Intrusion Detection Systems
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Outline

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

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*

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

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

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

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

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

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

Kinds of Intrusions

- External intrusions
- Internal intrusions

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

Internal Intrusions

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

Information From 2010 Verizon Report[1]

- Combines Verizon data with US Secret Service data
- Indicates external breaches still most common
- But insider attack components in 48% of all cases
  - Some involved both insiders and outsiders

[1] http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf