

Lecture Outline

- Intruders & Intrusion
 - Hackers
 - Criminal groups
 - Insiders

- Detection and IDS
 - Techniques
 - Detection
 - Principles
 - Requirements
 - Host-based
 - Network-based

- Honeypot



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, misfeator, clandestine user

Examples of Intrusion

- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Temporary agents or consultants
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

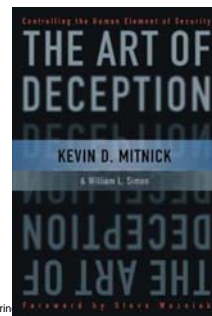
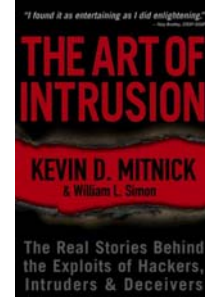
Hackers

- motivated by thrill of access and status
 - hacking community a strong meritocracy
 - status is determined by level of competence
 - share info with fellow hackers
- 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
 - What is the problem here?



Hacker Behavior Example

1. Exploit newly discovered weaknesses and evade detection and countermeasures
2. select target using IP lookup tools
3. map network for accessible services
4. identify potentially vulnerable services
5. brute force (guess) passwords
6. install remote administration tool
7. wait for admin to log on and capture password
8. 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

internet forums like darkmarket.org - [related news](#)



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.

IDSs and IPSs can also be used for these types of attackers, but may be less effective because of the quick in-and-out nature of the attack.

For e-commerce sites, **database encryption** should be used for sensitive customer information, especially credit cards.

For hosted e-commerce sites (provided by an outsider service), **the e-commerce organization should make use of a dedicated server** (not used to support multiple customers) and closely monitor the provider's security services.

Insider Attacks

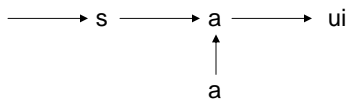
- among most difficult to detect and prevent
- employees have access & systems knowledge
- may be motivated by revenge / entitlement
 - when employment terminated
 - taking customer data when move to competitor
 - Kenneth Peterson cc
 - VP of Sales
- IDS / IPS may help but also need:
 - least privilege,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

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
ratemyboss
6. perform large downloads and file copying
7. access the network during off hours.

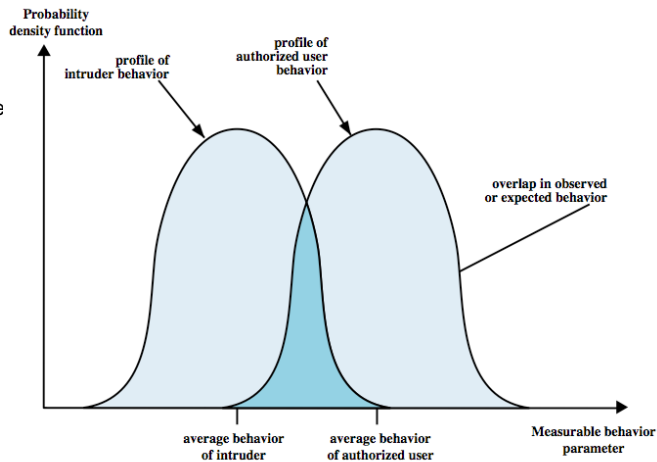
Intrusion Detection Systems

- classify intrusion detection systems (IDSs) as:
 - Host-based IDS: monitor single host activity for suspicious activity
 - Network-based IDS: monitor network traffic
 - Analyzes transport and application activity
- IDS has 3 logical components:
 - sensors - collect data
 - Input: network packet, log files
 - analyzers - determine if intrusion has occurred
 - user interface - manage / direct / view IDS



IDS Principles

- IDS detection based on assumption that intruder behavior differs from legitimate users in ways that can be quantified
 - expect overlap as shown – not b/w
 - observe deviations from past history
 - problems of:
 - false positives
 - false negatives
 - must compromise



CSCI 415: Computer and Network Security

IDS Requirements

- run continually with minimal human supervision.
- be fault tolerant in the sense that it must be able to recover from system crashes and reinitializations.
- resist subversion. The IDS must be able to monitor itself and detect if it has been modified by an attacker.
- impose a minimal overhead on the system where it is running.
- be able to be configured according to the security policies of the system that is being monitored.
- be able to adapt to changes in system and user behavior over time.
- be able to scale to monitor a large number of hosts.
- provide graceful degradation of service in the sense that if some components of the IDS stop working for any reason, the rest of them should be affected as little as possible.
- allow dynamic reconfiguration; that is, the ability to reconfigure the IDS without having to restart it.

CSCI 415: Computer and Network Security

Dr. Nazli Hardy

Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

Host-Based IDS

- specialized software to monitor (vulnerable/ sensitive) 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
- Follow two basic approaches, often used in combination:
 - **anomaly detection** - involves the collection of data relating to the behavior of legitimate users over a period of time.
 - statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.
 - attempt to define normal, or expected, behavior. This approach is effective against masqueraders, who are unlikely to mimic the behavior patterns of the accounts they appropriate. On the other hand, such techniques may be unable to deal with misfeasors. The following are two approaches to statistical anomaly detection:
 - threshold detection: involves defining thresholds, independent of user, for the frequency of occurrence of various events.
 - profile based: of activity of each user used to detect changes in user behavior
 - **signature detection** - defines a set of rules or attack patterns used to decide that a given behavior is that of an intruder.
 - it attempts to define proper behavior and may be able to recognize events and sequences that, in context, reveal penetration

Collection of Data

- a fundamental tool for intrusion detection
- two variants:
 - native audit records - provided by O/S (most multi-user operating systems include accounting software that collects information on user activity)
 - always available but may not be optimum
 - advantage or disadvantage?
 - 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 (Dorothy Denning)

Anomaly Detection

- threshold detection
 - involves counting the number of occurrences of a specific event type over an interval of time
 - checks excessive event occurrences over time
 - must determine both thresholds and time intervals
 - alone a crude and ineffective intruder detector (FP & FN), but useful in conjunction with other techniques

- profile based
 - characterize past behavior of users / groups
 - then detect significant deviations – set of parameters, not single item
 - based on analysis of audit records
 - gather metrics: counter, interval timer, resource utilization (to define typical behavior) – this becomes the input against which to gauge
 - analyze: statistical processes: mean and standard deviation, multivariate, markov process, time series

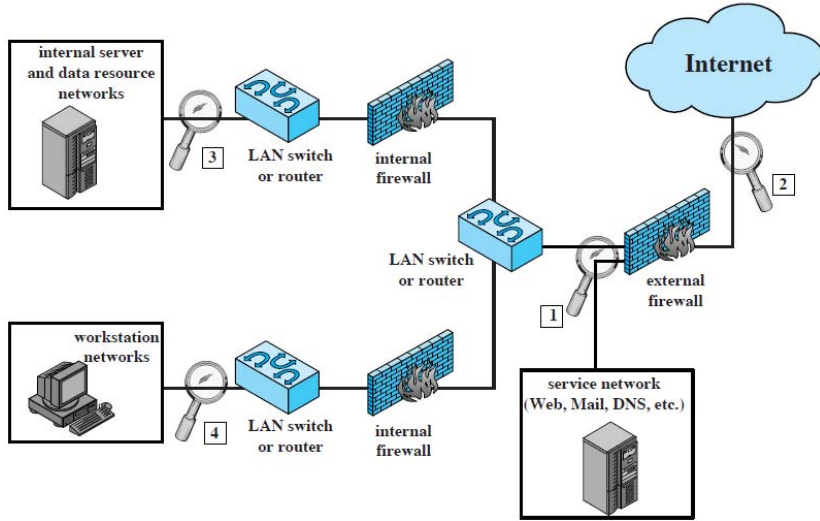
Signature Detection

- observe events on system and applying a set of **rules** to decide if intruder

- approaches:
 - rule-based anomaly detection
 - similar in approach and strengths to statistical anomaly detection
 - historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns
 - rules may represent past behavior patterns of users, programs, privileges, time slots, terminals etc.
 - current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.

 - rule-based penetration identification
 - rules identify known penetrations / weaknesses
 - typically, the rules used in these systems are specific to the machine and operating system
 - often by analyzing attack scripts from Internet
 - supplemented with rules from security experts

Placement of Network-Based IDS



Advantages and Disadvantages of Each Location
