COMP 290-040
Network Intrusion Detection

Introduction & Overview

Kevin Jeffay
Department of Computer Science
University of North Carolina at Chapel Hill
jeffay@cs.unc.edu
January 19, 2005

http://www.cs.unc.edu/~jeffay/courses/nidsS05

©2005 by Kevin Jeffay

Network Intrusion Detection
Background & History

- Intrusion detection is the new cool systems topic!
  - » That started in the early 70s…
- The good olde days…
  - » Centralized systems
  - » Primary concern was untrusted "insiders" gaining access to unauthorized information
    - ❖ Legit users doing inappropriate things
  - » Primary source of the problem: too many unforeseen ways people could access memory
    - ❖ Invalid assumptions made by programmers
    - ❖ Systems designed to aid debugging or add new function ("new paradigm") could be corrupted
    - ❖ Configuration problems ("user error")

©2005 by Kevin Jeffay

Network Intrusion Detection
History

- Intrusions detected through audit of logs
  - » Develop models of normal usage
  - » Instrument system to log "significant events"
    - ❖ Events, counts, timestamps, durations, usage, …
  - » Detect anomalies
- Problems:
  - » False alarms
  - » "Normal" a slippery concept
  - » What if user covers their tracks?
  - » Intrusiveness of the detection system
- Distributed systems and the ability to edit logs led to network-based IDS

©2005 by Kevin Jeffay

Network Intrusion Detection
IDS Today

- Still grappling with the same fundamental problems
  - » System "features" can be exploited for unintended purposes
  - » Issue today is largely denial-of-service rather than access to sensitive information
    - ❖ Much easier ways to get this…
- IDS still largely network-based
- New(er) issues:
  - » Resource usage attacks
  - » Scale
    - ❖ Time, distance, effect, …

©2005 by Kevin Jeffay

Network Intrusion Detection
Detection basics

- Monitor network traffic…
  - » Decentralized end-system monitoring
  - » Centralized network-based monitoring
  - » Performance problems abound!
- Detect an intrusion — the signal detection problem
  - » Signal: An intrusion
  - » Noise: Normal traffic
  - » Classical approach: Learn distributions of each and classify each new X as it is observed

©2005 by Kevin Jeffay

Network Intrusion Detection
Detection basics

- Signal-only detection ("signature" based detection)
  - » You know what an intrusion "looks like" and explicitly look for it
- Noise-only detection ("anomaly detection")
  - » You know what normal traffic looks like and detect significant perturbations from normal
- Both assume you have a good characterization of the world

©2005 by Kevin Jeffay

Network Intrusion Detection
Signature detection basics

- Textual pattern matching
- Protocol field matching
- Packet pattern matching
- Always assumes you know what you are looking for!
- Pros:
  - » Low false alarm rate
- Cons:
  - » Can only detect yesterday's intrusions (high "false-negative" rate)
  - » Small deviations can defeat (cat & mouse syndrome)

©2005 by Kevin Jeffay

Network Intrusion Detection
Anomaly detection basics

- When is "strange" bad?
- Techniques
  - » Component analysis
  - » AI techniques
  - » Immunology
- Pros:
  - » Can recognize new attacks
- Cons:
  - » Requires training
  - » Can't classify or name attacks
  - » False alarms
  - » What if attacks evolve so slowly they appear normal?
  - » Is fundamental premise true?

©2005 by Kevin Jeffay

Network Intrusion Detection
Course pseudo-outline

- How to hack a system
  - » How to make a machine your slave
  - » How to build your own zombie army and take over the world
- What you can do with your army ("How to Own the Internet in Your Spare Time" by Staniford, Paxson, Weaver)
  - » Actual attacks
    - ❖ Worms, viruses, DoS, DDoS, …
  - » Theoretical attacks ("when smart people go bad")
    - ❖ Protocol attacks
    - ❖ Congestion control attacks

©2005 by Kevin Jeffay

Network Intrusion Detection
Course pseudo-outline

- Intrusion detection
  - » Measurement methods, practices, and limits
    - ❖ Direct measurement
    - ❖ Indirect measurement ("backscatter," "Internet background radiation")
  - » Data mining
    - ❖ Automatic extraction of features
  - » Internet signal processing
    - ❖ Component analysis
  - » Machine learning
    - ❖ Other AI techniques…
  - » Honeypots and tarpits
  - » IDS evasion & attacks on IDS
  - » State of practice

©2005 by Kevin Jeffay

Network Intrusion Detection
Course pseudo-outline

- Mitigation — practice
  - » Filtering
  - » Traffic normalization
- Mitigation — theory
  - » Fingerprinting — Finding the sources of attacks
  - » DoS-free protocol design

©2005 by Kevin Jeffay