

Intrusion Detection

CS 239

Computer Software

March 7, 2006

CS 239, Winter 2006

Lecture 15
Page 1

Outline

- Introduction
- Characteristics of intrusion detection systems
- Some sample intrusion detection systems

CS 239, Winter 2006

Lecture 15
Page 2

Introduction

- Many mechanisms exist for protecting systems from intruders
 - Access control, firewalls, authentication, etc.
- They all have one common characteristic:
 - They don't always work

CS 239, Winter 2006

Lecture 15
Page 3

Intrusion Detection

- Work from the assumption that sooner or later your security measures will fail
- Try to detect the improper behavior of the intruder who has defeated your security
- Inform the system or system administrators to take action

CS 239, Winter 2006

Lecture 15
Page 4

Why Intrusion Detection?

- If we can detect bad things, can't we simply prevent them?
- Possibly not:
 - May be too expensive
 - May involve many separate operations
 - May involve things we didn't foresee

CS 239, Winter 2006

Lecture 15
Page 5

For Example,

- Your intrusion detection system regards setting uid on root executables as suspicious
 - Yet the system must allow the system administrator to do so
- If the system detects several such events, it becomes suspicious
 - And reports the problem

CS 239, Winter 2006

Lecture 15
Page 6

Couldn't the System Just Have Stopped This?

- Perhaps, but -
- The real problem was that someone got root access
 - The changing of setuid bits was just a symptom
- And under some circumstances the behavior is legitimate

CS 239, Winter 2006

Lecture 15
Page 7

Intrusions

- “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource”¹
- Which covers a lot of ground
 - Implying they're hard to stop

¹Heady, Luger, Maccabe, and Servilla, “The Architecture of a Network Level Intrusion Detection System,” Tech Report, U. of New Mexico, 1990.

CS 239, Winter 2006

Lecture 15
Page 8

Is Intrusion Really a Problem?

- Is intrusion detection worth the trouble?
- Yes, at least for some installations
- Consider the experience of NetRanger intrusion detection users

CS 239, Winter 2006

Lecture 15
Page 9

The NetRanger Data

- Gathered during 5 months of 1997
 - Old, but not too much data like this is ever made public
- From all of NetRanger's licensed customers
- A reliable figure, since the software reports incidents to the company

CS 239, Winter 2006

Lecture 15
Page 10

NetRanger's Results

- 556,464 security alarms in 5 months
- Some serious, some not
 - “Serious” defined as attempting to gain unauthorized access
- For NetRanger customers, serious attacks occurred .5 to 5 times per month
 - Electronic commerce sites hit most

CS 239, Winter 2006

Lecture 15
Page 11

Kinds of Attacks Seen

- Often occurred in waves
 - When someone published code for a particular attack, it happened a lot
 - Because of “Script Kiddies”
- 100% of web attacks were on web commerce sites

CS 239, Winter 2006

Lecture 15
Page 12

Where Did Attacks Come From?

- Just about everywhere
- 48% from ISPs
- But also attacks from major companies, business partners, government sites, universities, etc.
- 39% from outside US
 - Only based on IP address, though

CS 239, Winter 2006

Lecture 15
Page 13

Kinds of Intrusions

- External intrusions
- Internal intrusions

CS 239, Winter 2006

Lecture 15
Page 14

External Intrusions

- What most people think of
- An unauthorized (usually remote) user trying to illicitly access your system
- Using various security vulnerabilities to break in
- The typical case of a hacker attack

CS 239, Winter 2006

Lecture 15
Page 15

Internal Intrusions

- An authorized user trying to gain privileges beyond those he is entitled to
- No longer the majority of problems
 - But often the most serious ones
- More dangerous, because insiders have a foothold and know more

CS 239, Winter 2006

Lecture 15
Page 16

Basics of Intrusion Detection

- Watch what's going on in the system
- Try to detect behavior that characterizes intruders
- While avoiding improper detection of legitimate access
- Hopefully all at a reasonable cost

CS 239, Winter 2006

Lecture 15
Page 17

Intrusion Detection and Logging

- A natural match
- The intrusion detection system examines the log
 - Which is being kept, anyway
- Secondary benefits of using the intrusion detection system to reduce the log

CS 239, Winter 2006

Lecture 15
Page 18

On-Line Vs. Off-Line Intrusion Detection

- Intrusion detection mechanisms can be complicated and heavy-weight
- Perhaps better to run them off-line
 - E.g., at nighttime
- Disadvantage is that you don't catch intrusions as they happen

CS 239, Winter 2006

Lecture 15
Page 19

Failures In Intrusion Detection

- False positives
 - Legitimate activity identified as an intrusion
- False negatives
 - An intrusion not noticed
- Subversion errors
 - Attacks on the intrusion detection system

CS 239, Winter 2006

Lecture 15
Page 20

Desired Characteristics in Intrusion Detection

- Continuously running
- Fault tolerant
- Subversion resistant
- Minimal overhead
- Must observe deviations
- Easily tailorable
- Evolving
- Difficult to fool

CS 239, Winter 2006

Lecture 15
Page 21

Host Intrusion Detection

- Run the intrusion detection system on a single computer
- Look for problems only on that computer
- Often by examining the logs of the computer

CS 239, Winter 2006

Lecture 15
Page 22

Advantages of the Host Approach

- Lots of information to work with
- Only need to deal with problems on one machine
- Can get information in readily understandable form

CS 239, Winter 2006

Lecture 15
Page 23

Network Intrusion Detection

- Do the same for a local (or wide) area network
- Either by using distributed systems techniques
- Or (more commonly) by sniffing network traffic

CS 239, Winter 2006

Lecture 15
Page 24

Advantages of Network Approach

- Need not use up any resources on users' machines
- Easier to properly configure for large installations
- Can observe things affecting multiple machines

CS 239, Winter 2006

Lecture 15
Page 25

Network Intrusion Detection and Data Volume

- Lots of information passes on the network
- If you grab it all, you will produce vast amounts of data
- Which will require vast amounts of time to process

CS 239, Winter 2006

Lecture 15
Page 26

Network Intrusion Detection and Sensors

- Use programs called sensors to grab only relevant data
- Sensors quickly examine network traffic
 - Record the relevant stuff
 - Discard the rest
- If you design sensors right, greatly reduces the problem of data volume

CS 239, Winter 2006

Lecture 15
Page 27

Styles of Intrusion Detection

- Misuse intrusion detection
 - Try to detect things known to be bad
- Anomaly intrusion detection
 - Try to detect deviations from normal behavior
- Specification intrusion detection
 - Try to detect deviations from defined “good states”

CS 239, Winter 2006

Lecture 15
Page 28

Misuse Detection

- Determine what actions are undesirable
- Watch for those to occur
- Signal an alert when they happen
- Often referred to as *signature detection*

CS 239, Winter 2006

Lecture 15
Page 29

Level of Misuse Detection

- Could look for specific attacks
 - E.g., Syn attacks or IP spoofing
- But that only detects already-known attacks
- Better to also look for known suspicious behavior
 - Like trying to become root
 - Or changing file permissions

CS 239, Winter 2006

Lecture 15
Page 30

How Is Misuse Detected?

- By examining logs
 - Only works after the fact
- By monitoring system activities
 - Often hard to trap what you need to see
- By scanning the state of the system
 - Can't trap actions that don't leave traces
- By sniffing the network
 - For network intrusion detection systems

CS 239, Winter 2006

Lecture 15
Page 31

Pluses and Minuses of Misuse Detection

- + Few false positives
- + Simple technology
- + Hard to fool
 - Only detects known problems
 - Gradually becomes less useful if not updated
- Sometimes signatures are hard to generate

CS 239, Winter 2006

Lecture 15
Page 32

Misuse Detection and Commercial Systems

- Essentially all commercial intrusion detection systems detect misuse
 - Primarily using signatures of attacks
- Many of these systems are very similar
 - With only different details
- Differentiated primarily by quality of their signature library
 - How large, how quickly updated

CS 239, Winter 2006

Lecture 15
Page 33

Anomaly Detection

- Misuse detection can only detect known problems
- And many potential misuses can also be perfectly legitimate
- Anomaly detection instead builds a model of valid behavior
 - And watches for deviations

CS 239, Winter 2006

Lecture 15
Page 34

Methods of Anomaly Detection

- Statistical models
 - User behavior
 - Program behavior
 - Overall system/network behavior
- Expert systems
- Misuse detection and anomaly detection sometimes blur together

CS 239, Winter 2006

Lecture 15
Page 35

Pluses and Minuses of Anomaly Detection

- + Can detect previously unknown attacks
- Hard to identify and diagnose nature of attacks
- Unless careful, may be prone to many false positives
- Depending on method, can be expensive and complex

CS 239, Winter 2006

Lecture 15
Page 36

Anomaly Detection and Academic Systems

- Most academic research on IDS in this area
 - More interesting problems
 - Greater promise for the future
- But few really effective systems currently use it
 - Not entirely clear that will ever change

CS 239, Winter 2006

Lecture 15
Page 37

Specification Detection

- Define some set of states of the system as good
- Detect when the system is in a different state
- Signal a problem if it is

CS 239, Winter 2006

Lecture 15
Page 38

How Does This Differ From Misuse and Anomaly Detection?

- Misuse detection says that certain things are bad
- Anomaly detection says deviations from statistically normal behavior are bad
- Specification detection specifies exactly what is good and calls the rest bad
- A relatively new approach

CS 239, Winter 2006

Lecture 15
Page 39

Some Challenges

- How much state do you have to look at?
 - Typically dealt with by limiting observation to state relevant to security
- How do you specify a good state?

CS 239, Winter 2006

Lecture 15
Page 40

Pluses and Minuses of Anomaly Detection

- + Allows formalization of what you're looking for
- + Limits where you need to look
- + Can detect unknown attacks
- Not very well understood yet
- Based on locating right states to examine

CS 239, Winter 2006

Lecture 15
Page 41

Customizing and Evolving Intrusion Detection

- A single intrusion detection solution is impossible
 - Good behavior on one system is bad behavior on another
 - Behaviors change and new vulnerabilities are discovered
- Intrusion detection systems must change to meet needs

CS 239, Winter 2006

Lecture 15
Page 42

How Do Intrusion Detection Systems Evolve?

- Manually or semi-automatically
 - New information added that allows them to detect new kinds of attacks
- Automatically
 - Deduce new problems or things to watch for without human intervention

CS 239, Winter 2006

Lecture 15
Page 43

A Problem With Evolving Intrusion Detection Systems

- Very clever intruders can use the evolution against them
- Instead of immediately performing dangerous actions, evolve towards them
- If the intruder is more clever than the system, the system gradually accepts the new behavior

CS 239, Winter 2006

Lecture 15
Page 44

Practicalities of Operation

- Most commercial intrusion detection systems are add-ons
 - They run as normal applications
- They must make use of readily available information
 - Audit logged information
 - Sniffed packets
 - Output of systems calls they make
- And performance is very important

CS 239, Winter 2006

Lecture 15
Page 45

Practicalities of Audit Logs for IDS

- Operating systems only log certain stuff
- They don't necessarily log what an intrusion detection system really needs
- They produce large amounts of data
 - Expensive to process
 - Expensive to store
- If attack was successful, may be corrupted

CS 239, Winter 2006

Lecture 15
Page 46

What Does an IDS Do When It Detects an Attack?

- Automated response
 - Shut down the “attacker”
 - Or more carefully protect the attacked service
- Alarms
 - Notify a system administrator
 - Who investigates and takes action

CS 239, Winter 2006

Lecture 15
Page 47

Consequences of the Choices

- Automated
 - Too many false positives and your network stops working
 - Is the automated response effective?
- Alarm
 - Too many false positives and your administrator ignores them
 - Is the administrator able to determine what's going on fast enough?

CS 239, Winter 2006

Lecture 15
Page 48

Intrusion Prevention Systems

- Essentially a new buzzword for IDS that takes automatic action when intrusion is detected
- Goal is to quickly take remedial actions to threats
- Since IPSs are automated, false positives could be very, very bad
- “Poor man’s” version is IDS controlling a firewall

CS 239, Winter 2006

Lecture 15
Page 49

Sample Intrusion Detection Systems

- Emerald
- NetRanger
- Snort

CS 239, Winter 2006

Lecture 15
Page 50

Emerald

- From SRI
- In a family of intrusion detection systems
 - IDES and NIDES were earlier versions
- Addresses practical intrusion detection problems
 - Heterogeneity
 - Scaling
 - Multiple levels of abstraction

CS 239, Winter 2006

Lecture 15
Page 51

Emerald Characteristics

- Combines multiple approaches to detecting problems
- Has built-in capabilities to invoke code to deal with problems
- Component-based architecture
- Intended to scale well

CS 239, Winter 2006

Lecture 15
Page 52

Emerald Architecture

- Divided into generic components and specific object components
- Generic components provide base engine for intrusion detection
 - No code relating to specific events or characteristics here
- Bulk of code in specific object components
- Highly configurable and pluggable architecture

CS 239, Winter 2006

Lecture 15
Page 53

Emerald Components

- Object Monitors
 - Watch for intrusions on particular types of system objects
- Signature Engines
 - Analyzes behavior to find problems
- Profiler Engines
 - Statistically -based subsystem to watch for unusual behavior
- Resolvers
 - Implements monitor’s response policy

CS 239, Winter 2006

Lecture 15
Page 54

NetRanger

- Now bundled into Cisco products
- For use in network environments
 - “Sensors” in promiscuous mode capture packets off the local network
- Examines data flows
 - Raises alarm for suspicious flows
- Using misuse detection techniques
 - Based on a signature database

CS 239, Winter 2006

Lecture 15
Page 55

Snort

- Popular open source network intrusion detection system
 - Analyzes all traffic on local network
- Uses language approach for describing acceptable/unacceptable traffic
- Detection engines allows other plugins
- Widely used
 - Free
 - Highly configurable
 - Performance (reputedly) not so great

CS 239, Winter 2006

Lecture 15
Page 56

Are Intrusion Detection Systems Useful?

- A good question
- They are widely used
 - 72% of respondents in CSI/FBI survey use them
 - 35% use intrusion prevention systems
- Some feel they don't yet meet their promise
- But they definitely are improving

CS 239, Winter 2006

Lecture 15
Page 57