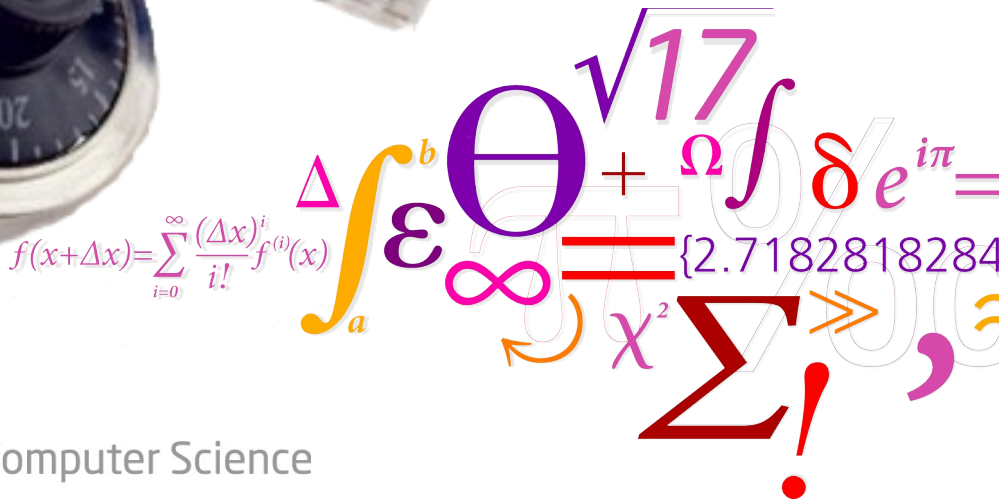
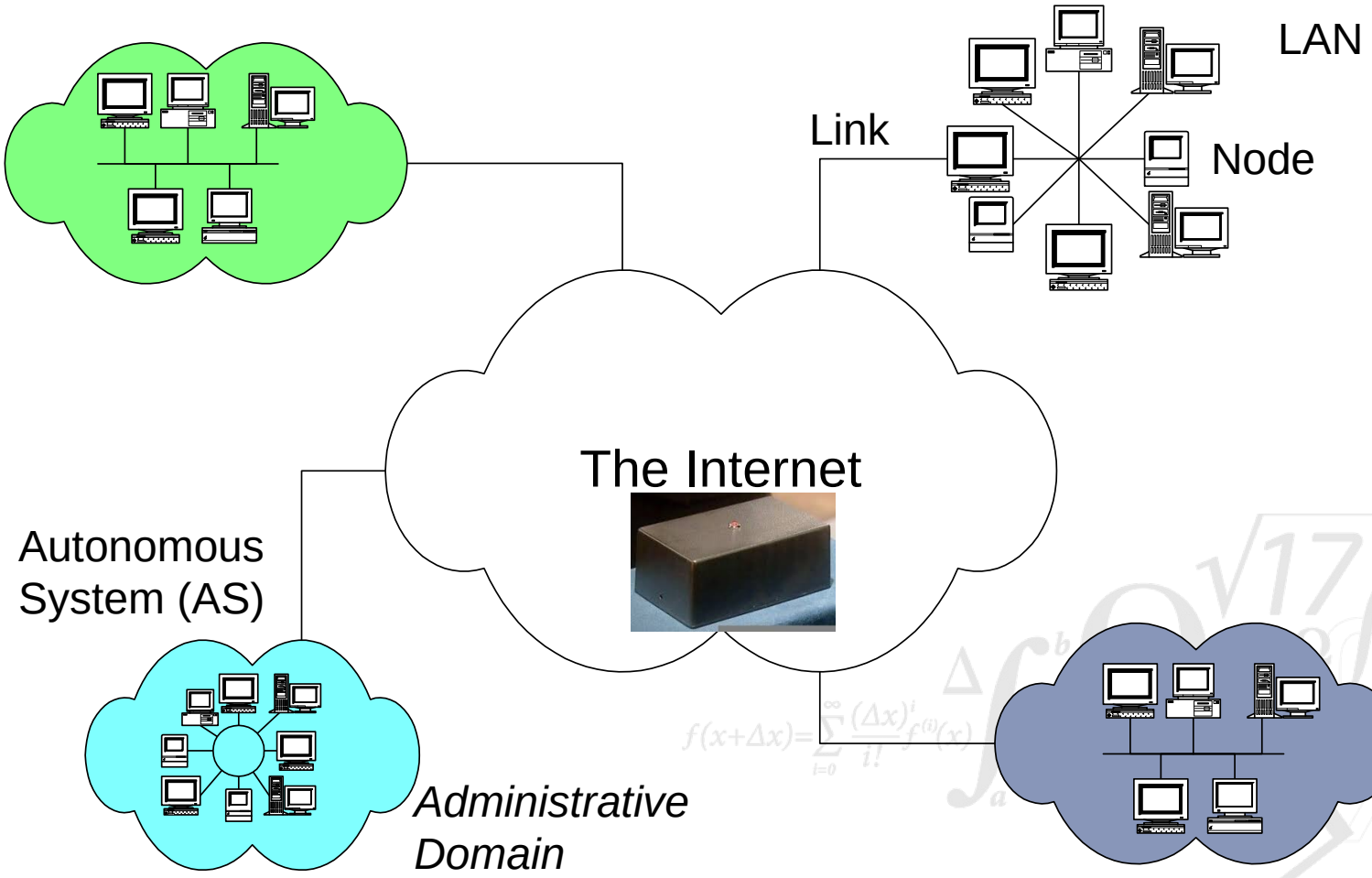
Security in Networks



DTU Compute
Department of Applied Mathematics and Computer Science

Network Definitions



Network Characteristics

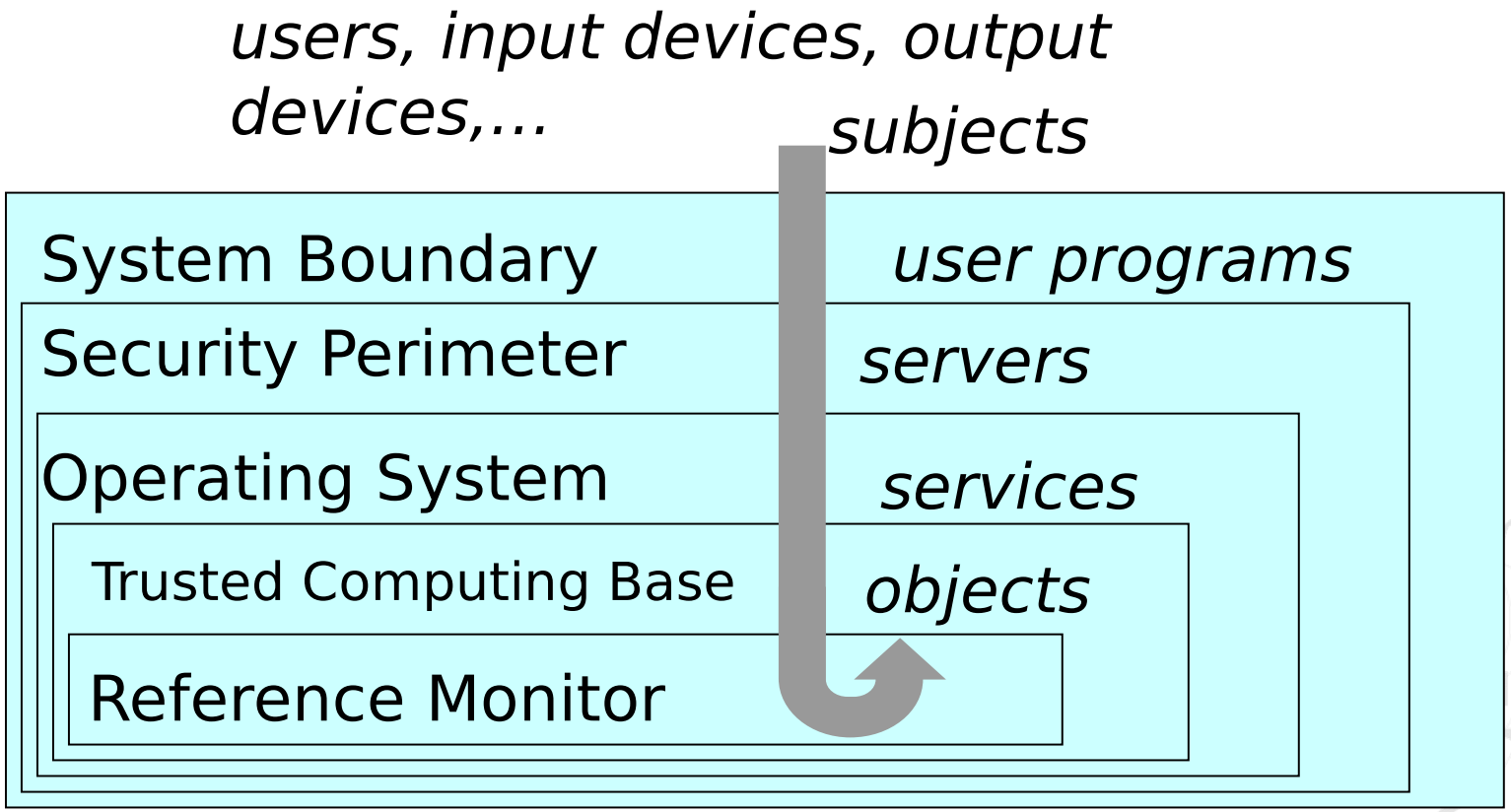
- Networks are defined by:
  - Boundary
    Distinguishes nodes inside the network from nodes outside the network. It is theoretically possible to make a list of all components belonging to the network
  - Ownership (Autonomous System/Administrative Domain)
    Nodes belonging to the same owner and managed by the same administrators. Ownership is sometimes difficult to determine, e.g., who owns the Internet?
  - Control (physical security)
    Not all nodes belonging to the network are under control of the administrator, e.g., your own laptop connected to DTU's wireless network, Bring Your Own Device (BYOD) in many companies.

Types of Networks

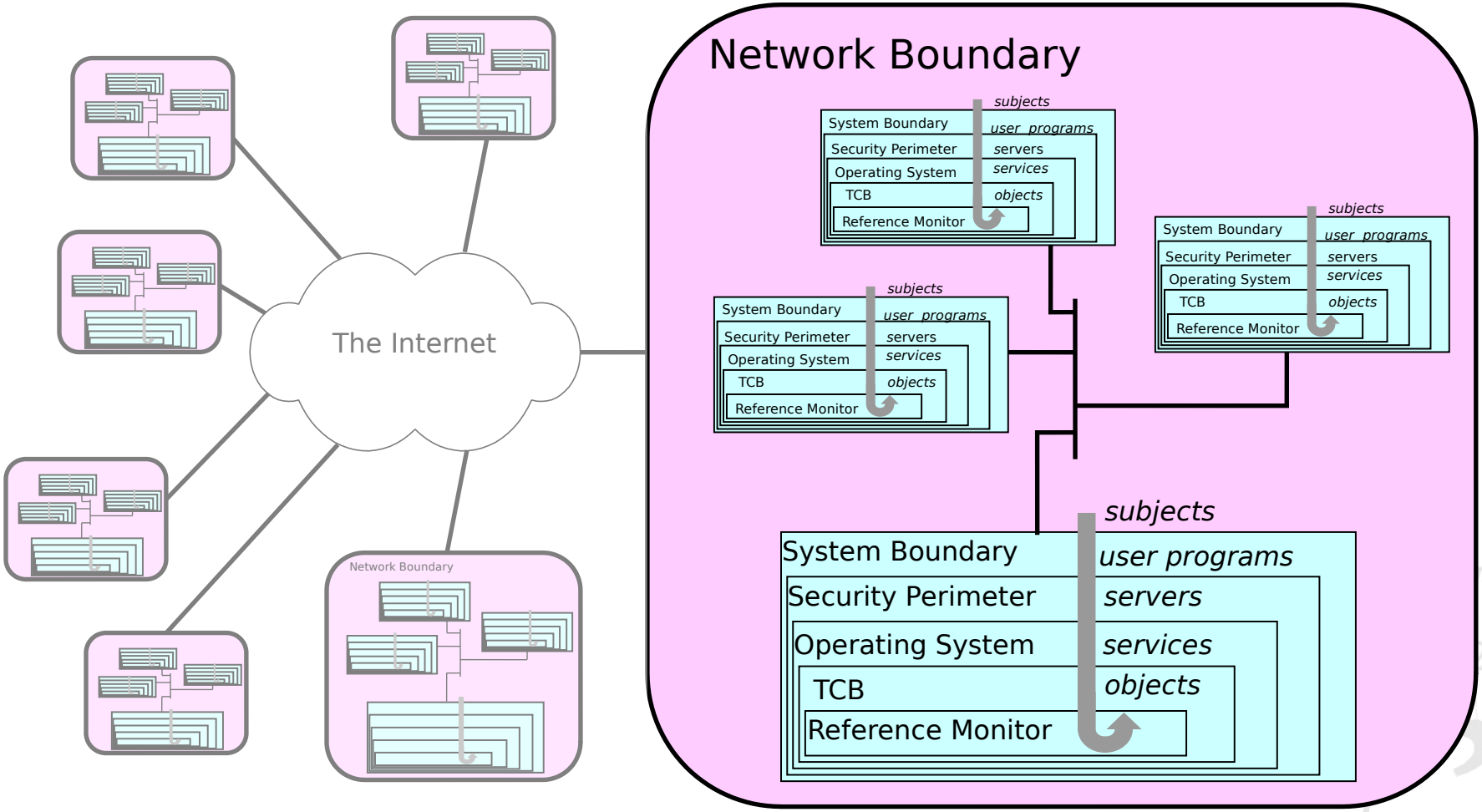
- 2 types of networks:
  - Shared medium (Bus, Token Ring, Mesh, …)
  - Point-to-point networks
- Classification based on diameter (reach):

1 m	System	Multi-processor
10 m	Room	Device connection, Body Area Networks
100 m	Building	LAN
1 km	Campus	
10 km	City	Metropolitan Area Network (MAN)
100 km	Country	WAN
1,000 km	Continent	
10,000 km	Planet	The Internet

Stand Alone Systems



Networked Systems



Network Vulnerabilities

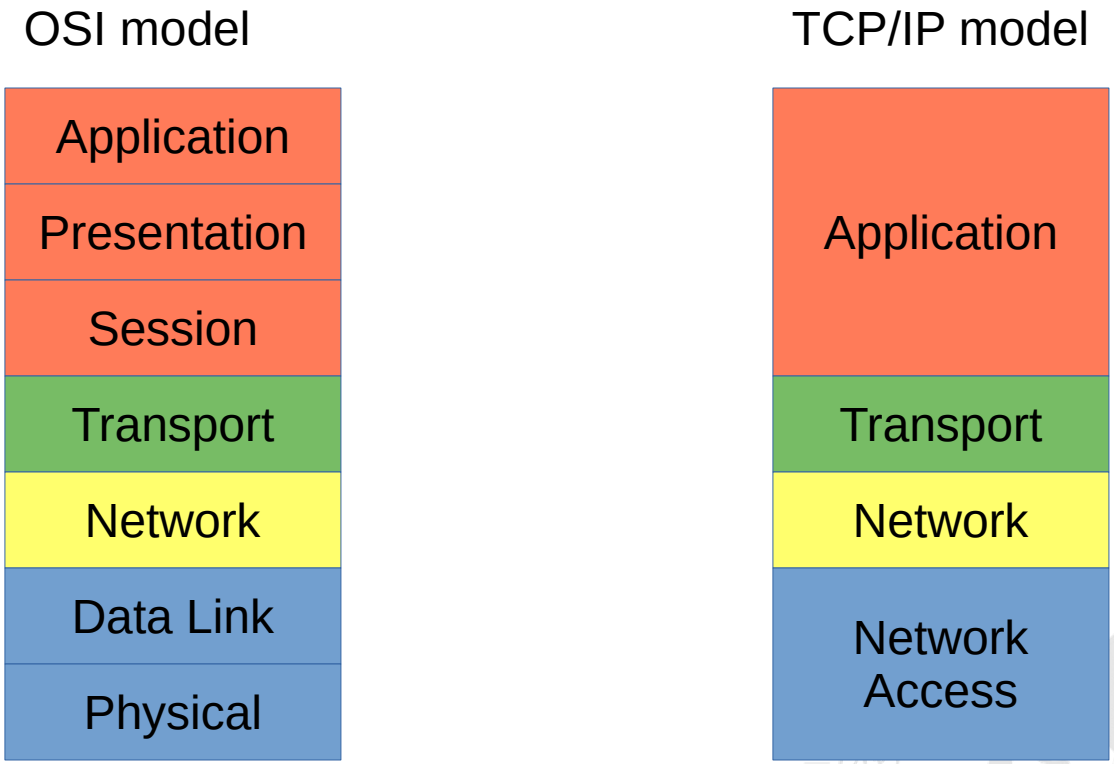
- Programming mistakes
  - Public services must handle active and passive data from untrusted sources
    - *Buffer overflows, malicious applets, …*
- Protocol Flaws
  - Internet was designed for a few hundred trusted computers
    - *This is evident in the lack of security in many protocols (SMTP)*
  - Protocols are often complex and specifications are ambigous
- Misconfiguration of software and systems
  - Complexity of systems and focus on functional requirements (short deadlines) leads to misconfigured systems
- Unpatched software
  - Vendors normally issue patches when vulnerabilities are exposed, responsibility of customers to apply patches

Communication Security

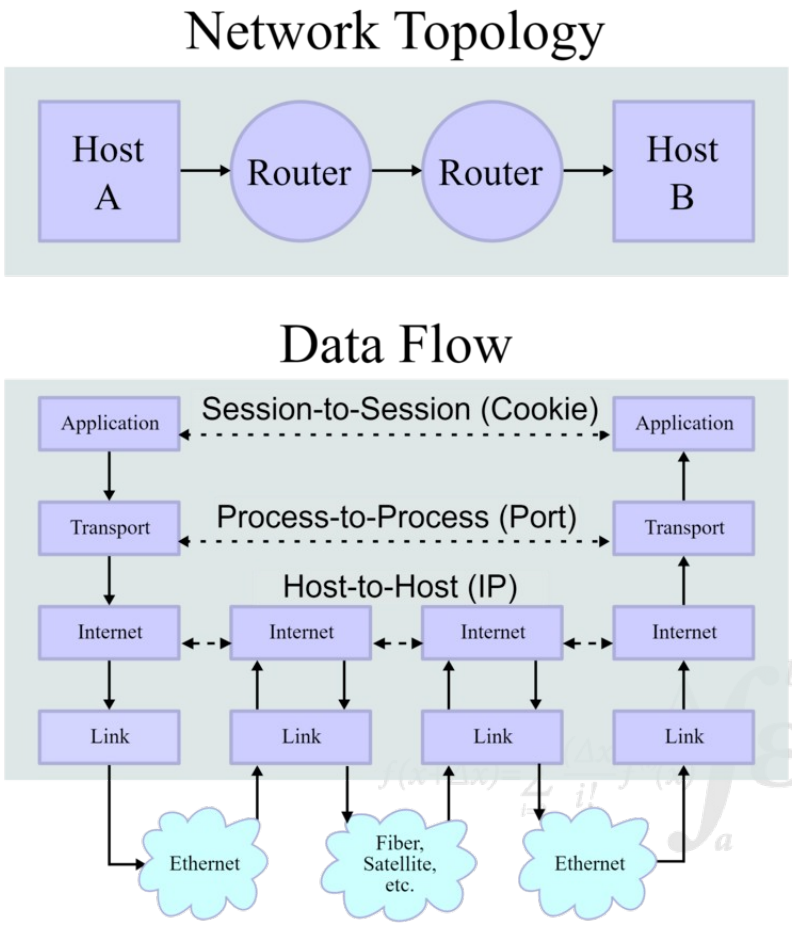
- Secure Routing
  - Finding communications paths between nodes on the network
    - *Network Layer protocols (OSI level 3, host configuration and network management)*
      - Many protocols are involved here (ARP, DHCP, DNS, ICMP, CIDR, BGP, …)
  - Connecting to a secure network
    - *Mutual authentication between nodes and network*
  - Maintaining routing information (reactive or proactive protocols)
    - *Routing tables between networks can be corrupted, e.g. by BGP high-jacking attacks*

- Secure communication
  - Protecting the contents of the communication

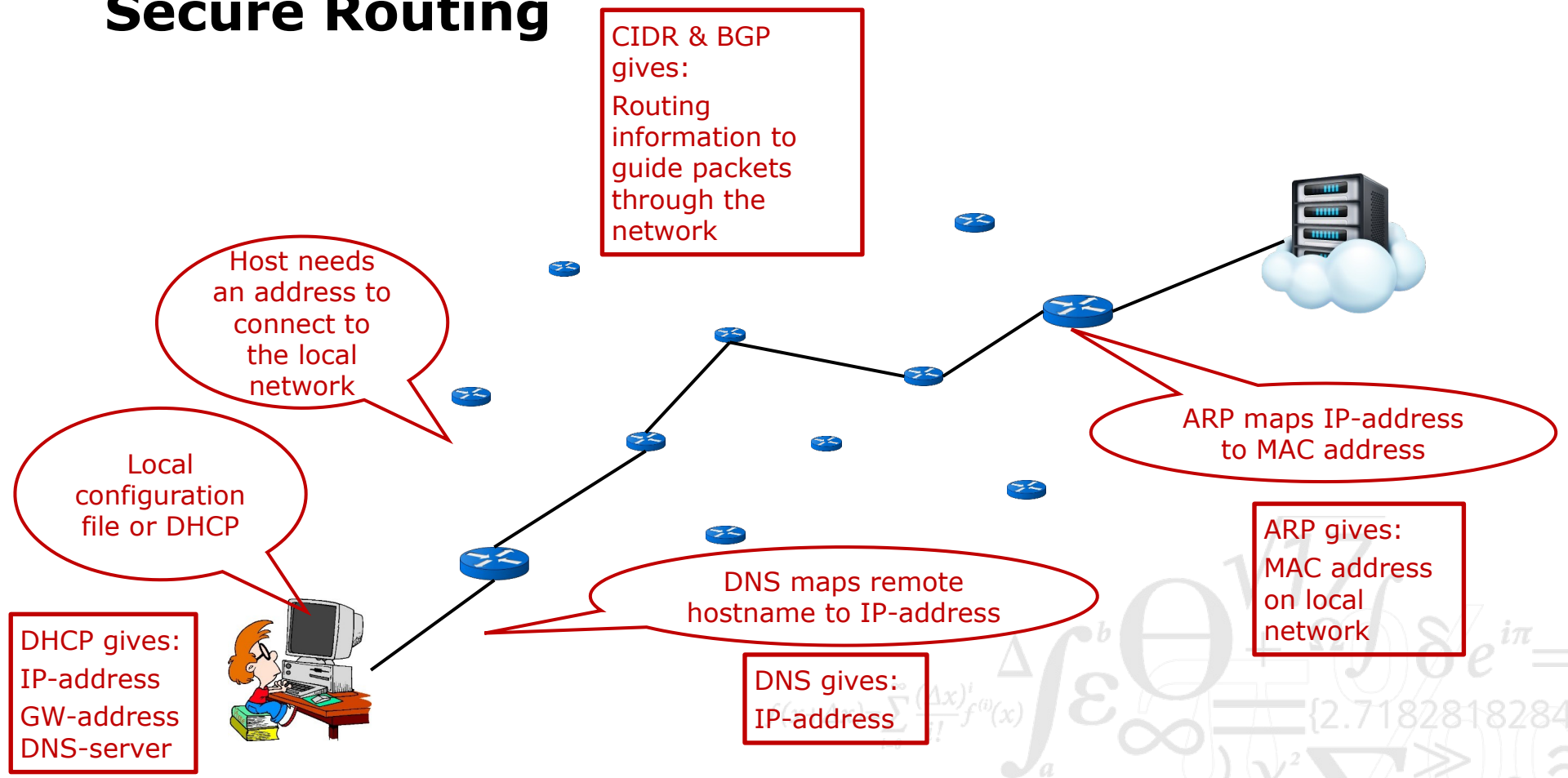
OSI model and TCP/IP model



Communication Security



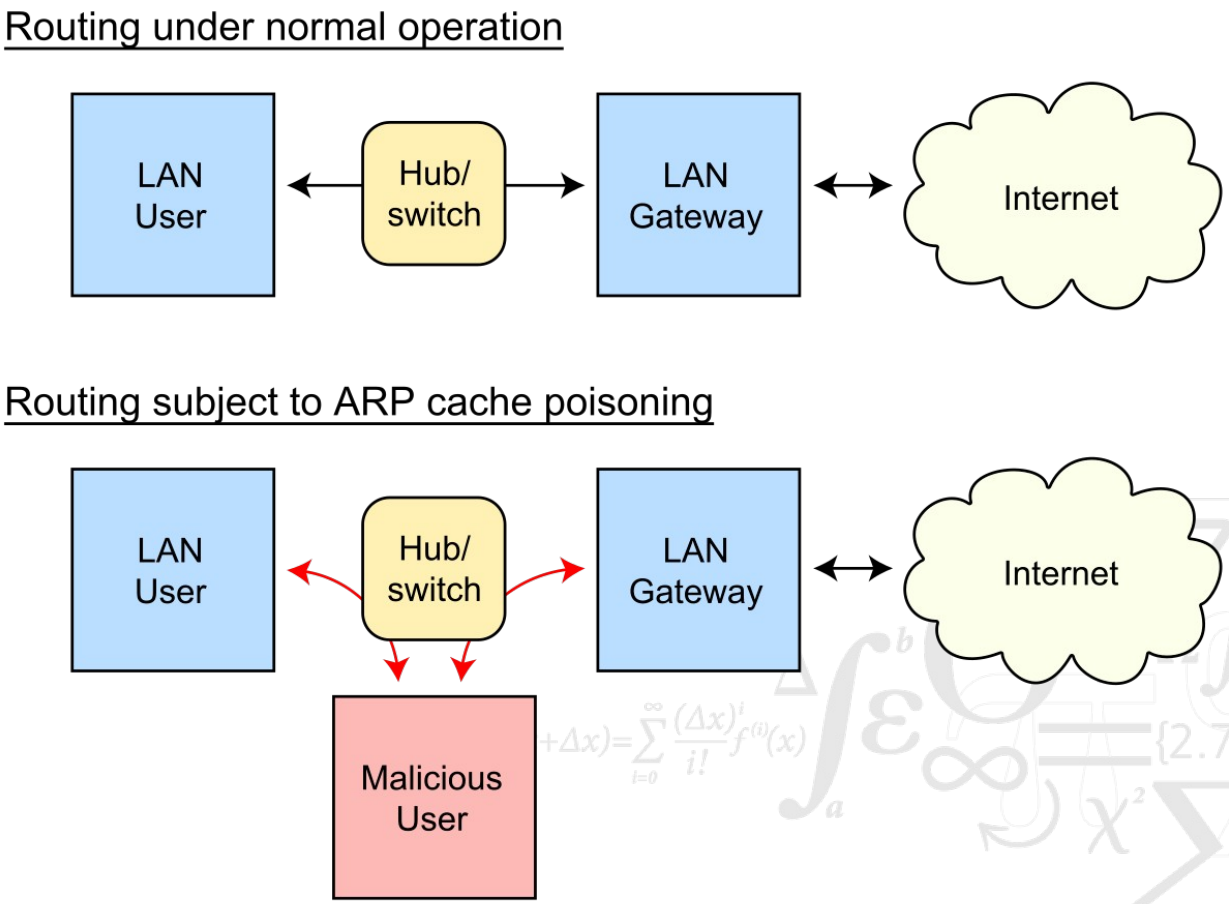
Secure Routing



ARP Spoofing/Poisonning

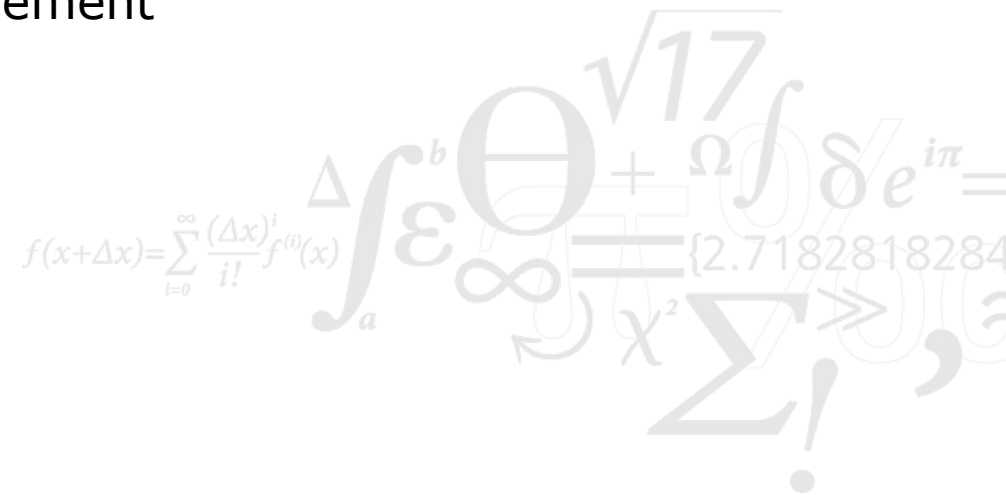
- Address Resolution Protocol (ARP) resolves Internet layer addresses to Link layer addresses
- Goal of the attack: associate attacker's host MAC address with the IP address of a target host
- Static ARP entries are not feasible for large networks:
  - On a network of n machines, this results in n^2-1 ARP entries
- Mitigation includes monitoring of network to look for inconsistencies
- Proper network segmentation can also help as ARP messages are limited to local sub-networks

ARP Spoofing/Poisonning



BGP Hijacking

- Border Gateway Protocol (BGP): exchange routing and reachability information among Autonomous Systems
- BGP hijacking: AS advertises a prefix that they do not own
- Again, network monitoring is one of the most effective mitigation
- Resource Public Key Infrastructure (RPKI) and BGPSec introduces cryptographic verification to ensure the validaty of the adversited routes but this is costly to implement



Communication Security
Link encryption

- Encryption performed in “the Data Link Layer”
- Each link on the route is encrypted independently
- Advantages:
  - Transparent to hosts (OS and applications)
  - May protect packet meta data (headers)
  - Fast encryption hardware can be used
- Disadvantages:
  - Data decrypted/re-encrypted on all intermediate nodes
    - *Modification of standard protocols*
    - *Introduces a performance penalty*
    - *Data is exposed on all intermediate nodes (routers)*
  - Everything or nothing gets encrypted

Communication Security
End-to-end encryption

- Encryption performed in the "application layer"
- Encrypted at source and only decrypted at destination
- Advantages:
  - Data protected all the way from sender to receiver
  - Flexible choice of encryption algorithms
    - *Balance security and performance*
  - Some data can be sent unencrypted
  - No modification of the existing routing infrastructure
- Disadvantages:
  - User (programmer) needs to manage encryption explicitly
  - Applications and services may need to be modified
    - *Expensive and difficult to update encryption technology*

Virtual Private Networks (VPNs)

- VPNs use a public network (usually the Internet) to provide a secure connection between two private parts of a network or remote users on a network
- They can be used to connect a PC into a LAN (i.e., a telecommuter) or two connect two LANs (i.e., a branch office to a corporate headquarters)
- They are inexpensive to use
  - they eliminate the need for a costly private leased circuit
  - and they provide privacy over a public network

Tunneling

- Tunneling is the technique used by the ends of a VPN to communicate
  - a packet send over a VPN is encapsulated in a secure protocol prior to being embedded into the IP protocol
- The receiving end (at the router) strips off the header and trailer information of the packet and the private network protocols decapsulates the packet and send the packet on
- Several private network protocols are available to encrypt the packet on a VPN

Tunneling

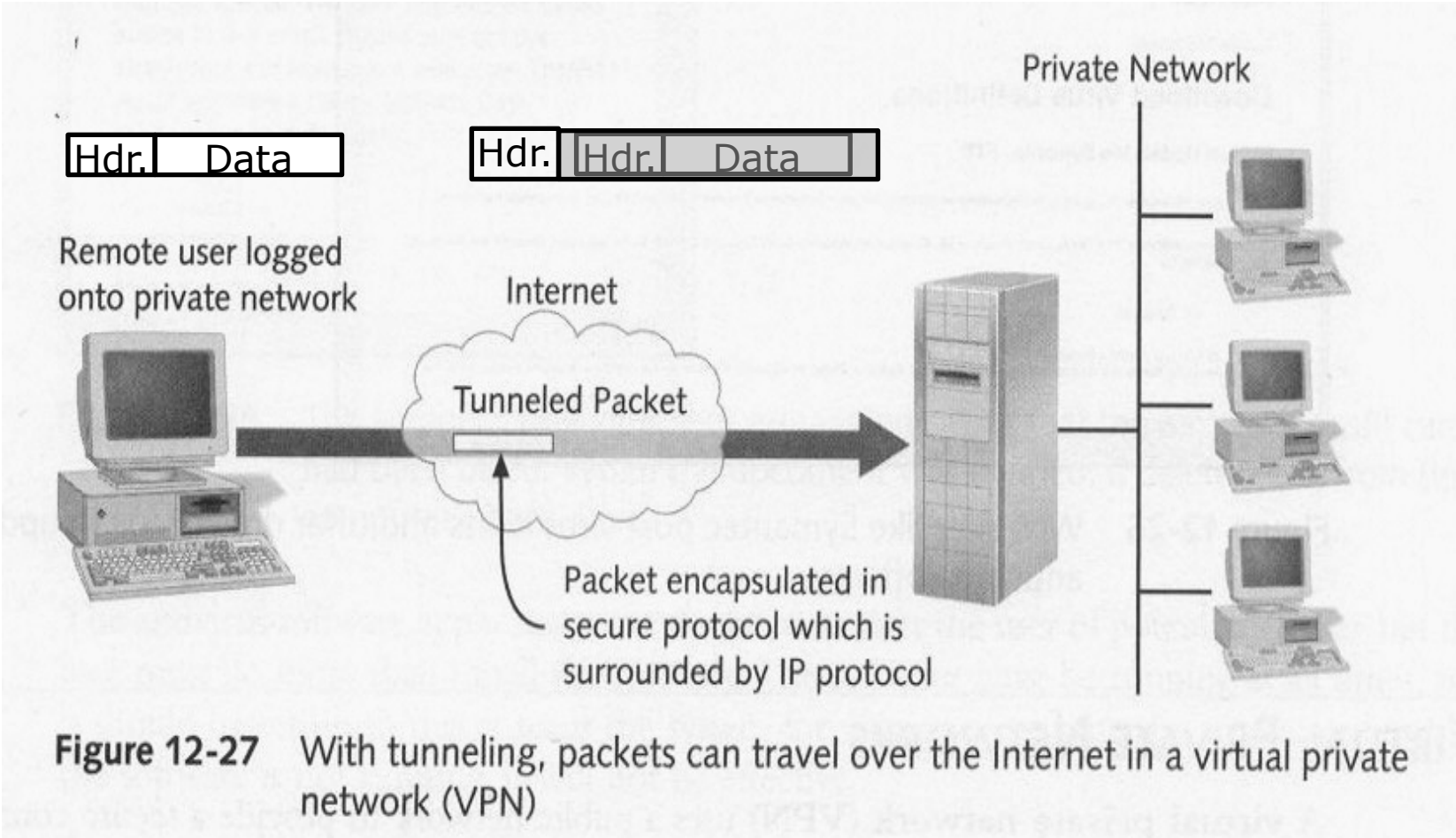
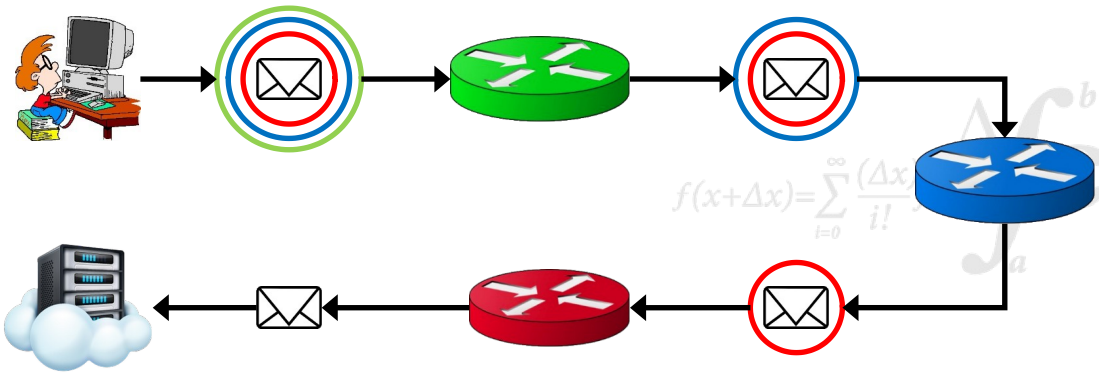


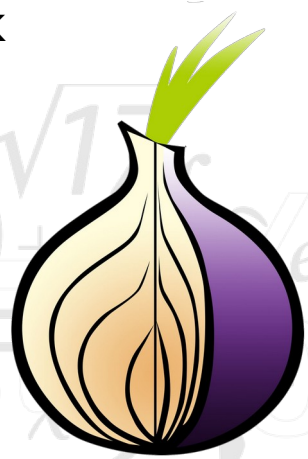
Figure 12-27 With tunneling, packets can travel over the Internet in a virtual private network (VPN)

See: Untraceable electronic mail, return addresses, and digital pseudonyms, David Chaum

Private Communication

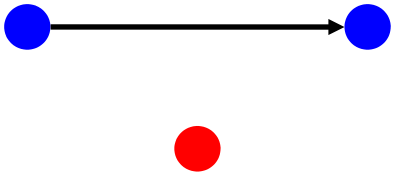
- Typically achieved by several tunnels through a network of mix-nodes
  - "Mixes" all communication currently flowing through the node
    - *Must confuse message sizes and arrival/departure times*
    - *Makes individual messages indistinguishable from other flows through mix-node*
      - Flow volume decides privacy of communication
- The Onion Router (TOR) is the best known mix-network



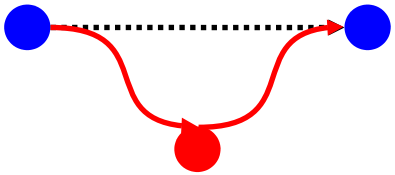


Network Attacks

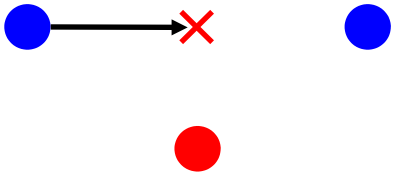
Active attacks



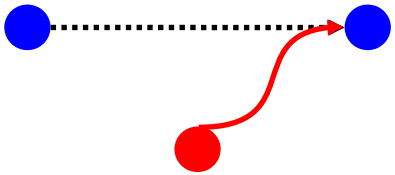
Normal communication



Modification

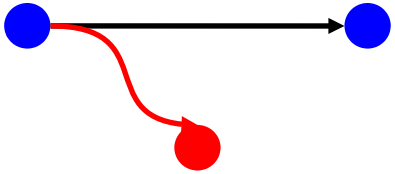


Deletion

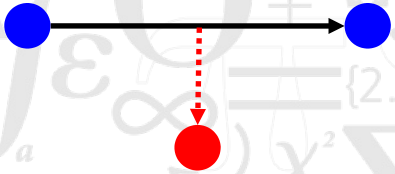


Fabrication

Passive attacks



Eaves dropping



Traffic analysis

Prevent – Detect – React (– Recover)

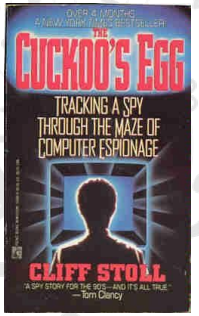
- Network attack prevention
  - Firewalls - *perimeter security (including Web Application Firewalls, WAF)*
  - Identity and Access Management (IAM) – *network access authorisation*
  - Segmentation - *compartmentalisation + security in depth*
  - Virtual Private Networks (VPN) – *secure communication*
- Network attack detection
  - Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS)
  - Honey Pots
  - Security Information and Event Management (SIEM)
- Network attack reaction
  - Systems-/Network Operation Centres (SOC/NOC)
  - Contingency-/Disaster plans
    - *Procedures described in playbooks or runbooks*

Perimeter Security

- Defending the Network Boundary
  - Keep unwanted outsiders away from valuable resources on the network
  - Don’t want outsiders coming in (except for special web-services)
    - *Implies filtering of traffic*
  - Allow insiders to go out
    - *Network Address Translation (NAT) may suffice*
- Filtering traffic at the network boundary (corporate firewalls)
  - Network wide filtering
  - Configured/managed by system administrators
  - Transparent to individual nodes/users
- Filtering traffic at each individual node (personal firewalls)
  - Host-based policy (locally or globally defined)
  - May allow local policy override
  - May require intervention by local users

Impersonation Attacks falsely obtain valid authentication details

- Guess identity and authentication details (login, password)
  - Try popular logins (guest, admin) and passwords (secret, password)
- Obtain identity and authentication details by eavesdropping
  - **`telnet`** sends login/password over the wire in the clear
  - Bad encryption is sometimes used (MS LAN manager, WEP)
- Circumvent/disable authentication
  - Exploit buffer overflows
  - Social engineering ("I forgot my password, please reset to BANANA")
- Use a target that will not be authenticated
  - Remote authentication from "trusted hosts" is sometimes disabled
  - Public accounts (anonymous FTP, GUEST accounts)
- Use a target whose authentication details are well known
  - Standard accounts with default passwords
    You can sometimes find these in the manuals



Spoofing
falsify authentication details

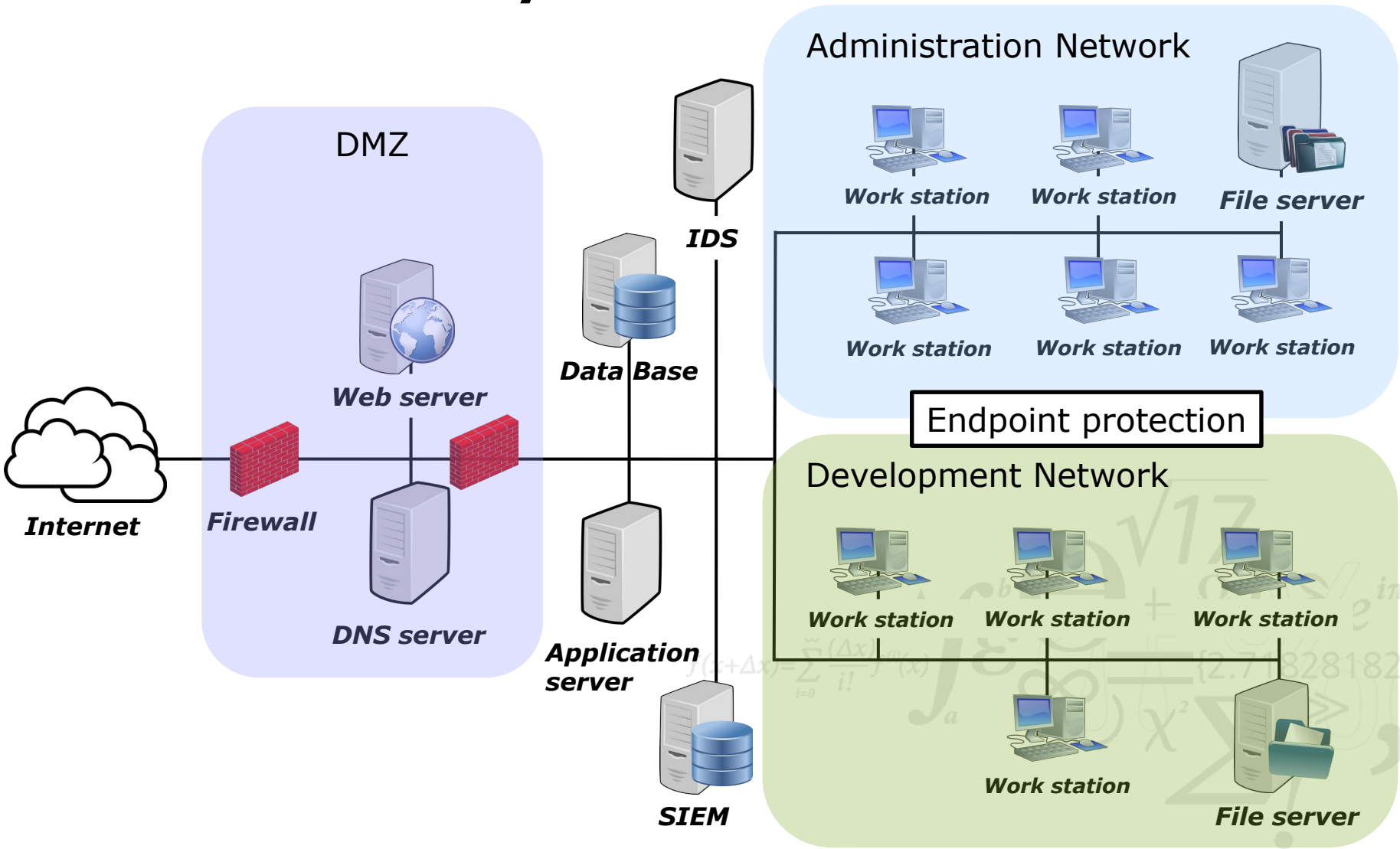
- Masquerading
  - Falsify DNS entries, choose similar hostnames, …
    - *www.whitehouse.com used to be a porn site*
    - *www.whitehouse.net is a spoof site against George W. Bush*
    - *www.whitehouse.gov is the official site*
- Session Hijacking
  - Intercepting a session initiated by another entity
    - *Redirect network communication to the attacker's host*
    - *Insert redirection on the victims web-site*
- Man-in-the-Middle Attack
  - Alice wishes to talk to Bob
    - *Charlie pretends to be Alice to Bob and to be Bob to Alice*
    - *Charlie intercept all messages between Alice and Bob and forwards, possibly modified versions, to the other entity*

Availability Threats
Denial of Service (DoS)

- Transmission failure
  - hardware/software failure of nodes or links
- Connection flooding
  - Exhaust bandwidth (sending too much traffic to the victim)
    - *This is what the Low Orbit Ion Cannon (LOIC) does*
  - Exhausting resources at the victims site (SYN floods)
  - DNS attacks
    - *Redirecting traffic to the victims site*
    - *Redirecting traffic away from the victims site*
- Distributed Denial of Service (DDoS)
  - Break into many hosts (zombies) on the network (create a Botnet)
  - Instruct zombies to overload victim at a given time
  - Individual zombies may appear to be valid clients

Pause

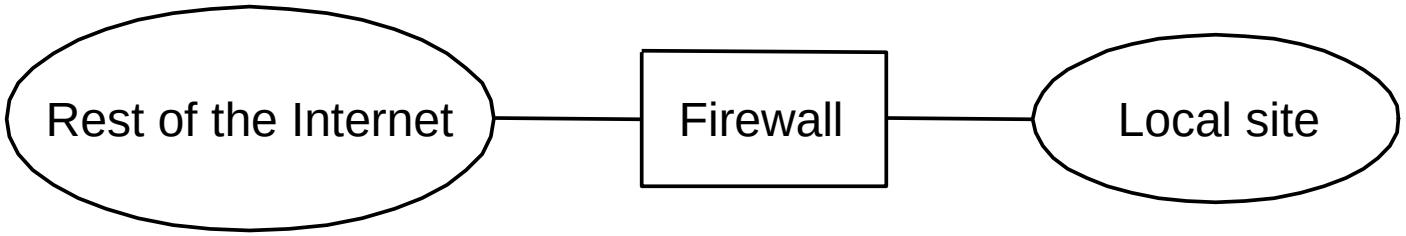
Network Security Architecture



Firewalls

- A firewall filters information that is sent and received from outside the network
  - It is software that resides on the network's gateway
- A firewall can filter packets based on
  - Packet headers
    - *Data packets, examining the source & destination IP*
    - *Ports and applications, in order to deny access*
      - May include external data, e.g. time of day, in decision
  - Packet content (payload), e.g. macros, inappropriate web content, …
    - *Deep packet inspection*
    - *Difficult with encrypted payloads (e.g. https)*
      - May require local proxies to serve as Man in the Middle (as CA)
  - Packet flows
    - *Consider more packets from the same flow*

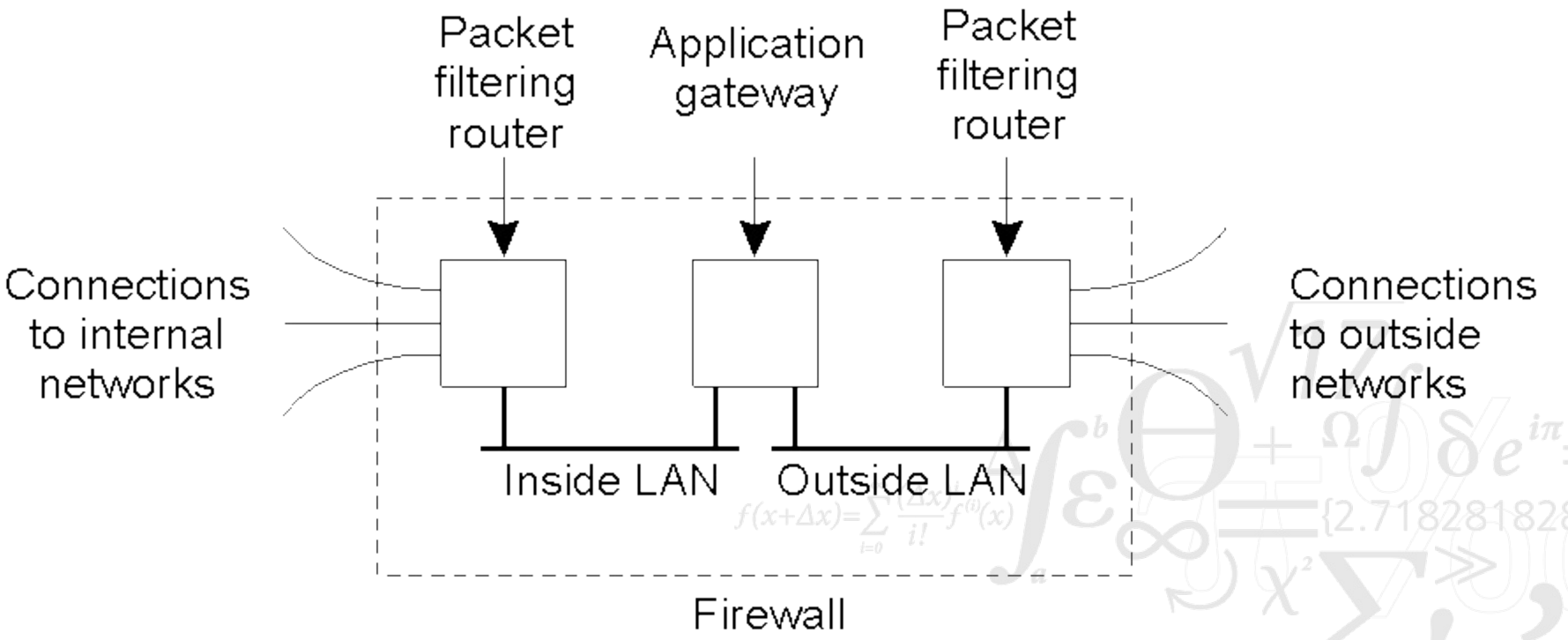
Filtering Firewalls



- Simple packet filter
  - example (IP-Addr, port, …)
    (192.12.13.14, 1234, 128.7.6.5, 80)
    (,*, 128.7.6.5, 80)*
  - default: forward or not forward?
  - how dynamic?

Firewalls

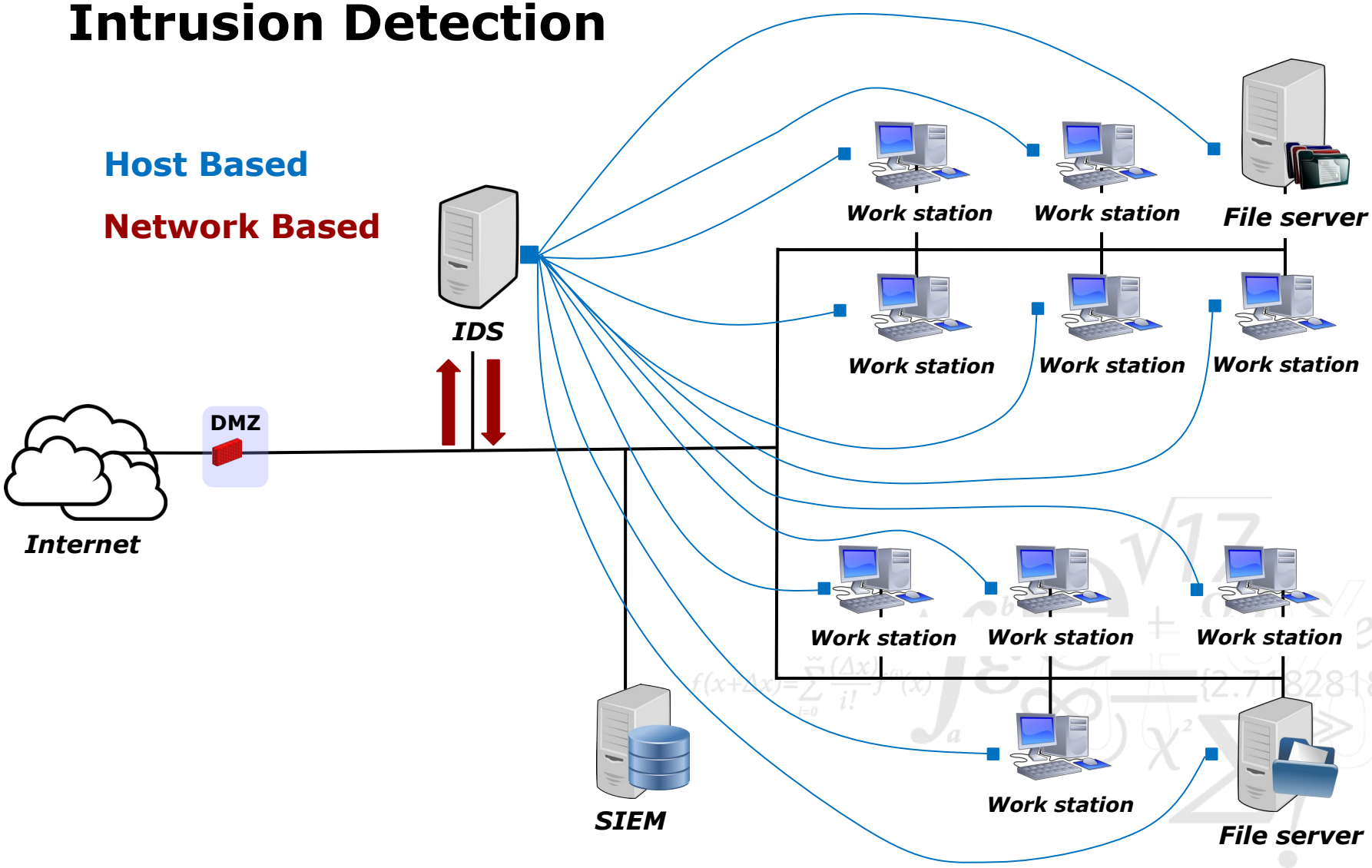
- A common implementation of a firewall



Intrusion Detection
definition

- *Intrusion detection is the process of identifying and responding to malicious activity targeted at computing and networking resources*
  - Process
    - *Interaction between people and tools, it takes time*
  - Identifying
    - *Before, during or after the intrusion*
  - Responding
    - *Collect evidence, limit damage (honey pots), shut-out*
  - Malicious activity
    - *Intentional attempts to do harm*
  - Computing and networking resources
    - *Logical intrusions as opposed to physical intrusions*

Intrusion Detection



Host Based IDS Systems

- Inspects locally available information
  - Historical data (sends alerts after the fact)
    - *System log-files*
    - *Application log-files*
    - *Much of this data is already collected and consolidated in SIEM*
  - Real-time data (alerts about ongoing activities, IPS may block it)
    - *Monitor running applications*
      - scanning software before running it (virus detection)
        - » signatures of already scanned apps may be cached & shared
    - *Monitor system usage*
      - Unusual application workloads (CPU, memory, network traffic, …)
        - » High CPU load or system call patterns may indicate ransomware
      - Unusual service requests
        - » DNS resolution for well-known Bot-net C&C servers

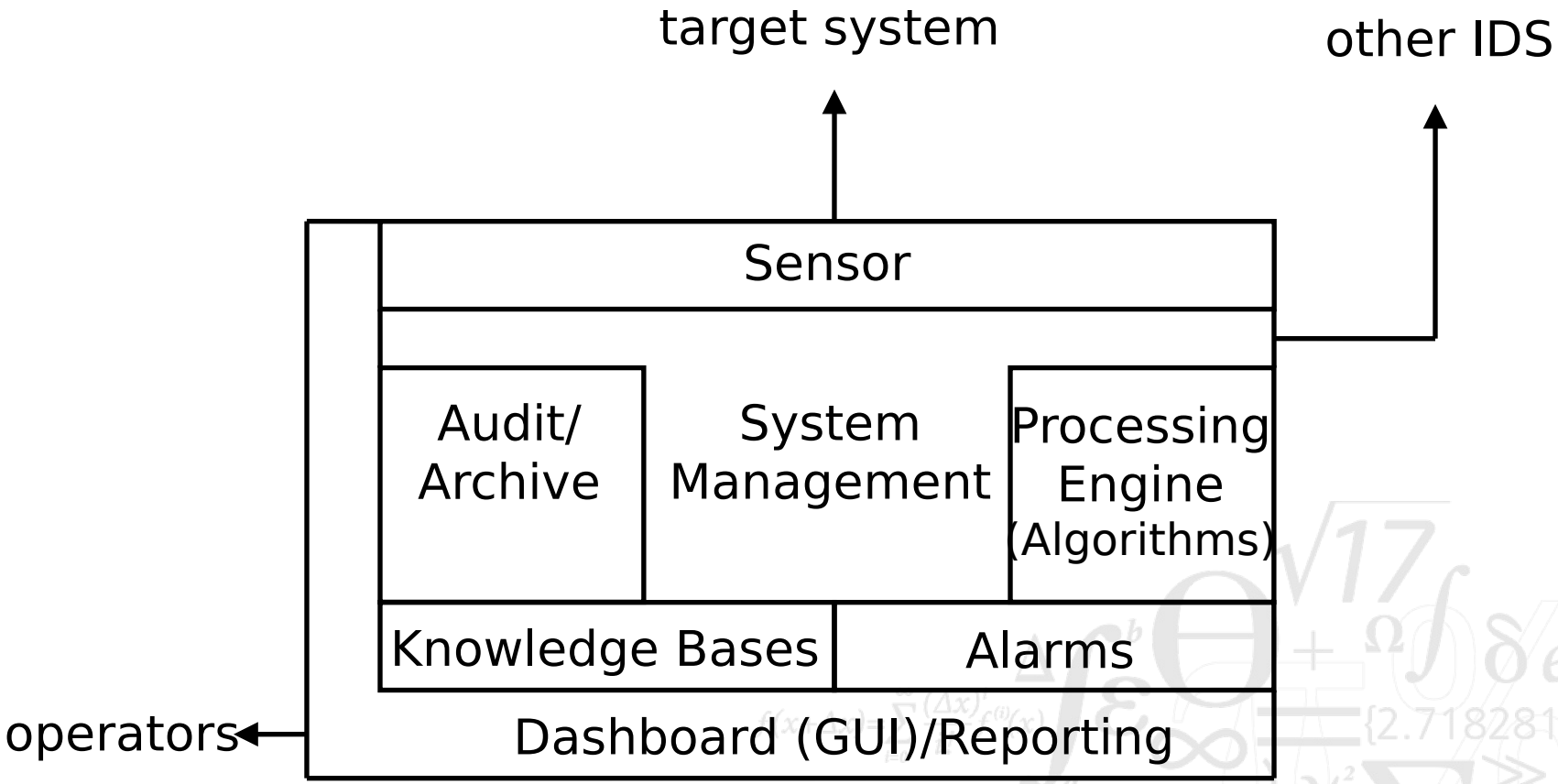
Network Based IDS Systems

- Inspects traffic on the network
- Signature Based Systems
  - Relies on established patterns (“signatures”) in malicious network traffic
  - Similar to the signatures used in virus checkers
- Anomally Detection Systems
  - Establishes base line for normal communication
  - Detects abnormal traffic pattern
    - *Employs techniques from machine learning, pattern matching, big data*

How to detect an intrusion?

- Heuristics based intrusion detection
  - Repetition of a suspicious action (e.g. failed login attempts)
  - Mistyped command from an automated sequence
  - Known signatures (exploits)
  - Directional inconsistencies (inbound and outbound traffic)
  - Unexpected attributes of some service request or packet
  - Unexplained problems in a subsystem
- Anomally detection
  - Statistics based
    - *Markov process, outlier detection, …*
  - AI based
    - *Machine learning, Artificial Neural Networks, Deep Learning, …*

Typical IDS Components



Trapping Intruders

- The IDS may include a copy of the real system
  - Redirect intruders to this trap system
  - Must present a consistent view of the system in order to prevent detection
- The IDS may construct a honey pot
  - A trap system that looks attractive to intruder
    - *Based on his search for information*
    - *Example in Clifford Stoll: The Cuckoo's Egg*

Honeypots/Honeynets

- Machines that appear interesting to attackers
  - Offers no real data or services
  - Only "users" are attackers
    - *Configured with sensors to detect and record usage*
      - If used raise alarm
    - *Provides clues to objectives and motives of attackers*

- Purpose is to attract and retain attackers
  - Attract them away from production environment
  - Retain them while communication is analysed and tracked
  - Possibility of misinformation or misdirection

- Honeypots can be extended to networks
  - Check: **`https://www.honeynet.org`**

Ethics of Intrusion Detection

- Intrusion detection requires monitoring of all network communication
  - Equivalent to Orwell's Big Brother!

- Data collected for intrusion detection may be used (or abused) in another context
  - Establish activity of employees in a company