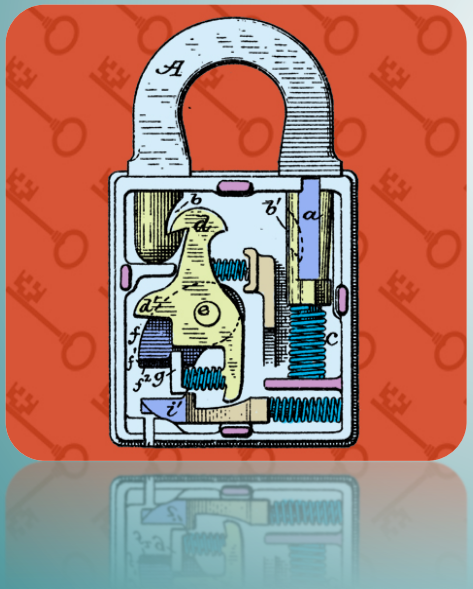
Garantía y Seguridad en Sistemas y Redes

Tema 9. Intrusion Detection



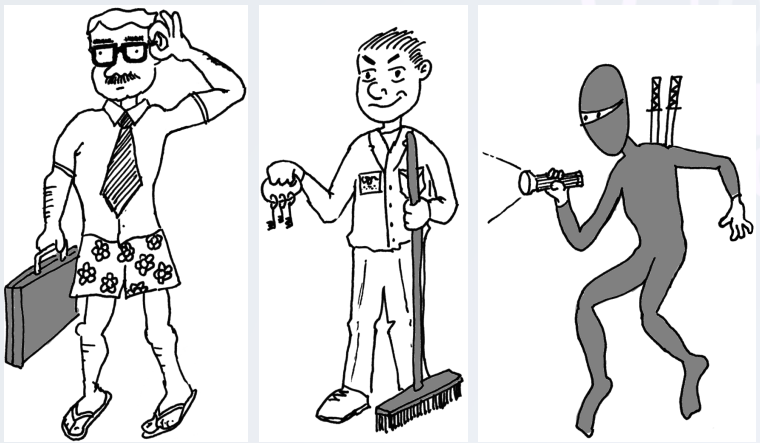
Esteban Stafford

Departamento de Ingeniería Informática y Electrónica

Contents

Intruder classification

- **Masquerader** Enters system by ilegally using legitimate user's account.
- **Misfeasor** Legitimate user accesses unauthorized data or misuses privileges.
- **Clandestine User** Gains access to system by eluding controls.



Intruder behaviour

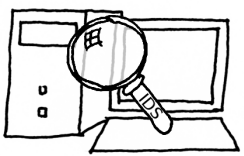
- **Hacker** Seek thrill or status. Opportunistic.
  - Select the target using IP lookup tools.
  - Map network for accessible (Port scanning).
  - Identify potentially vulnerable services.
  - Install rootkit.
  - Wait for administrator to log on and capture his password.
- **Criminal** Look for sensitive data. Targeted.
  - Act quickly and precisely to make their activities harder to detect.
  - Exploit perimeter through vulnerable ports.
  - Use Trojan horses (hidden software) to leave back doors for reentry.
  - Retrieve valuable data from databases.
  - Make few or no mistakes.
- **Insider** Revenge or feel entitled. Most difficult.
  - Create network accounts for themselves and their friends.
  - Access accounts and applications they wouldn't normally use.
  - E-mail former and prospective employers.
  - Conduct furtive instant-messaging chats.
  - Perform large downloads and file copying.
  - Access the network during off hours.

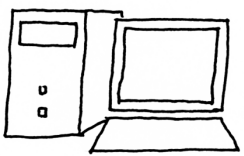
Intrusion Detection

IDS motivation

- Quick detection might allow ejecting intruder before consequences.
- Deployment of effective IDS can act as deterrent.
- Information gathering can help strengthen security measures.

Placement





- Host
- Distributed
- Network
- Distributed
- Adaptive

Intrusion Detection

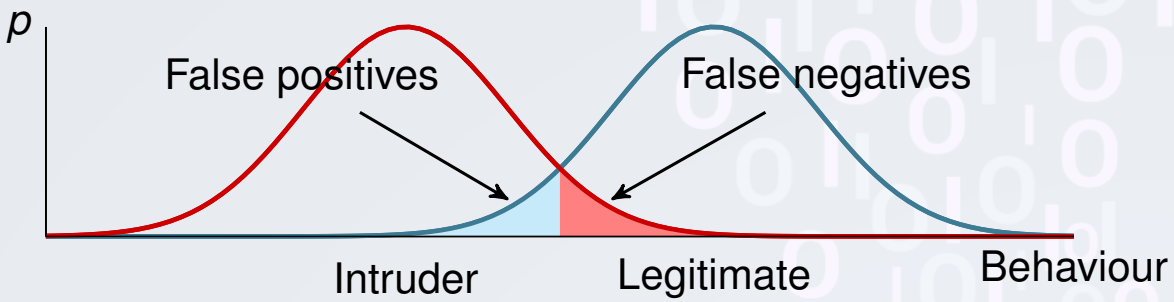
Logical components

Sensors: Network monitor, log files, system call traces...

Analyzers: Combine the information of sensors to decide if an intrusion has occured. Indicates intrusion and supplies evidence and possible actions.

User interface: Used to configure the behaviour of the IDS and view intrusion information.

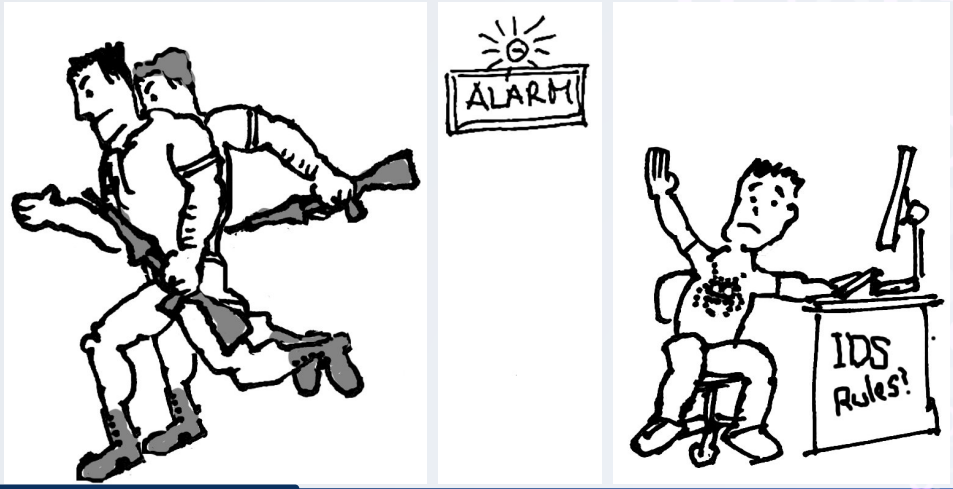
Detection Principles



- False positives mean that the security team has to investigate a suspicious event.
- High number of false positives mean a lot of unnecessary work (Paranoid setting).
- False negatives are intrusions that have not been detected.
- High number of false positives give a false sense of security (Relaxed setting).

Base-Rate Fallacy

- Intrusion Detection System with 0.1% error probability.
- We guess there is a chance of 1:10000 of intrusion.
- The alarm goes of! Shall we call the marines?
- **Wait!** False alarm probability is 0.909
- For a reasonable false alarm probability with lots of events, error probability must be REALY low.



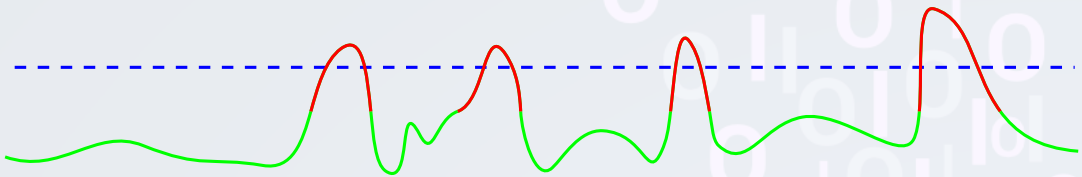
Detection methods

Detection methods

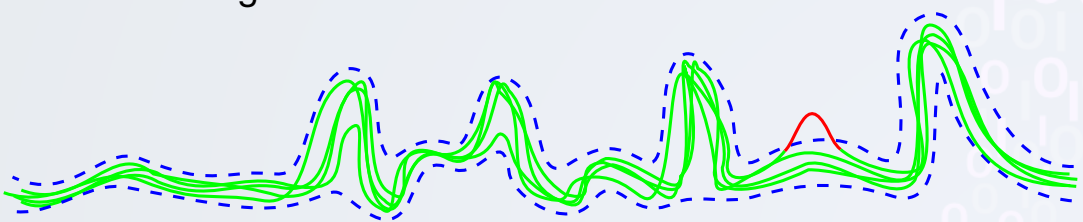
- Change detection
  - Store hash of sensitive files and check periodically.
  - Only usefull for seldom changed files.
- Statistical anomaly detection
  - Detect suspicious behaviour.
  - Allows detecting novel intrusions.
- Signature detection
  - Identify known intrusion patterns.
  - Unable to detect variations on intrusion patterns.

Statistical anomaly detection

- Threshold detection.
  - Count occurrences of specific event over time.
    - If exceeds a reasonable value - assume intrusion.
    - By itself a crude and ineffective detector.



- Profile based detection.
  - Characterize past behavior of users: mean and std. deviation, multivariate analysis, Markov processes, timing parameters.
  - Detect significant deviations from known behaviour.



Signature detection

- Observe events on system and apply rules to decide if activity is suspicious or not.
- Rule-based anomaly detection:
  - Analyze historical audit records to identify usage patterns.
  - Auto-generate rules for usage patterns, might require 10^4 to 10^6 rules.
  - Observe current behavior and match against rules.
  - Does not require prior knowledge of security flaws.
- Rule-based penetration identification:
  - Rules identify known penetration, weakness patterns or suspicious behavior.
  - Rules usually machine and OS specific.
  - Rules are generated by experts who review and code knowledge of previous attacks.
  - Quality depends on how well this is done.

Host-Based Intrusion Detection

System Requirements

- Run continually with minimal human supervision. Recover from reboot.
- Resist subversion. Must be able detect if modified by attacker.
- Impose a minimal overhead on the system.
- Be able to adapt to changes in system and user behavior.
- Be able to scale to monitor a large number of hosts.
- Provide graceful degradation of service. Modular.
- Allow reconfiguration without having to restart.

Host-Based Intrusion Detection

Audit Records

- Native audit records
  - Part of all common multi-user O/S.
  - Already available for use.
  - May not have the required info in desired form.
- Detection-specific audit records.
  - Created specifically to collect required info.
  - At cost of additional overhead on the system.
  - Time-stamp, subject, action, object, exception-conditions, resource-usage

```
smith@localhost:~$ cp game.exe /usr/bin

10821678 smith execute /bin/cp, 0, cpu=0002
10821679 smith read /home/smith/game.exe, 0, records=0
10821679 smith write /usr/bin/game.exe, write-violation, records=0
```

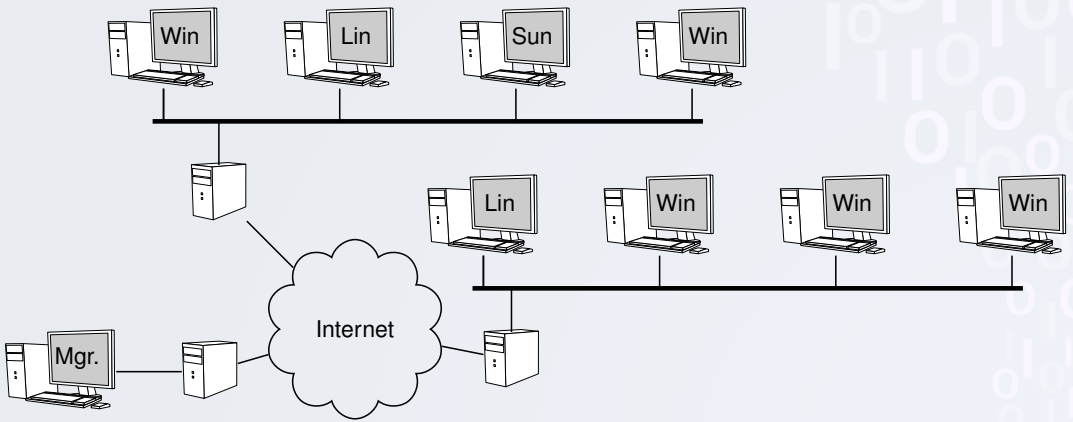
Host-Based Intrusion Detection

Metric/Model Combination Examples

- Login Frequency by day and time (event counter, mean/std. deviation model)
- Location Frequency (event counter, mean/std. deviation model)
- Output Volume (resource measure, mean/std. deviation model)
- Password Fails (event counter, operational model)
- Execution Frequency (event counter, mean/std. deviation model)
- Execution Denied (event counter, operational model)
- Record Access (event counter, mean/std. deviation model)

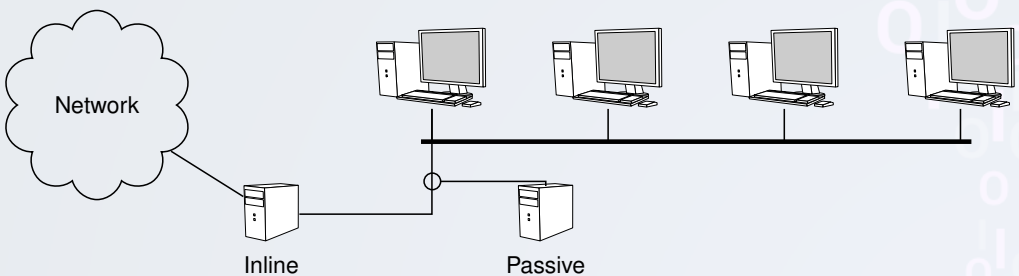
Distributed Host-Based Intrusion Detection

- Traditional IDS focus is on single systems.
- Can't information from several systems be combined?
- Not so easy:
  - Deal with varying audit record formats.
  - Maintain integrity and confidentiality of networked data.
  - Centralized or decentralized architecture?

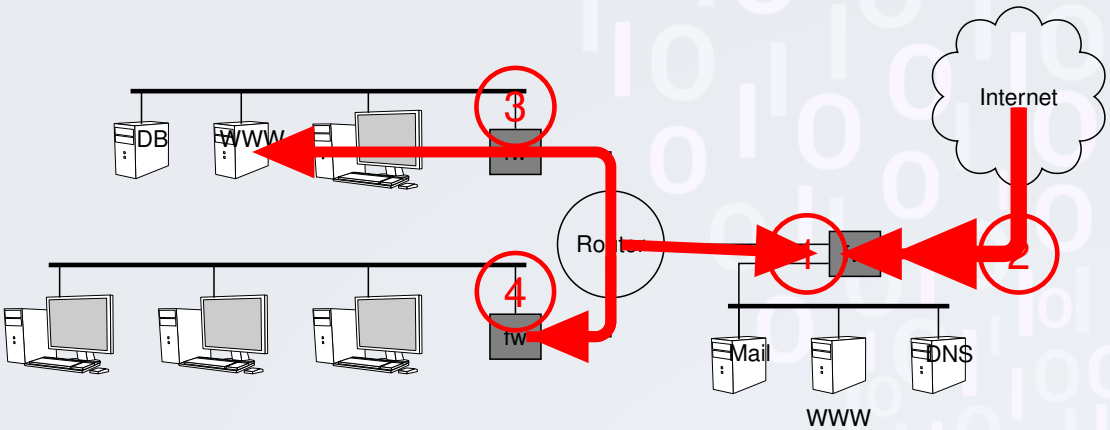


Network-Based IDS (NIDS)

- Monitor traffic at selected points on a network.
- May examine network, transport and/or application level protocol activity directed toward systems.
- Comprises a number of sensors (distributed):
  - Inline sensors: possibly as part of net devices.
    - Switch with NIC in promiscuous mode.
    - Slow NIDS might act as bottle neck.
  - Passive sensors: monitors copy of traffic.
    - Wire/Optical Fiber taps.



NIDS Sensor Deployment



- 1: Threats from outside. Highlight firewall problems. Check outgoing traffic.
- 2: Measure attack pressure. Types and numbers. High workload.
- 3: Protect internal services (Intranet). Spot insider threats.
- 4: Dept. granularity. Protect critical systems. Restrict resource use.

Intrusion Detection Techniques

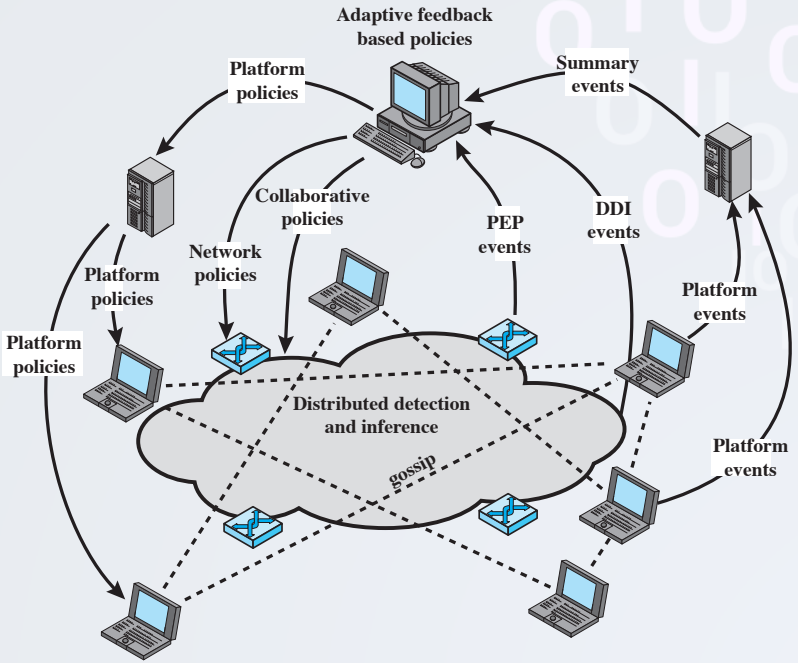
- Statistical anomaly detection:
  - Denial of service attacks (flood or app.), scanning (fast/slow), worms (duplication activity)
- Signature detection (Deep packet inspection):
  - Application, Transport, Network layers. Unexpected application services, unusual packets, policy violations.
- When a potential violation is detected, a sensor sends an alert and logs information
  - Used by analysis module to refine intrusion detection parameters and algorithms.
  - Used by security manager to improve protection.

Distributed Adaptive Intrusion Detection

- Perimeter defense and intrusion detection
  - Organizational defenses: Firewalls, HIDS, NIDS
  - Each has limited data to analyze. Low-rate attacks are below thresholds.
  - Difficult to recognize new attacks. Difficult to keep all protections updated.
  - Loose organization boundaries: Wifi, laptops, mobile phones.
- Combine all IDSs together
  - More sensors at broader areas. Gossip protocol can correlate more data. Achieve higher statistical accuracy in shorter time.
    - When unsure about an attack, false positive rate may be too high.
    - Once an attack is collaboratively identified, (when see similar activities in other network,) predict the attack is on the way, false positive rate becomes low.
  - Host-based IDS provides rich App info

Distributed Adaptive Intrusion Detection

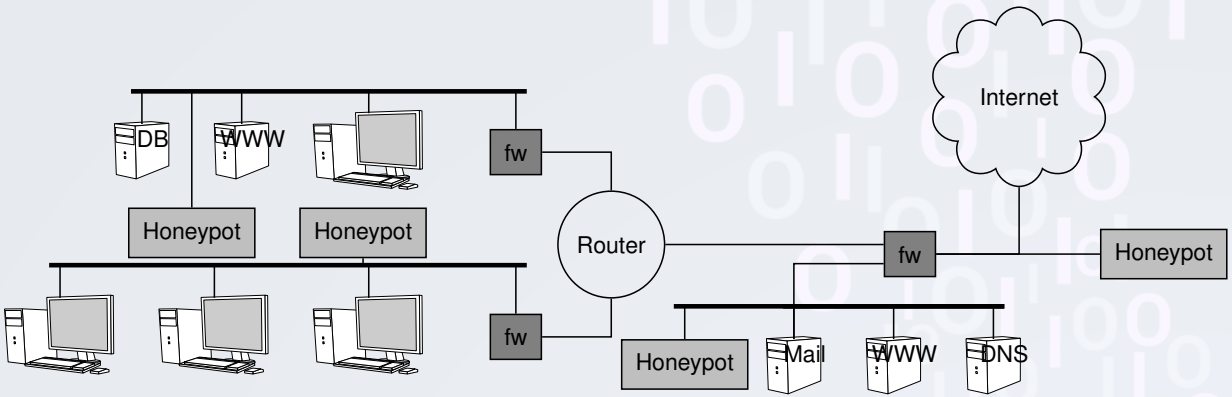
- DDI: Distributed detection and inference
- PEP: Policy enforce point



Honeypots

- They are decoy systems:
  - Filled with fabricated information.
  - Instrumented with monitors or event-loggers.
  - Divert and hold attacker to collect activity info.
  - Do not expose production systems.
- Initially were single-PC systems.
- More recently are/emulate entire networks.
- Virtual Machines (VMs) makes this easier.

Honeypot Deployment



- 1: Outside external firewall. Diverts attackers but misses insiders.
- 2: Near externally available services. Need to open firewall to fake services.
- 3: Attracts internal attacks. Feedback for firewall. Dangerous if compromised.