DEALING WITH PATTERNS

- If we want to find something unusual about a system, we need to know something about
  - expected behavior of the system
  - behavior of functionalities
  - whether there are additional, unwanted, functionalities introduced

DEALING WITH PATTERNS

- This is a preliminary discussion about detecting intrusions, or executions that may be abnormal, off-nominal, etc.

INTRUSION DETECTION TERMS

- Just a few words to commonly used terms
  - Misuse detection / Signature detection
  - Anomaly detection

  - False positives
  - False negatives
  - Data overload

DATA MINING

- Restated from SANS Intrusion Detection FAQ
  - http://www.sans.org/resources/idfaq/data_mining.php
  - What is data-mining?
    - According to R.L. Grossman in "Data Mining: Challenges and Opportunities for Data Mining During the Next Decade", he defines data mining as being "concerned with uncovering patterns, associations, changes, anomalies, and statistically significant structures and events in data."
    - Simply put it is the ability to take data and pull from it patterns or deviations which may not be seen easily to the naked eye.
    - Another term sometimes used is knowledge discovery.
- Restated from http://www.sas.com/technologies/data_mining/
    - Data mining is the process of selecting, exploring and modeling large amounts of data to uncover previously unknown patterns for business advantage.

INTRUSION DETECTION AND SURVIVABILITY

- "Recognition is the first step to Recovery"
  - basis for this brief overview of intrusion detection are the "*Intrusion Detection Pages*" at
    - http://www.cerias.purdue.edu/coast/
    - the material below is partially restated from this article
- Intrusion
  - someone attempting to break or misuse the system
- Intrusion Detection System (IDS)
  - attempts to detect an intruder breaking into your system or
  - attempts to detect a legitimate user misusing system resources
  - IDS runs on your system at all time

INTRUSION DETECTION AND SURVIVABILITY

- Outside Intruders
  - what most people are afraid of
- Inside Intruders
  - FBI studies have revealed that vast majority of intrusions and attacks come from within organizations.
  - an insider knows
    - layout of your system
    - where the valuable data is
    - what security precautions are in place
  - survivability methods must face the same issues for both types of intruders

INTRUSION DETECTION AND SURVIVABILITY

- Security Policy
  - defines what is permitted and what is denied on a system
  - Prohibitive
    - where everything that is not expressly permitted is denied.
  - Permissive
    - where everything that is not expressly denied is permitted.
  - Trying to use full potential of computers assumes certain freedoms of behavior
    - does not work well for detecting malicious behavior
    - unless: there is a notion of trust between the users
    - however: what if the population of trusted users has been invaded?
  - enforced set of rules would maintain every user's privacy and integrity
  - rules must be enforced (and be seen to be enforced)

INTRUSION DETECTION AND SURVIVABILITY

- Elements of System's Security
  - Availability
    - system must be available for use when the users need it.
    - critical data must be available at all times.
  - Utility
    - system, and data on the system, must be useful for a purpose
  - Integrity
    - system and its data must be complete, whole, and in a readable condition

INTRUSION DETECTION AND SURVIVABILITY

- Elements of System's Security cont.
  - Authenticity
    - able to verify the identity of users
    - users should be able to verify the identity of the system
  - Confidentiality
    - private data should be known only to the owner or a chosen few
  - Possession
    - owners of the system must be able to control it
    - losing control of system to malicious user affects security of system for all other users.

INTRUSION DETECTION AND SURVIVABILITY

- Intrusion Classification
  - Intrusion definition
    - any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
  - Two main classes
    - Misuse
      - intrusions are well defined attacks on known weak points of a system.
      - can be detected by watching for certain actions being performed on certain objects.
    - Anomaly
      - intrusions are based on observations of deviations from normal system usage patterns.
      - they are detected by building up a profile of the system being monitored, and detecting significant deviations from this profile.

INTRUSION DETECTION AND SURVIVABILITY

- Misuse Intrusions follow well-defined patterns
  - can be detected by pattern matching on audit-trail information
- Anomalous Intrusions
  - detected by observing significant deviations from normal behavior
  - classic model:
    - a model is built which contains metrics that are derived from system operation
    - metric is defined as a random variable *x* representing a quantitative measure accumulated over a period
    - metrics are computed from available system parameters such as
      - average CPU load,
      - number of network connections per minute,
      - number of processes per user, etc.

INTRUSION DETECTION AND SURVIVABILITY

- Anomalous Intrusions (cont.)
  - Anomaly may be a symptom of a possible intrusion
    - exploitation of a system's vulnerabilities involves abnormal use of the system; therefore, security violations could be detected from abnormal patterns of system usage
      - [Denning, IEEE Trans on Software Engineering, 13(2):222-232, February 1987]
  - Anomaly detection has also been performed through other mechanisms,
    - such as neural networks
    - machine learning classification techniques
    - mimicking of the biological immune systems
  - Anomalous intrusions are harder to detect

INTRUSION DETECTION AND SURVIVABILITY

- Intrusion Detection Characteristics
  - must **run continually**,
    - should be examinable from outside.
  - must be **fault tolerant**
    - in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart
  - must **resist subversion**
    - use self diagnosis to determine if intrusion detection systems has been compromised

INTRUSION DETECTION AND SURVIVABILITY

- Intrusion Detection Characteristics cont.
  - **minimal overhead** on the system
  - must **observe deviations** from normal behavior
  - must be easily tailored to the system
    - every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns
  - must cope with **changing system behavior** over time
  - must be **difficult to fool**

INTRUSION DETECTION AND SURVIVABILITY

- Type of errors likely to occur
  - false positive
    - occurs when system classifies action as anomalous (a possible intrusion) when it is a legitimate action
      - will lead users of the intrusion detection system to ignore its output
      - classify legitimate actions as intrusions
      - if too many false positives are generated, the operators will come to ignore the output of the system over time, which may lead to an actual intrusion being detected but ignored by the users

INTRUSION DETECTION AND SURVIVABILITY

- false negative
  - occurs when actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.
    - more serious than false positive errors because they give a misleading sense of security
    - suspicious action will not be brought to the attention of the operator
    - intrusion detection system is now a liability

INTRUSION DETECTION AND SURVIVABILITY

- subversion errors
  - occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.
    - more complex and tie in with false negative errors
    - intruder could use knowledge about the internals of an intrusion detection system to alter its operation
  - could fool system over time
    - slowly changing over to new usage pattern,
    - gradually letting the system update its notion of normal system usage

INTRUSION DETECTION AND SURVIVABILITY

- Survivability of Intrusion Detection Systems
  - the IDS can be seen as an essential service
  - need to access logging information to determine what happened
  - this information could be used for adopting a good recovery strategy
  - two points of view
    - intrusion detection is first step, initiating recovery and thus survivability
    - on the other hand, survivability mechanisms can be used as intrusion detection systems
      - e.g. fault masking mechanisms indicate when there is disagreement

INTRUSION DETECTION AND SURVIVABILITY

Conclusion

- an Intrusion Detection System should be part of an overall Survivability Approach
  - i.e., it should be an integral part of the Survivable System

- There are many IDS systems & projects out there
  - check out some of the projects at

    http://www-rnks.informatik.tu-cottbus.de/en/node/209 or

    http://isl.cse.sc.edu/mirrorSobireys.shtml