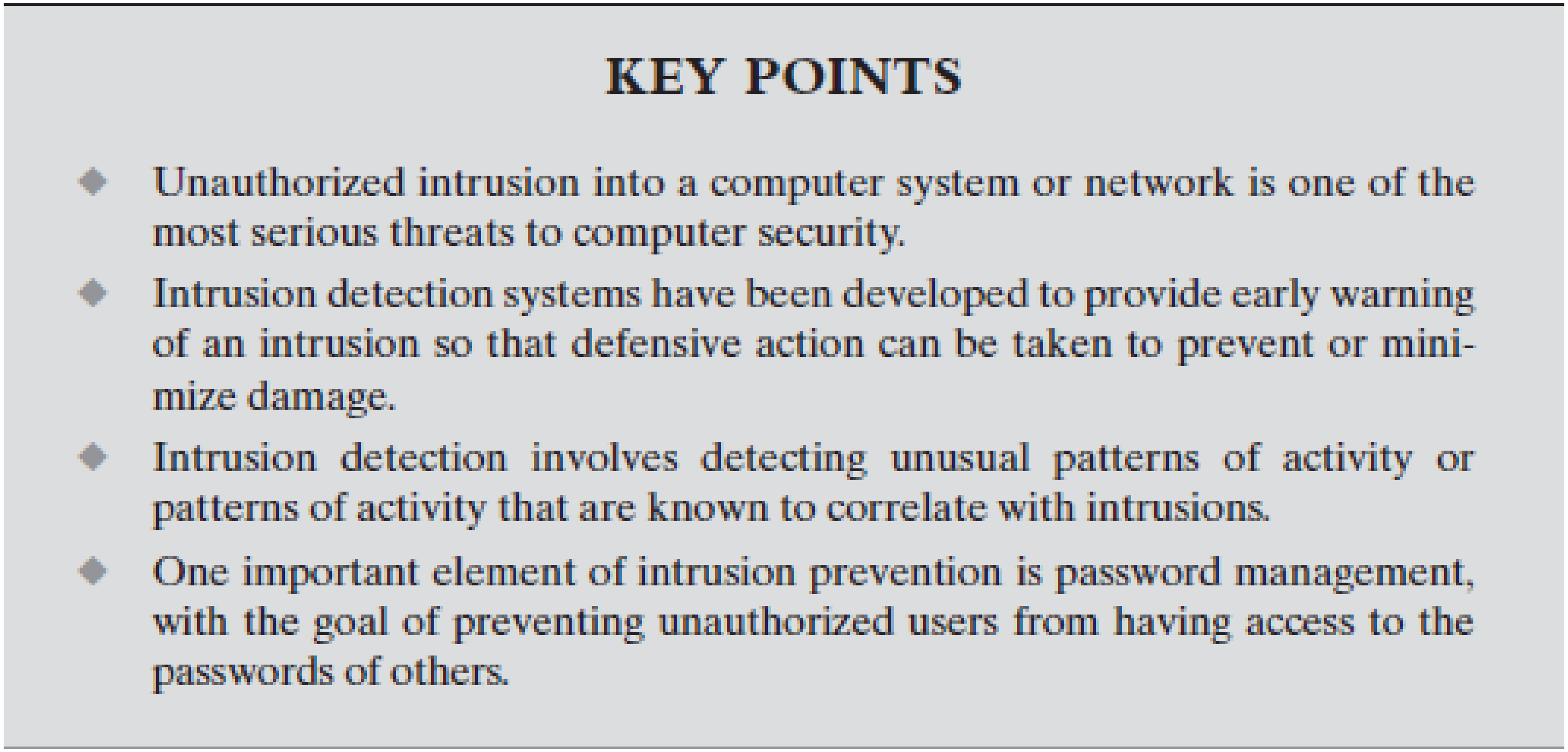
Chapter 20

Intruders

Contents

- problem of intrusion, behavior and techniques
- intrusion detection (statistical & rule-based)
- password management



KEY POINTS

- Unauthorized intrusion into a computer system or network is one of the most serious threats to computer security.
- Intrusion detection systems have been developed to provide early warning of an intrusion so that defensive action can be taken to prevent or minimize damage.
- Intrusion detection involves detecting unusual patterns of activity or patterns of activity that are known to correlate with intrusions.
- One important element of intrusion prevention is password management, with the goal of preventing unauthorized users from having access to the passwords of others.

Intruders

- Generally referred to as hacker, cracker.
- Intruders trespass networked system through unauthorized login to use a system, they may by a local or remote users or software: virus, worm, or Trojan horse.

- **Intruders Classification:**
  - **Masquerader:** An individual who is not authorized to use the computer
  - **Misfeasor:** A legitimate user who accesses unauthorized data, programs, or resources
  - **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

- **Varying levels of competence:**
  - Intruder attacks range from the benign (simply exploring net to see what is there); to the serious (who attempt to read privileged data, perform unauthorized modifications, or disrupt system).

Examples of Intrusion

- Performing a remote root compromise of an e-mail server
- 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
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- 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

Hacker Behavior Example

1. Select target using IP lookup tools
2. Map network for accessible services
3. Identify potentially vulnerable services
4. Brute force (guess) passwords
5. Install remote administration tool
6. Wait for admin to log on and capture password
7. Use password to access remainder of network

Intrusion Techniques

- Aim to gain access and/or increase privileges on a system
- Often use system / software vulnerabilities
- Key goal often is to acquire passwords
  - Access rights as an owner
- Basic attack methodology
  - Target acquisition and information gathering
  - Initial access
  - Privilege access

Password Guessing

- One of the most common attacks
- Attacker knows a login (from email/web page …. etc)
- Attempts to guess password for it
  - defaults, short passwords, common word searches
  - user info (variations on names, birthday, phone, common words/interests)
  - exhaustively searching all possible passwords
- Check by login or against stolen password file
- Success depends on password chosen by user
- Surveys show many users choose poorly
- If have to actually attempt to login to check guesses, then system should detect an abnormal number of failed logins, and hence trigger appropriate countermeasures by admins /security.

Password Capture

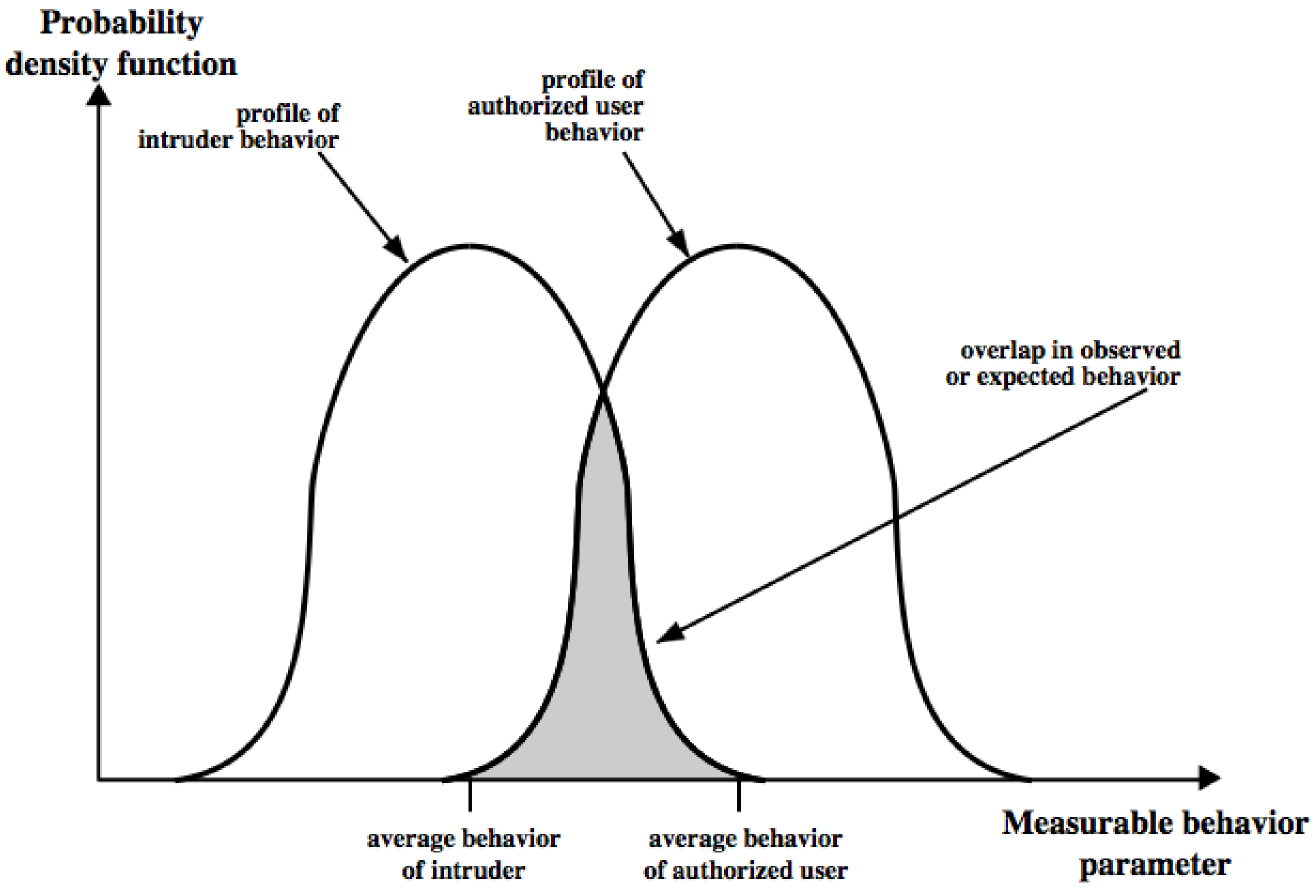
- Another attack involves **password capture**
  - Watching over shoulder as password is entered
  - Using a trojan horse program to collect
  - Monitoring an insecure network login
    - eg. telnet, FTP, web, email
  - Extracting recorded info after successful login (web history/cache, last number dialed etc)
- Using valid login/password can impersonate user
- Users need to be educated to use suitable precautions/ countermeasures

Intrusion Detection

- Will have security failures
- So need also to detect intrusions so can
  - Block if detected quickly
  - Act as deterrent
  - Collect info to improve security
- Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified.

Intrusion Detection

- **Overlap between intruder and authorized user behaviors leads to:**
  - false positives: authorized users identified as intruders.
  - false negatives: Intruders is not identified as intruders.


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

Intrusion Detection Approaches

1. **Signature based IDS:** Signature detection involves searching network traffic for a series of bytes or packet sequences known to be malicious.
2. **Anomaly (Abnormally) based IDS:**

   2.1. Statistical anomaly detection: collect data relating to the behavior of legitimate users, then use statistical tests to determine with a high level of confidence whether new behavior is legitimate user behavior or not.

   a. **Threshold detection:** define thresholds, independent of user, for the frequency of occurrence of events.

   b. **Profile based:** develop profile of activity of each user and use to detect changes in the behavior

   2.2. Rule-based detection: attempt to define a set of rules used to decide if given behavior is an intruder

   a. **Anomaly detection:** rules detect deviation from previous usage patterns

   b. **Penetration identification:** expert system approach that searches for suspicious behavior

Statistical Anomaly Detection

- **Threshold detection**
  - count occurrences of specific event over time
  - if exceed reasonable value assume intrusion
  - alone is a simple & ineffective detector

- **Profile based**
  - characterize past behavior of users
  - detect significant deviations from this
  - profile usually multi-parameter

Rule-Based Intrusion Detection

- Observe events on system & apply rules to decide if activity is suspicious or not
- **Rule-based anomaly detection**
  - Analyze historical audit records to identify usage patterns & auto-generate rules for them
  - Then observe current behavior & match against rules to see if conforms
  - like statistical anomaly detection does not require prior knowledge of security flaws

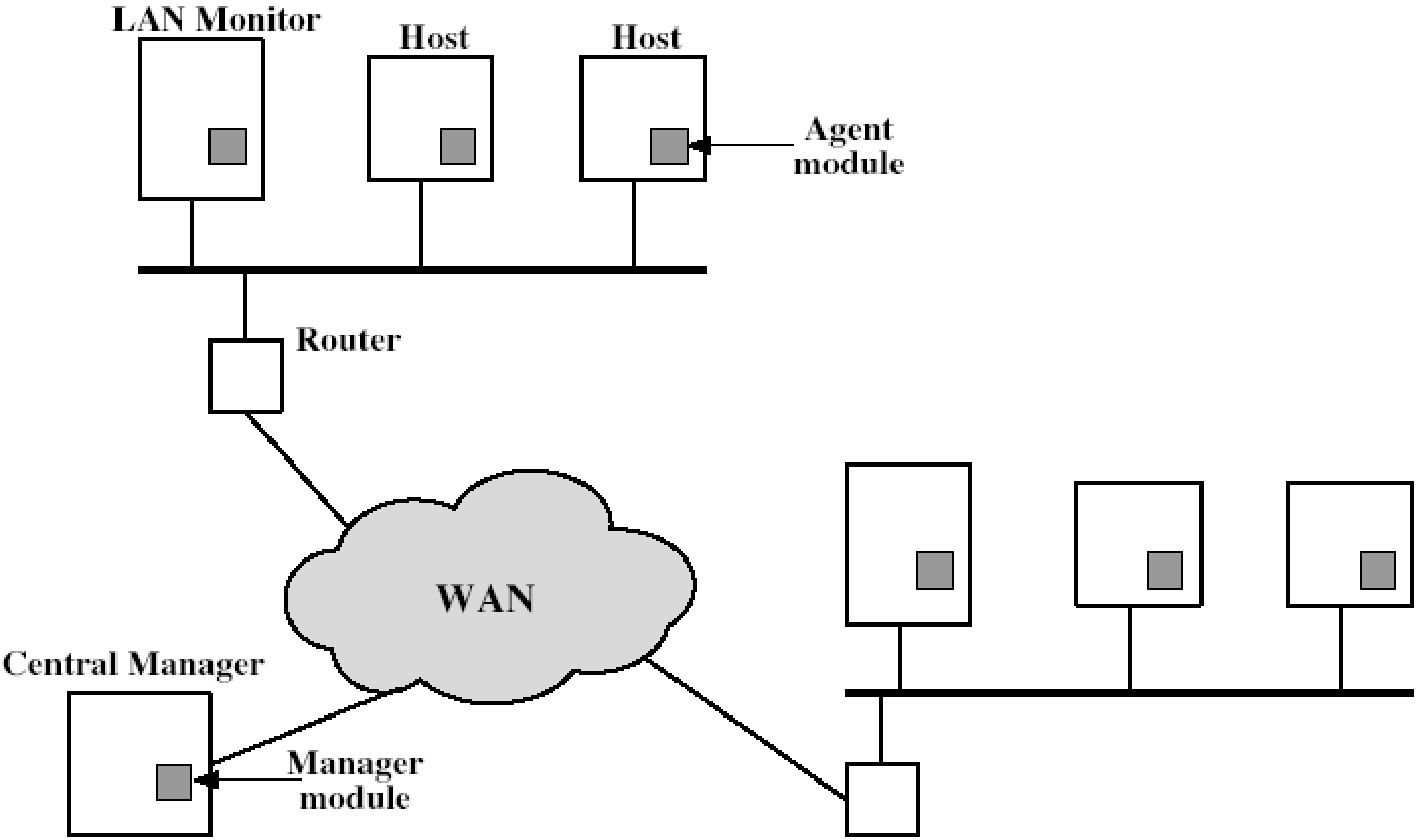
Rule-Based Intrusion Detection

- **Rule-based penetration identification**
  - Uses expert systems technology
  - With rules identifying known penetration, weakness patterns, or suspicious behavior
  - Compare audit records or states against rules
  - Rules usually machine & O/S specific
  - Rules are generated by experts who interview & sort knowledge of security admins
  - Quality depends on how well this is done

Distributed Intrusion Detection System (DIDS)

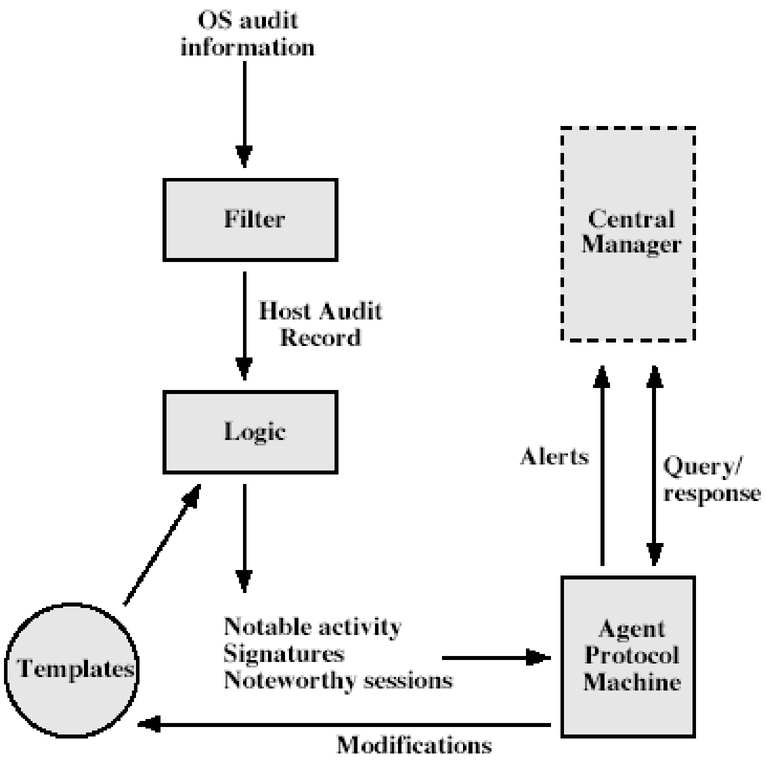
- Traditional focus is on single systems, but typically have networked systems
- More effective defense has these working together to detect intrusions
- Issues
  - Integrity & confidentiality of networked data
  - Centralized or decentralized architecture

- DIDS Architecture consists of three components:
  - Host agent module: audit collection module operating as a background process on a monitored system
  - LAN monitor agent module: like a host agent module except it analyzes LAN traffic
  - Central manager module: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion



DIDS –Agent Implementation

- The agent captures each native O/S audit record & applies a filter that retains only records of security interest.
- These records are then reformatted into a standardized format (HAR).
- Then a template-driven logic module analyzes the records for suspicious activity.
- When suspicious activity is detected, an alert is sent to the central manager.
- The central manager includes an expert system that draw inferences from received data.
- The manager may also query individual systems for copies of HARs to correlate with those from other agents.



Honeypots

- Honeypots are decoy systems, designed to lure a potential attacker away from critical systems, and:
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker’s activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- These systems are filled with fabricated information designed to appear valuable but which any legitimate user of the system wouldn’t access, thus, any access is suspect.
- They are instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker’s activities.
- Have seen evolution from single host honeypots to honeynets of multiple dispersed systems.

Password Management

- Front-line defense against intruders
- Users supply both:
  - login –determines privileges of that user
  - password –to identify them
- Passwords often stored encrypted
  - Unix uses multiple DES (variant with salt)
  - More recent systems use crypto hash function
- Should protect password file on system

Managing Passwords - Education

- Can use policies and good user education
- Educate on importance of good passwords
- Give guidelines for good passwords
  - Minimum length (>6)
  - Require a mix of upper & lower case letters, numbers, punctuation
  - Not dictionary words
- But likely to be ignored by many users

Managing Passwords - Computer Generated

- let computer create passwords
- If random likely not memorisable, so will be written down (sticky label syndrome)
- Even pronounceable not remembered
- Have history of poor user acceptance
- FIPS PUB 181 one of best generators
  - Has both description & sample code
  - Generates words from concatenating random pronounceable syllables

Managing Passwords - Reactive Checking

- Reactively run password guessing tools
  - Note that good dictionaries exist for almost any language/interest group
- Cracked passwords are disabled
- But is resource intensive
- Bad passwords are vulnerable till found

Managing Passwords -Proactive Checking

- Most promising approach to improving password security
- Allow users to select own password
- But have system verify it is acceptable
  - Simple rule enforcement (see earlier slide)
  - Compare against dictionary of bad passwords
  - Use algorithmic (markov model or bloom filter) to detect poor choices