Computer Security DD2395

http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasak10/

Spring 2010

Sonja Buchegger
buc@kth.se

Lecture 5, Feb. 1, 2010

Intrusion Detection

Intruders

- significant issue hostile/unwanted trespass
  - from benign to serious
- user trespass
  - unauthorized logon, privilege abuse
- software trespass
  - virus, worm, or trojan horse
- classes of intruders:
  - masquerader, misfeasor, clandestine user

Examples of Intrusion

- remote root compromise
- web server defacement
- guessing / cracking passwords
- copying viewing sensitive data / databases
- running a packet sniffer
- distributing pirated software
- using an unsecured modem to access net
- impersonating a user to reset password
- using an unattended workstation

Security Intrusion & Detection

Security Intrusion

a security event, or combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Intrusion Detection

a security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.

Hackers

- motivated by thrill of access and status
  - hacking community a strong meritocracy
  - status is determined by level of competence
- benign intruders might be tolerable
  - do consume resources and may slow performance
  - can’t know in advance whether benign or malign
- IDS / IPS / VPNs can help counter
- awareness led to establishment of CERTs
  - collect / disseminate vulnerability info / responses

Hacker Behavior Example

1. select target using IP lookup tools
2. map network for accessible services
3. identify potentially vulnerable services
4. brute force (guess) passwords
5. install remote administration tool
6. wait for admin to log on and capture password
7. use password to access remainder of network

Criminal Enterprise

- organized groups of hackers now a threat
  - corporation / government / loosely affiliated gangs
  - typically young
  - often Eastern European or Russian hackers
  - common target credit cards on e-commerce server
- criminal hackers usually have specific targets
- once penetrated act quickly and get out
- IDS / IPS help but less effective
- sensitive data needs strong protection

Criminal Enterprise Behavior

1. act quickly and precisely to make their activities harder to detect
2. exploit perimeter via vulnerable ports
3. use trojan horses (hidden software) to leave back doors for re-entry
4. use sniffers to capture passwords
5. do not stick around until noticed
6. make few or no mistakes.

Insider Attacks

- among most difficult to detect and prevent
- employees have access & systems knowledge
- may be motivated by revenge / entitlement
  - when employment terminated
  - taking customer data when move to competitor
- IDS / IPS may help but also need:
  - least privilege, monitor logs, strong authentication, termination process to block access & mirror data

Insider Behavior Example

1. create network accounts for themselves and their friends
2. access accounts and applications they wouldn't normally use for their daily jobs
3. e-mail former and prospective employers
4. conduct furtive instant-messaging chats
5. visit web sites that cater to disgruntled employees, such as f'dcompany.com
6. perform large downloads and file copying
7. access the network during off hours.

Intrusion Techniques

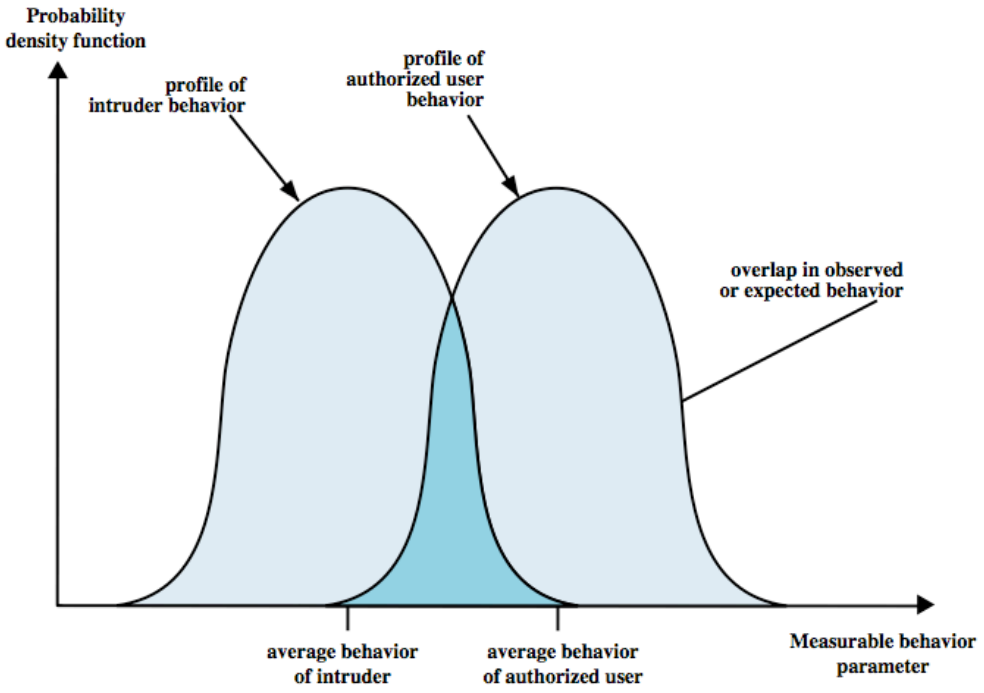
- objective to gain access or increase privileges
- initial attacks often exploit system or software vulnerabilities to execute code to get backdoor
  - e.g. buffer overflow
- or to gain protected information
  - e.g. password guessing or acquisition

Intrusion Detection Systems

- classify intrusion detection systems (IDSs) as:
  - Host-based IDS: monitor single host activity
  - Network-based IDS: monitor network traffic
- logical components:
  - sensors - collect data
  - analyzers - determine if intrusion has occurred
  - user interface - manage / direct / view IDS

IDS Principles

- assume intruder behavior differs from legitimate users
  - expect overlap as shown
  - observe deviations from past history
  - problems of:
    - false positives
    - false negatives
    - must compromise



IDS Requirements

- run continually
- be fault tolerant
- resist subversion
- impose a minimal overhead on system
- configured according to system security policies
- adapt to changes in systems and users
- scale to monitor large numbers of systems
- provide graceful degradation of service
- allow dynamic reconfiguration

Host-Based IDS

- specialized software to monitor system activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions
- two approaches, often used in combination:
  - anomaly detection - defines normal/expected behavior
    - threshold detection
    - profile based
  - signature detection - defines proper behavior

Audit Records

- a fundamental tool for intrusion detection
- two variants:
  - native audit records - provided by O/S
    - always available but may not be optimum
  - detection-specific audit records - IDS specific
    - additional overhead but specific to IDS task
    - often log individual elementary actions
    - e.g. may contain fields for: subject, action, object, exception-condition, resource-usage, time-stamp

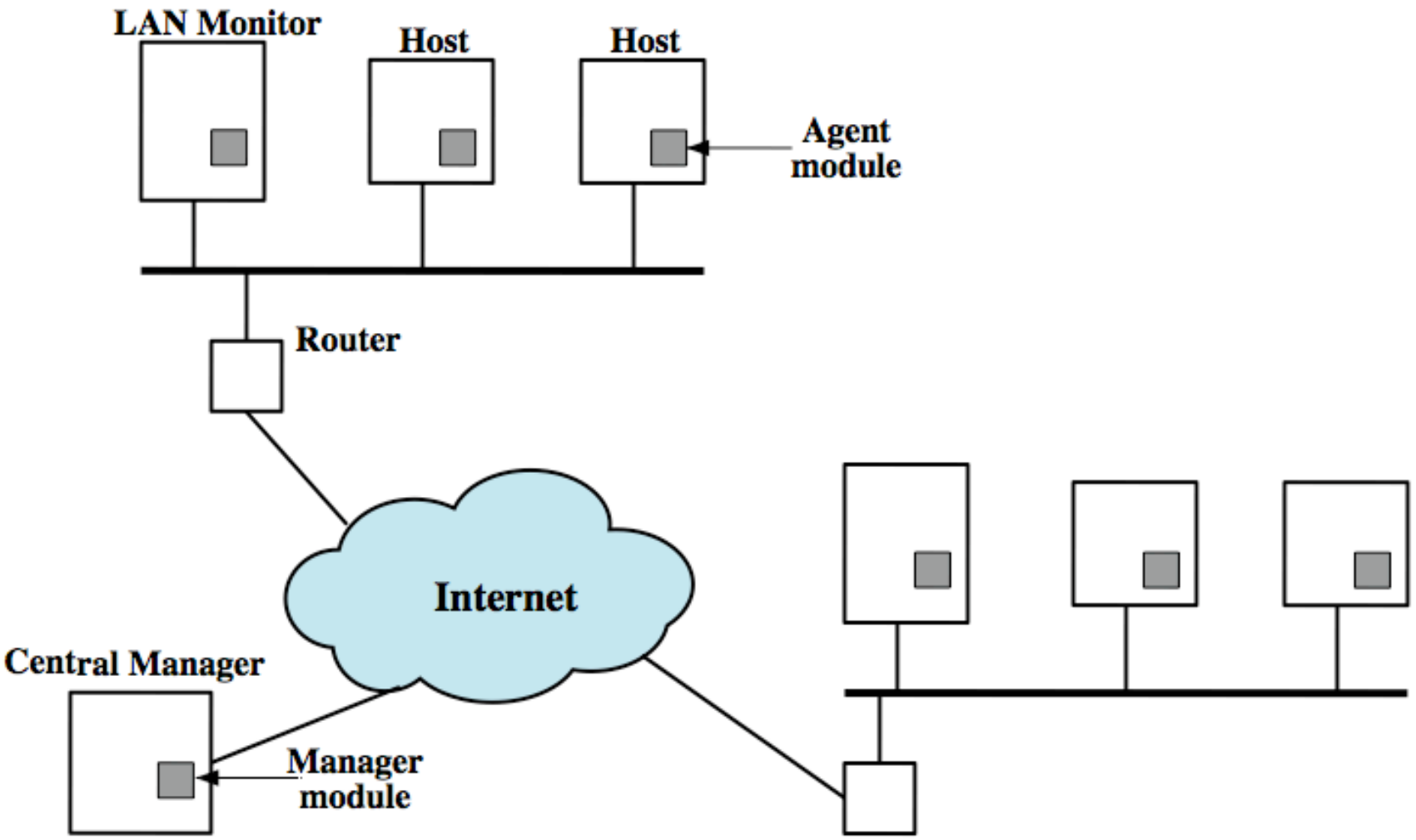
Anomaly Detection

- threshold detection
  - checks excessive event occurrences over time
  - alone a crude and ineffective intruder detector
  - must determine both thresholds and time intervals
- profile based
  - characterize past behavior of users / groups
  - then detect significant deviations
  - based on analysis of audit records
    - gather metrics: counter, guage, interval timer, resource utilization
    - analyze: mean and standard deviation, multivariate, markov process, time series, operational model

Signature Detection

- observe events on system and applying a set of rules to decide if intruder
- approaches:
  - rule-based anomaly detection
    - analyze historical audit records for expected behavior, then match with current behavior
  - rule-based penetration identification
    - rules identify known penetrations / weaknesses
    - often by analyzing attack scripts from Internet
    - supplemented with rules from security experts

Distributed Host-Based IDS



Distributed Host-Based IDS