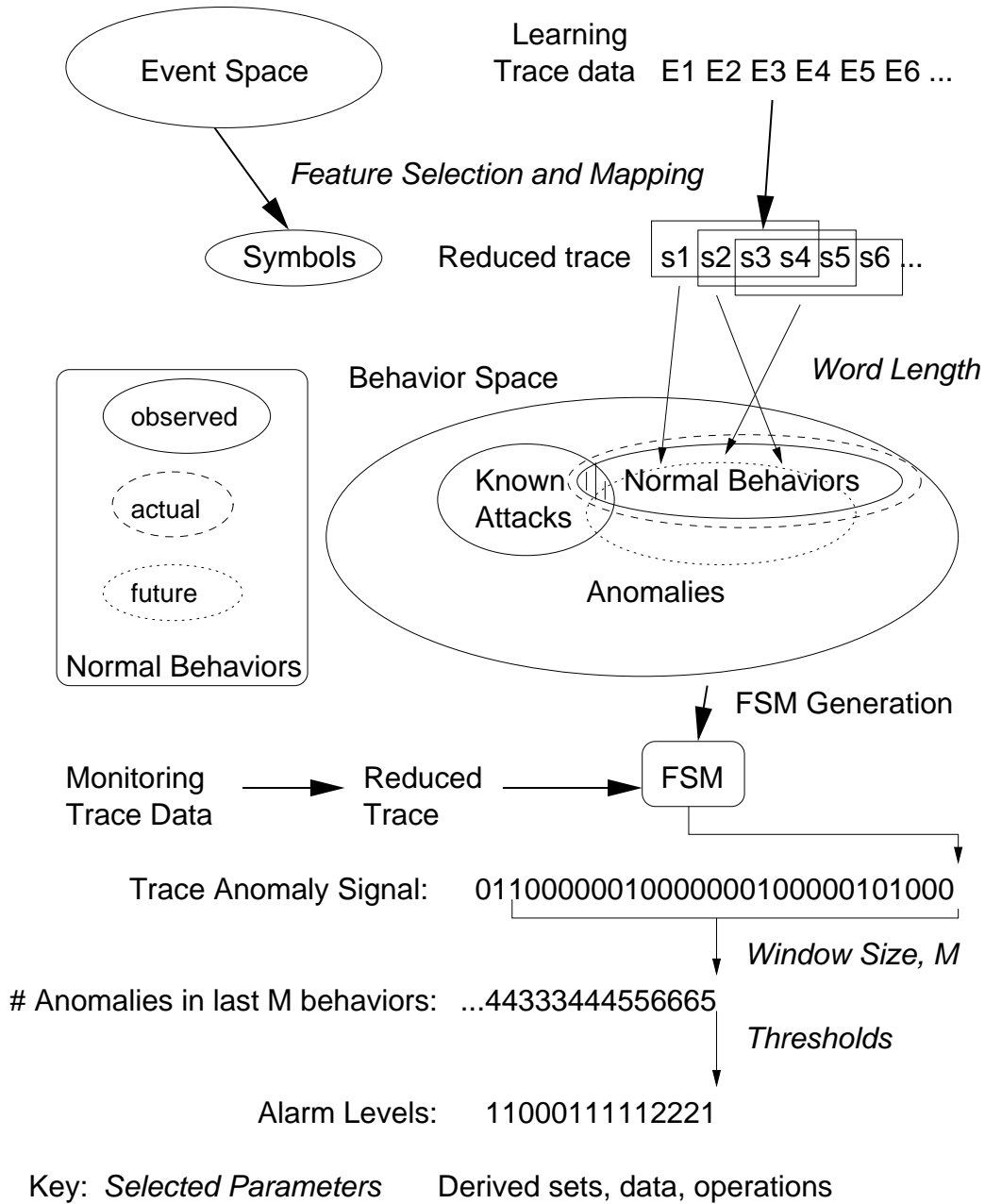
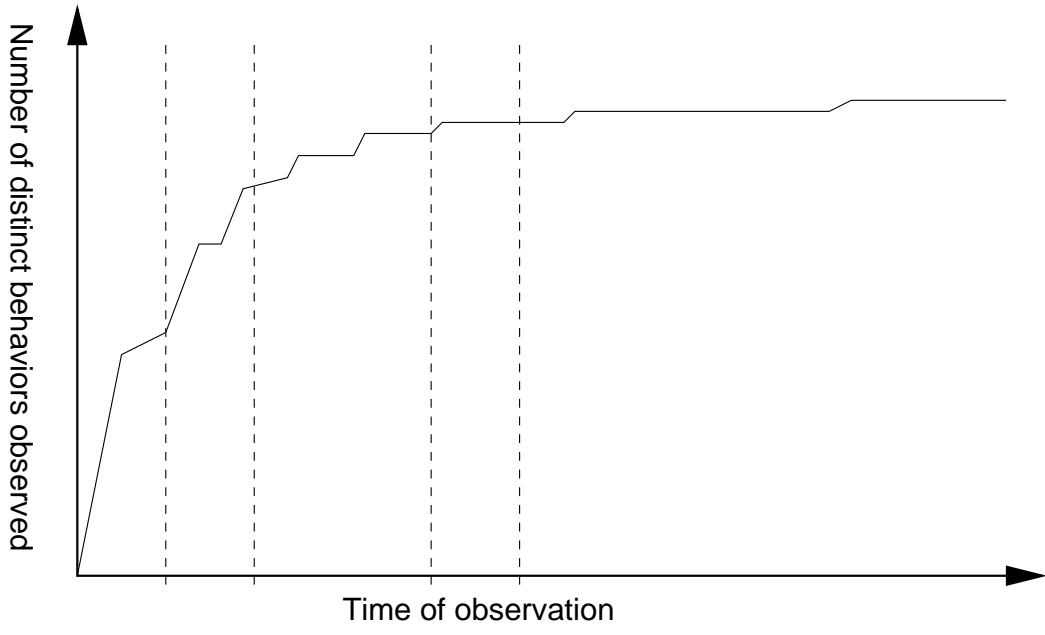


Figure 8: A Formal Language-based Anomaly Detection Model



Learning what is normal

Figure 9: Learning Normal

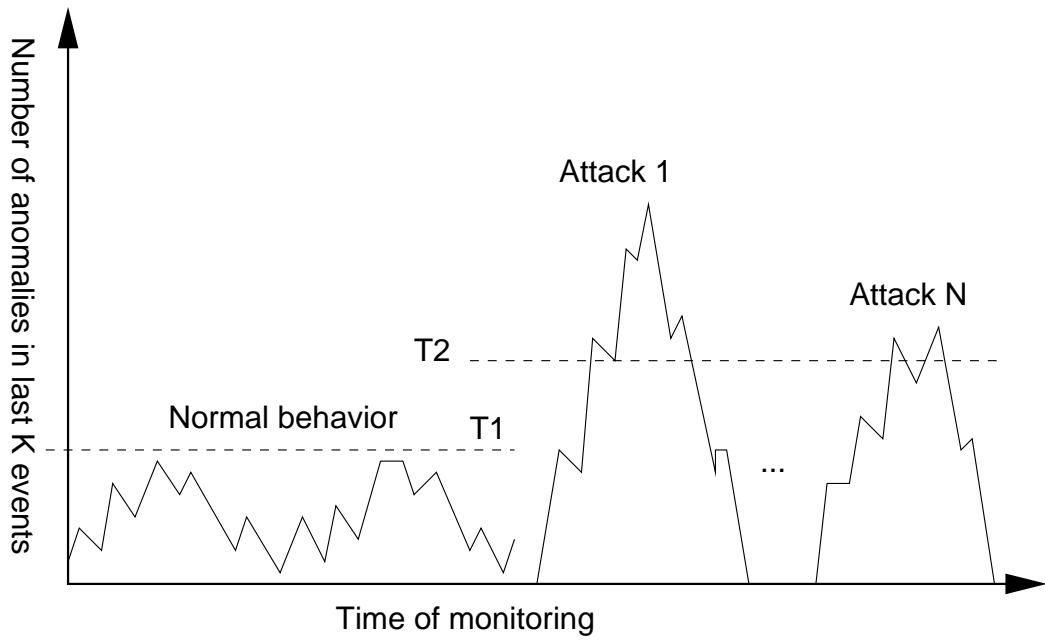


Figure 10: Setting Thresholds

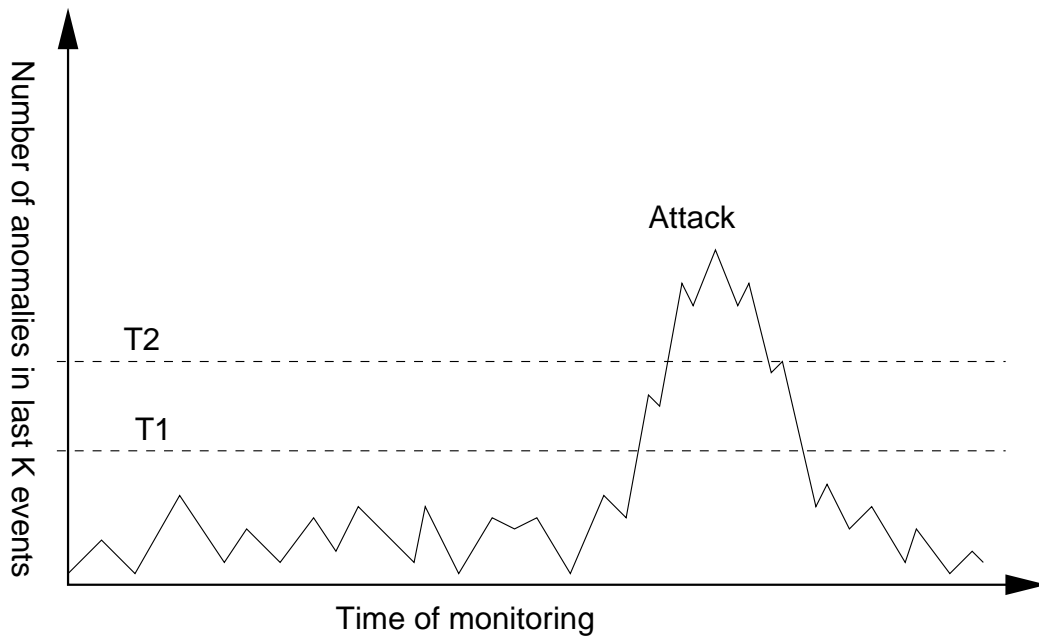


Figure 11: Running the anomaly detector