KF School of Computing and Information Sciences
Florida International University

CNT 4403
Computing and Network Security

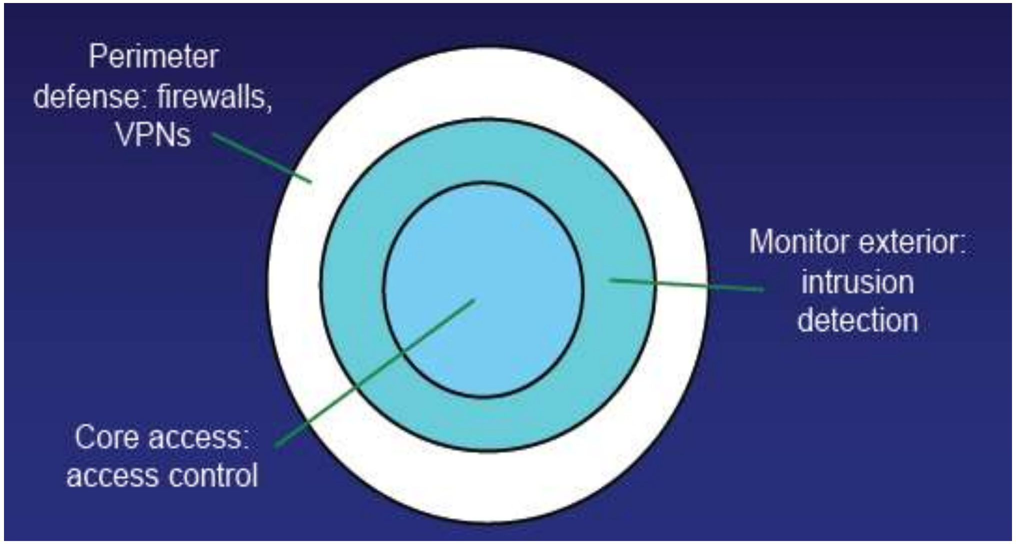
Network Security – Firewalls

Dr. Kemal Akkaya

E-mail: *kakkaya@fiu.edu*

Intrusion Detection Systems (IDS)

- ❑ **An IDS is any combination of hardware & software that monitors a system or network for malicious activity.**
  - ➢ Car alarms, Fire detectors, House alarms, Surveillance systems
- ❑ **Why IDS?**
  - ➢ Passive security methods are not enough to protect networks from attacks!
  - ➢ IDS are part of reactive defense strategies.
    - ✓ What you do after prevention has failed
    - ✓ Take action or send an alarm to an officer


Perimeter defense: firewalls, VPNs
Monitor exterior: intrusion detection
Core access: access control

What should be detected?

- ❑ **Attempted and successful break-ins**
- ❑ **Attacks by legitimate users**
  - ➢ For example, illegitimate use of root privileges
  - ➢ Unauthorized access to resources and data
- ❑ **Trojan horses**
- ❑ **Viruses and worms**
- ❑ **Denial of service attacks**

Many organizations deploy IDS

-Provide warnings to network administrator

-Administrator can then improve network's security

-Vigorous investigation could lead to attackers

Efficiency of IDS

- ❑ **Accuracy**
  - ➢ The proper detection of attacks and the absence of false alarms
    - ✓ False positive:
      - – Alarm in normal traffic
    - ✓ False negative
      - – No alarm during an attack
- ❑ **Performance**
  - ➢ The rate at which traffic and audit events are processed
    - ✓ To keep up with traffic, may not be able to put IDS at network entry point
    - ✓ Instead, place multiple IDSs downstream
- ❑ **Fault tolerance**
  - ➢ Resistance to attacks
    - ✓ Should be run on a single hardened host that supports only intrusion detection services
- ❑ **Timeliness**
  - ➢ Time elapsed between intrusion and detection

Classification of IDS

- Different classes of IDS based on different criteria
- Based on data collection mechanism
  - **Host-based**
    - ✓ OS audits and system and applications logs
  - **Network-based**
    - ✓ Packets captured from network traffic
- Based on detection techniques
  - **Anomaly (Behavior-based)**
    - ✓ Any behavior outside of a “normal profile”
  - **Misuse (Rule-based)**
    - ✓ Monitored activity is compared to set of signatures (patterns) for known attacks

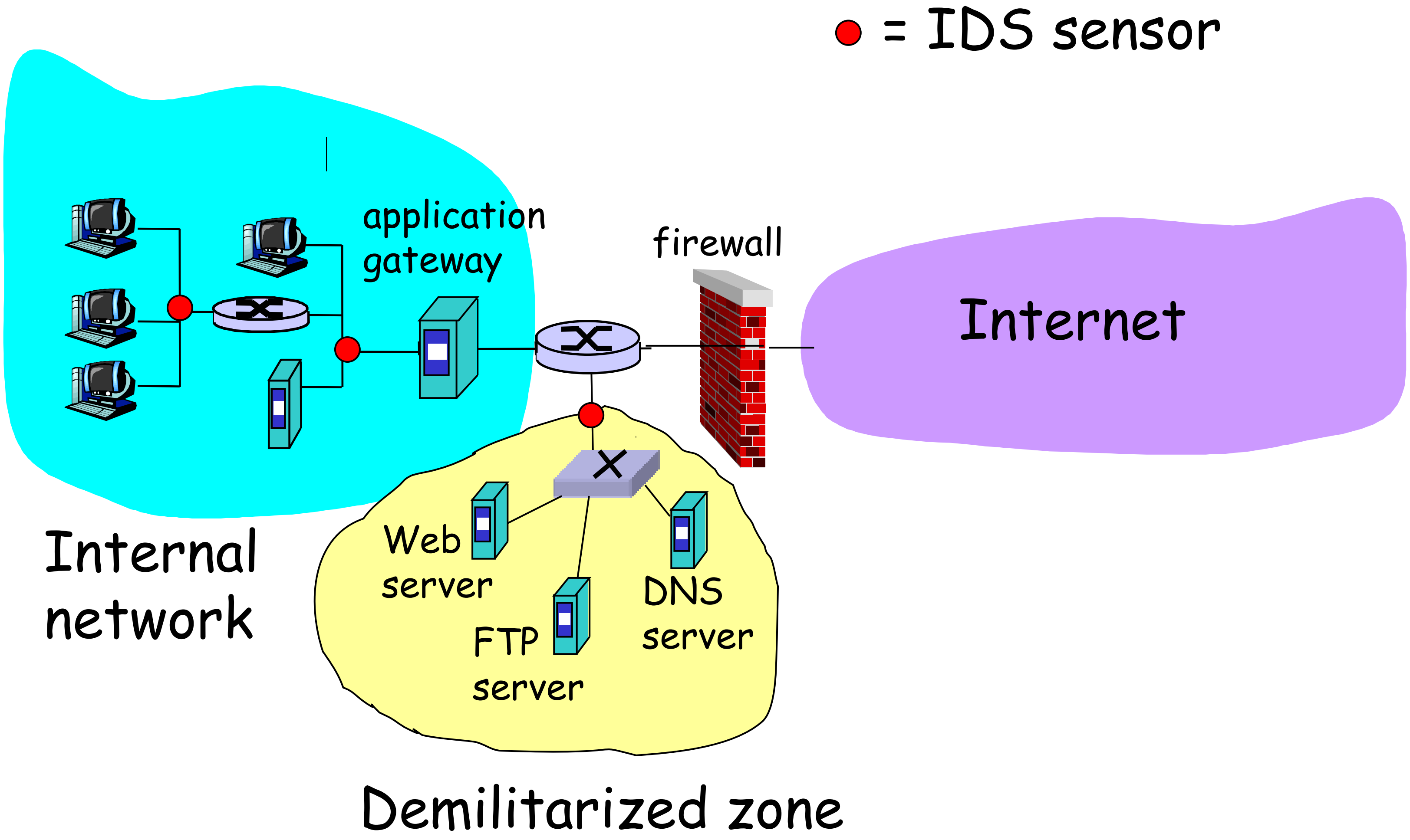
Host-based IDS

- Run on hosts
- Monitor attacks on OSes, applications.
- Have access to audit logs, error messages, any resources that can be monitored on host
- Privileged host access
  - Psswd files, Registry in Windows
- Tuned for system/OS/apps
- High detection accuracy
- Mostly for insider attacks
  - Exemployee utilizing old account, employee modifying performance evaluation, etc.
- Disadvantages
  - Only covers one host
  - IDS to be placed on every critical host
  - Need version for each OS

Network-based IDS

- ❑ **Often placed on a router or firewall**
- ❑ **Monitor traffic, examine packet headers and payloads**
  - ➢ TCP/IP packets
- ❑ **Mostly for outsider attacks**
- ❑ **Advantage:**
  - ➢ Single Network-based IDS can protect many hosts and look for global patterns
- ❑ **Disadvantage**
  - ➢ Deployment issues – where to put the sensors
  - ➢ Can be easily detected – Airsniff
  - ➢ May not deal with huge number of packets
  - ➢ Can not deal with encrypted traffic
    - ✓ If packet header or payload is encrypted, no signature analysis can be done

IDS sensors


● = IDS sensor
application gateway
firewall
Internet
Internal network
Web server
FTP server
DNS server
Demilitarized zone

Anomaly Detection (Behavior-based)

- **Define a profile describing "normal" behavior**
  - Works best for "small", well-defined systems (single program rather than huge multi-user OS)
- **Profile may be statistical**
  - Build it manually (this is hard)
  - Use machine learning and data mining techniques
    - ✓ Log system activities for a while, then "train" IDS to recognize normal and abnormal patterns
  - Risk: attacker trains IDS to accept his activity as normal
    - ✓ Daily low-volume port scan may train IDS to accept port scans
- **IDS flags deviations from the "normal" profile**
- **Doesn't rely on having previous knowledge of attack**
- **Big research topic in security**
  - Still in the laboratory

Misuse Detection (Signature-based)

- **Set of rules defining a behavioral signature likely to be associated with attack of a certain type**
  - Example: SYN flooding (denial of service)
    - ✓ Large number of SYN packets without ACKs coming back

      …or is this simply a poor network connection?
- **Skilled security engineers research known attacks**
  - Put them in a database
  - Match attack signatures
- **Disadvantages**
  - Attack signatures are usually very specific and may miss variants of known attacks
    - ✓ Big research challenge: fast, automatic extraction of signatures of new attacks
  - No knowledge of intention of activity
    - ✓ Triggers alarms even if traffic is benign
  - Signature bases are getting larger – **zero-day attacks?**
    - ✓ Every packet must be compared with each signature

IDS versus IPS

- **Intrusion Prevention System (IPS) is often able to recognize the attack and respond appropriately**
- **Both IDS and IPS devices recognize attacks, but they operate with some differences**
- **IDS**
  - Operates parallel to the network
  - Passive device
  - Monitors all traffic and sends alerts
- **IPS**
  - Operates in-line to the network
  - Active device
  - Monitors all traffic, sends alerts *and* drops or blocks the offending traffic