

# Week 16

---

WIRELESS NETWORK SECURITY  
LINUX/WINDOWS SECURITY

# Chapter 24

## Wireless Network Security

# Introduction

---

Wireless data communications have revolutionized computer networking

- Wireless data networks found virtually everywhere

Wireless networks have been targets for attackers

- Early wireless networking standards had vulnerabilities
- Changes in wireless network security yielded security comparable to wired networks

# Wireless Security

---

Key factors contributing to higher security risk of wireless networks compared to wired networks include:

- Channel
  - Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
  - Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols
- Mobility
  - Wireless devices are far more portable and mobile, thus resulting in a number of risks
- Resources
  - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware
- Accessibility
  - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks



**Bluetooth®**

# Wireless Attacks

---

## Bluetooth

- Uses short-range radio frequency transmissions
- Provides for rapid, ad-hoc device pairings
  - Example: smartphone and Bluetooth headphones

## Bluejacking

- Attack that sends unsolicited messages to Bluetooth-enabled devices
  - Text messages, images, or sounds
- Considered more annoying than harmful
  - No data is stolen

## Bluesnarfing

- Unauthorized access to wireless information through a Bluetooth connection
- Often between cell phones and laptops
- Attacker copies e-mails, contacts, or other data by connecting to the Bluetooth device without owner's knowledge

# Wireless LAN

---



Institute of Electrical and Electronics Engineers (IEEE)

- Most influential organization for computer networking and wireless communications
- Dates back to 1884
- Began developing network architecture standards in the 1980s

1997: release of IEEE 802.11

- Standard for wireless local area networks (WLANs)
- Higher speeds added in 1999: IEEE 802.11b

# Wireless LAN Technical Standards

---

## IEEE 802.11a

- Specifies maximum rated speed of 54Mbps using the 5GHz spectrum

## IEEE 802.11g

- Preserves stable and widely accepted features of 802.11b
- Increases data transfer rates similar to 802.11a

## IEEE 802.11n

- Ratified in 2009

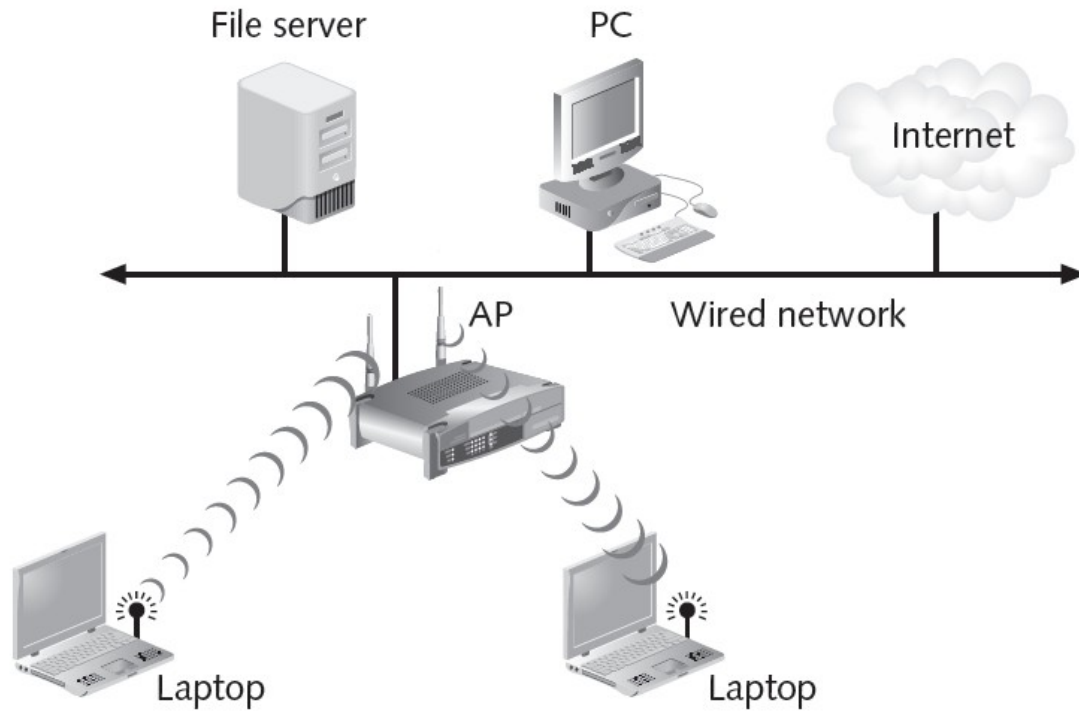
## Improvements in IEEE 802.11n

- Speed
- Coverage area
- Interference
- Security

## Wireless client network interface card adapter

- Performs same functions as wired adapter
- Antenna sends and receives signals

# Wireless LAN Attacks



## Access point (AP) major parts

- Antenna and radio transmitter/receiver send and receive wireless signals
- Bridging software to interface wireless devices to other devices
- Wired network interface allows it to connect by cable to standard wired network

## AP functions

- Acts as “base station” for wireless network



# Wireless LAN Attacks (cont.)

---

## Wireless broadband routers

- Single hardware device containing AP, firewall, router, and DHCP server

## Wireless networks have been vulnerable targets for attackers

- Not restricted to a cable

## Discovering the network

- One of first steps in attack is to discover presence of a network

## Beaconing

- AP sends signal at regular intervals to announce its presence and provide connection information
- Wireless device scans for beacon frames

## War driving

- Process of passive discovery of wireless network locations

# Wireless LAN Attacks (cont.)

---

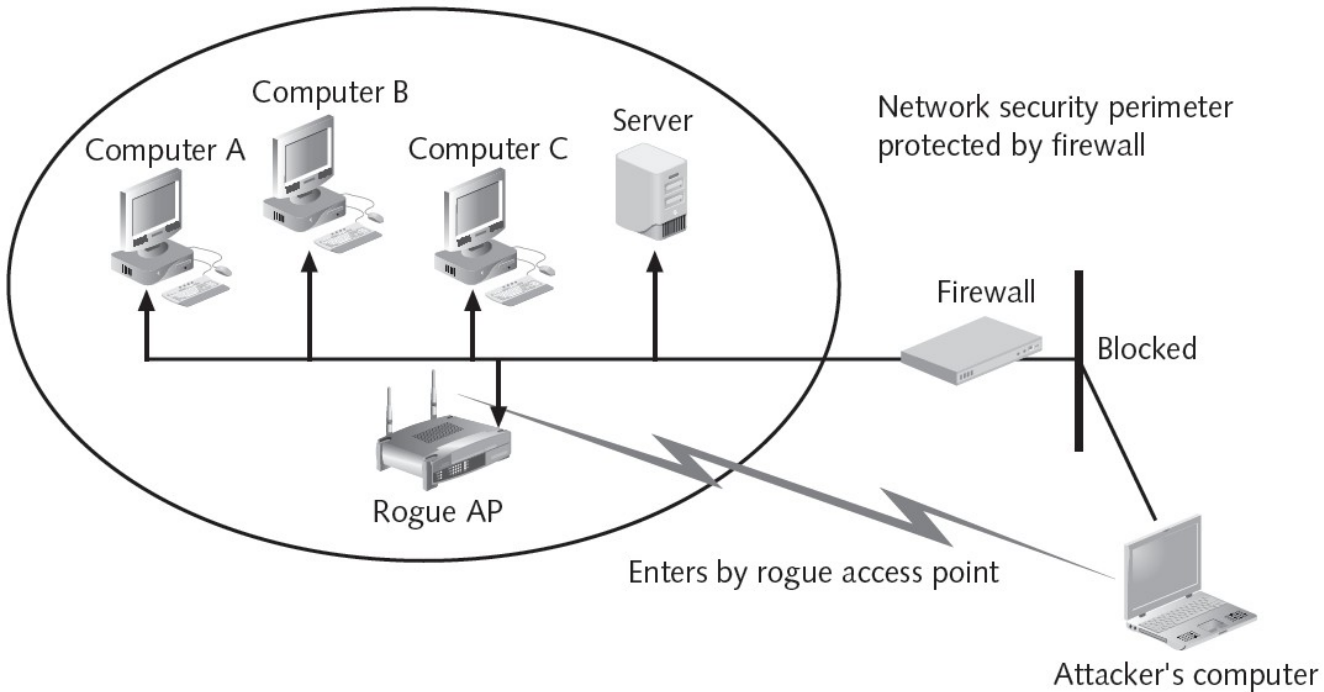
## Attacks through the RF spectrum

- Wireless protocol analyzer
- Generating interference

## Wireless protocol analyzer

- Wireless traffic captured to decode and analyze packet contents
- Network interface card (NIC) adapter must be in correct mode

# Wireless LAN Attacks (cont.)



## Attacks using access points

- Rogue access points
- Evil twins

## Rogue access point

- Unauthorized access point that allows attacker to bypass network security configurations
- May be set up behind a firewall, opening the network to attacks

# Wireless LAN Attacks (cont.)

---

## Evil twin

- AP set up by an attacker
- Attempts to mimic an authorized AP
- Attackers capture transmissions from users to evil twin AP

# Wireless Network Threats

---

**Accidental  
association**

**Malicious  
association**

**Ad hoc  
networks**

**Nontraditi  
onal  
networks**

**Identity  
theft  
(MAC  
spoofing)**

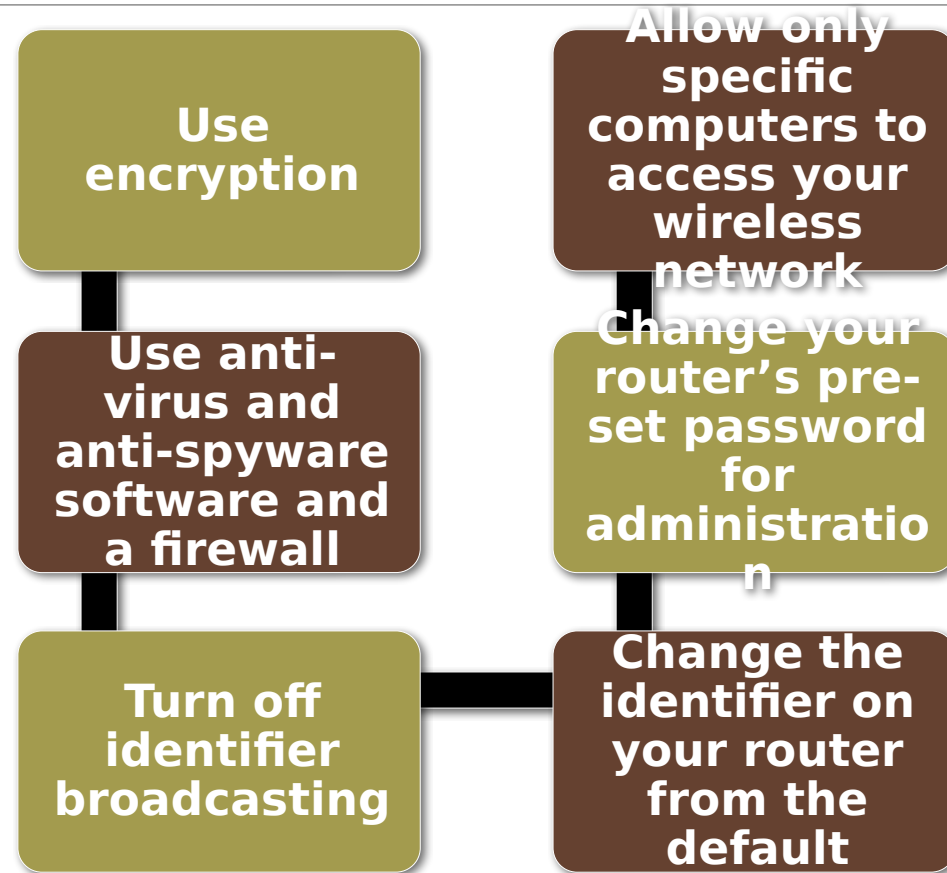
**Man-in-  
the  
middle  
attacks**

**Denial of  
service  
(DoS)**

**Network  
injection**

# Wireless Network Security Techniques

---



# Mobile Device Security – Needs/Concerns

---

An organization's networks must accommodate:

- Growing use of new devices
  - Significant growth in employee's use of mobile devices
- Cloud-based applications
  - Applications no longer run solely on physical servers in corporate data centers
- De-perimeterization
  - There are a multitude of network perimeters around devices, applications, users, and data
- External business requirements
  - The enterprise must also provide guests, third-party contractors, and business partners network access using various devices from a multitude of locations

# Security Threats

---

Lack of physical  
security  
controls

Use of  
untrusted  
networks

Use of  
untrusted  
mobile devices

Use of  
untrusted  
applications

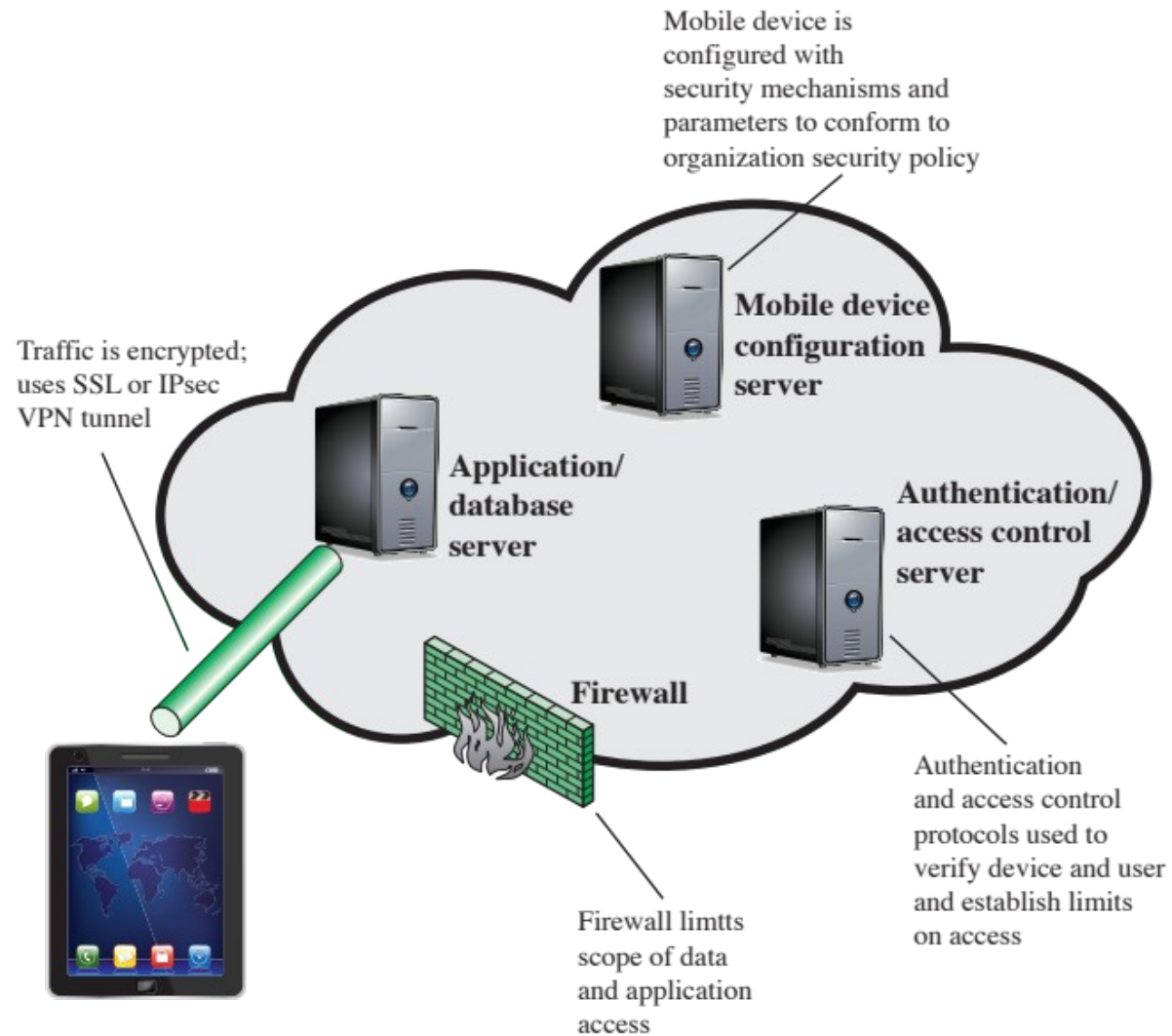
Interaction with  
other systems

Use of  
untrusted  
content

Use of location  
services



# Mobile Device Security Elements



**Figure 24.2 Mobile Device Security Elements**

# Wireless Fidelity (Wi-Fi) Alliance

---

## 802.11b

- First 802.11 standard to gain broad industry acceptance

## Wireless Ethernet Compatibility Alliance (WECA)

- Industry consortium formed in 1999 to address the concern of products from different vendors successfully interoperating
- Later renamed the Wi-Fi Alliance

## Term used for certified 802.11b products is Wi-Fi

- Has been extended to 802.11g products

## Wi-Fi Protected Access (WPA)

- Wi-Fi Alliance certification procedures for IEEE802.11 security standards
- WPA2 incorporates all of the features of the IEEE802.11i WLAN security specification

# Wireless LAN Security Methods

---

## Wired Equivalent Privacy (WEP) algorithm

- 802.11 privacy

## Wi-Fi Protected Access (WPA)

- Set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard
- Robust Security Network (RSN)
- Final form of the 802.11i standard
- Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program

# 802.11 Protocol Stack

---

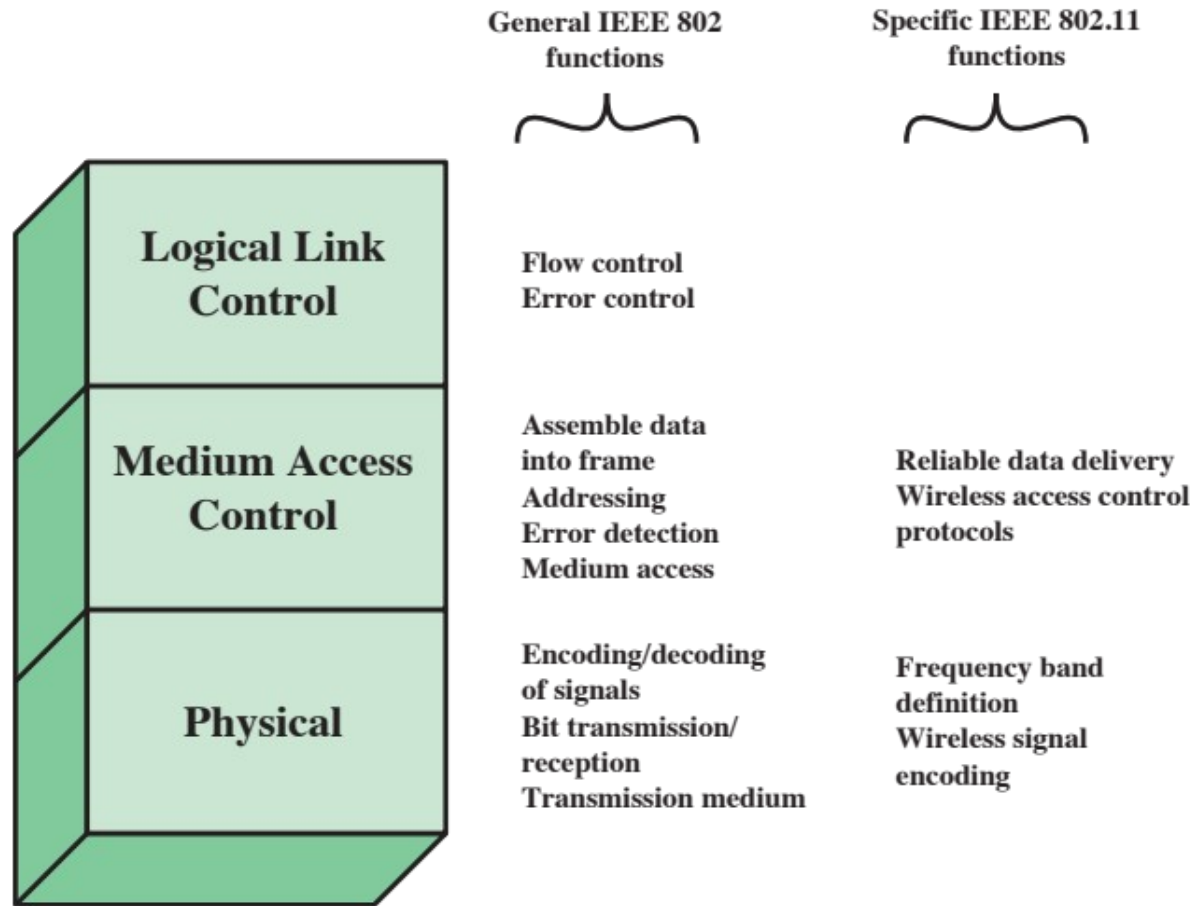
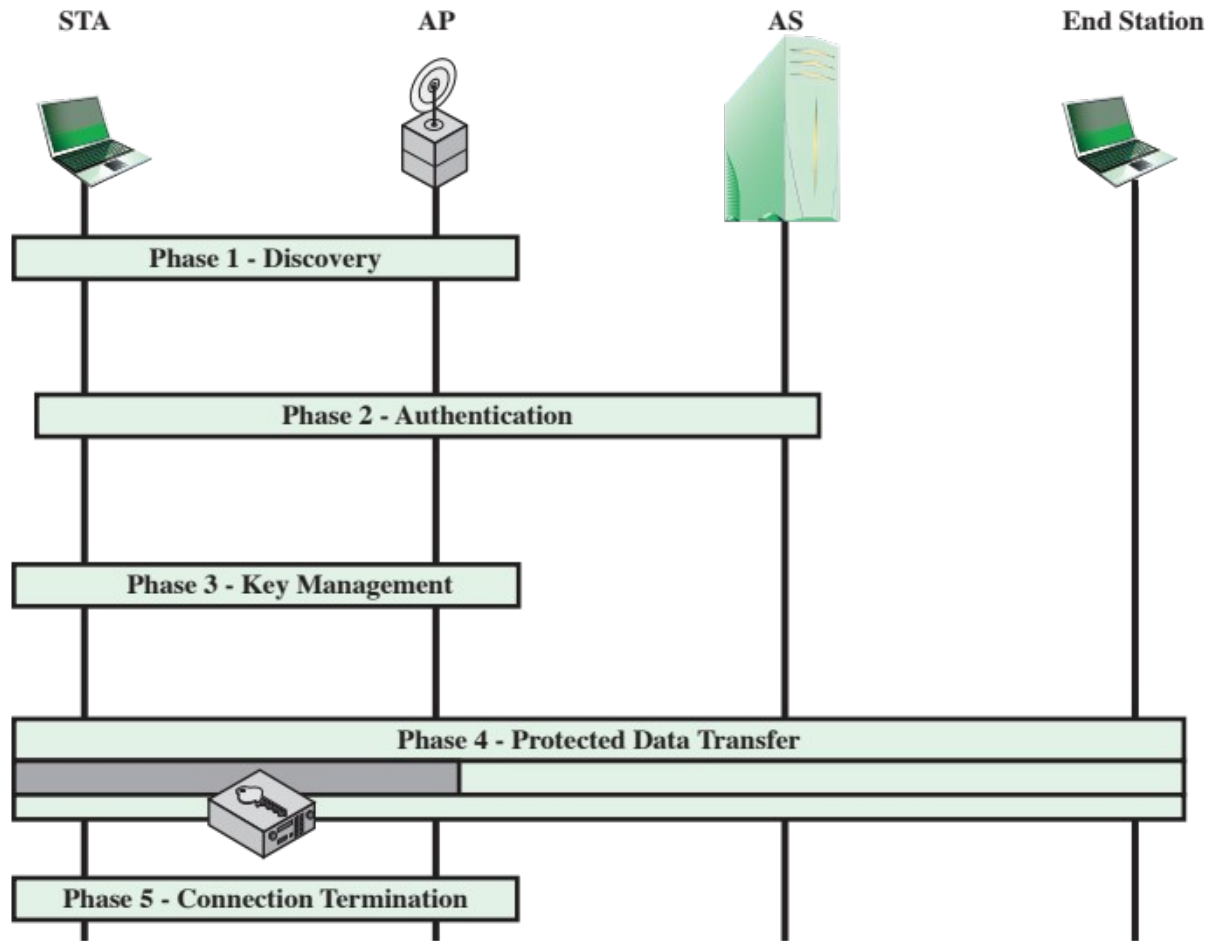


Figure 24.3 IEEE 802.11 Protocol Stack



# Phases of Operation

Figure 24.7 IEEE 802.11i Phases of Operation

# Chapter 25- 26

Linux/Windows Security

# Linux

---

Created in 1991 by Linus Torvalds

Has evolved into one of the world's most popular and versatile operating systems

- Free
- Open-sourced
- Available in a wide variety of distributions targeted at almost every usage scenario imaginable

Examples of distributions include:

- Red Hat Enterprise Linux
  - Conservative and commercially supported
- Ubuntu
  - Completely free
- uClinux
  - Stripped-down but hyper-stable embedded version designed for use in appliances and consumer products

# Linux Security

---


The traditional Linux security model can be summed up quite succinctly: People or processes with “root” privileges can do anything; other accounts can do much less



From the attacker’s perspective the challenge in cracking a Linux system is gaining root privileges



Once an attacker gains root privileges they can:

- Erase or edit logs
  - Hide their processes, files, and directories
  - Basically redefine the reality of the system as experienced by its administrators and users
- 

Thus, Linux security (and UNIX security in general) is a game of “root takes all”



# Linux's DAC (Discretionary Access Control)

---

**Linux's security model**

**In the Linux DAC system there are**

- **Users:** each of which belongs to one or more groups
- **Objects:** files and directories

**Users read, write, and execute the objects based on the object's permissions**

**Each object has three sets of permissions:**

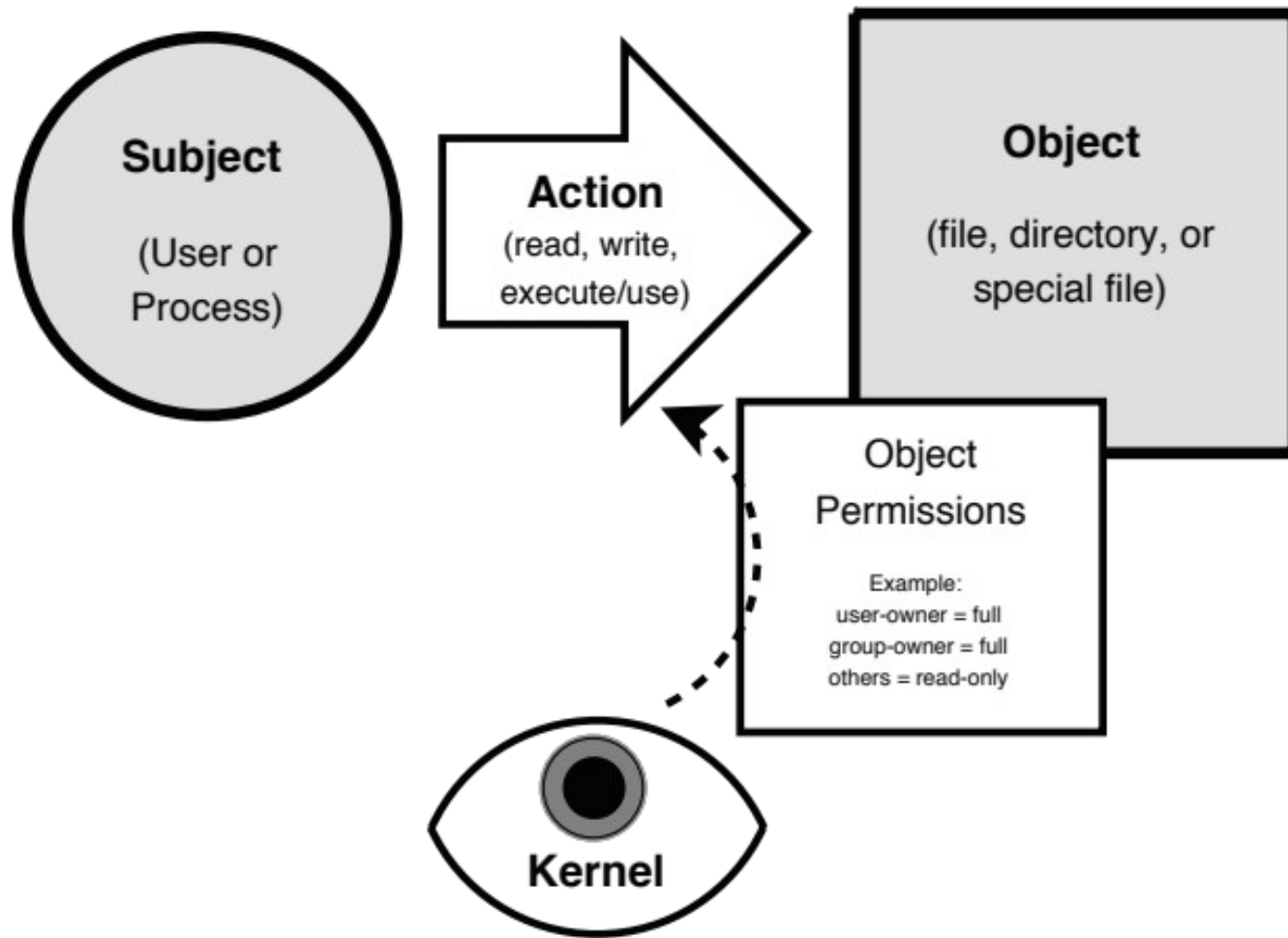
- **User-owner**
- **Group-owner**
- **Other (everyone else)**

**Permissions are enforced by the Linux kernel**

# Permissions

---

- Prior to being executed a program's file-permissions restrict who can execute, access, or change it
- When running, a process normally runs as the identity of the user and group of the person or process that executed it
- If a running process attempts to read, write, or execute some other object the kernel will first evaluate that object's permissions against the process's user and group identity
- Whoever owns an object can set or change its permissions
- The system **superuser** account has the ability to both take ownership and change the permissions of all objects in the system



# Linux Transactions (security)

---

**Figure 25.1 Linux Security Transactions**

# Users, Groups, and Permissions

---

There are two things on a UNIX system that aren't represented by files:

- User accounts
- Group accounts

## User account

- Represents someone or something capable of using files
- Can be associated with both actual human beings and processes

## Group account

- A list of user accounts
- Each user account is defined with a main group membership, but may belong to as many groups as you need it to

# Simple File Permissions

---

Each file on a UNIX system has two owners (a user and a group)

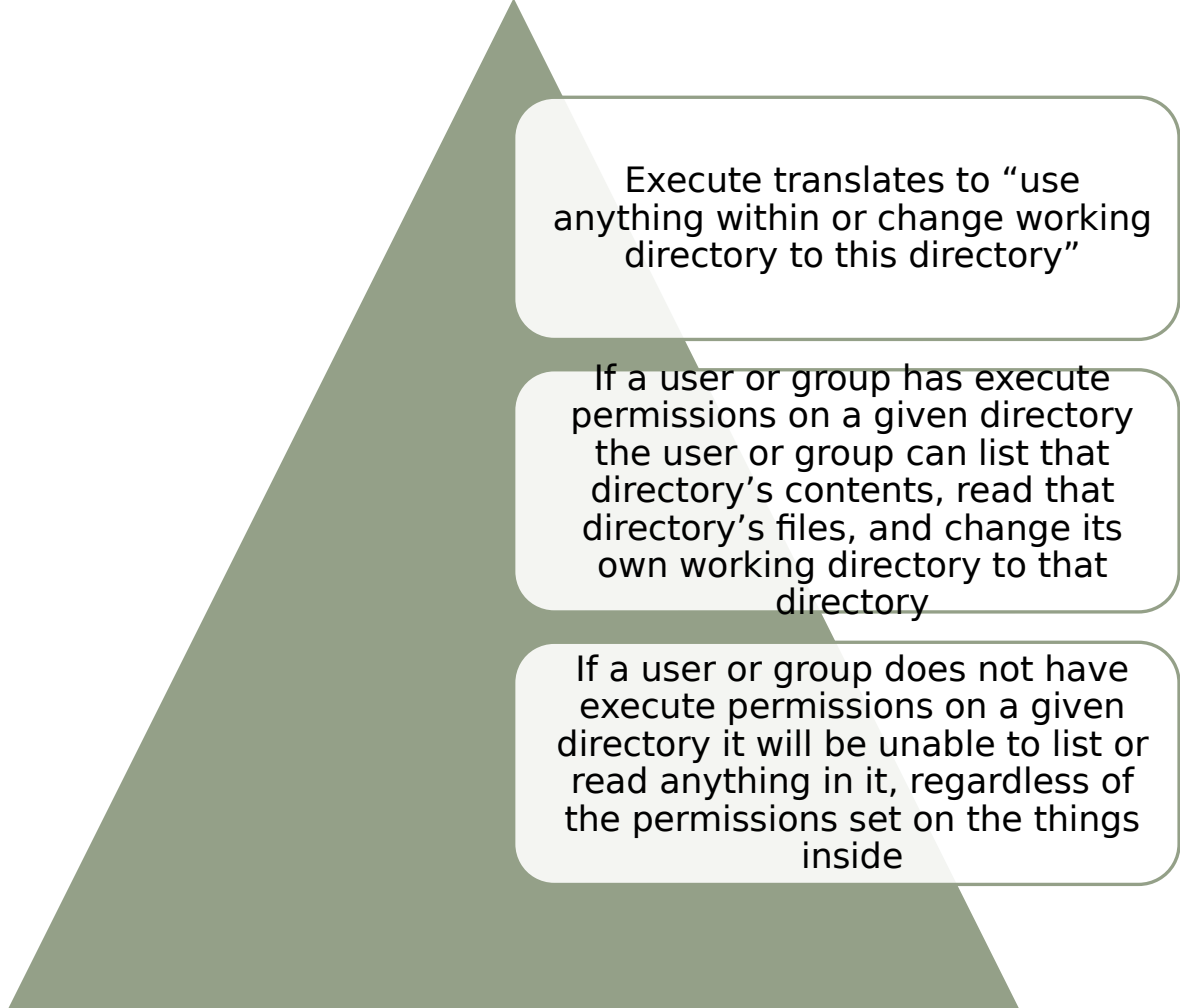
Each user and group has its own set of permissions that specify what the user or group may do with the file (read it, write to it, delete it, execute it)

Other

- User accounts that don't own the file or belong to the group that owns it
- Listing 25-3 shows a long file-listing for the file `/home/maestro/baton_dealers.txt`

```
-rw-rw-r-- 1 maestro conductors 35414 Mar 25 01:38  
          baton_dealers.txt
```

**Listing 25-3: File-Listing Showing Permissions**

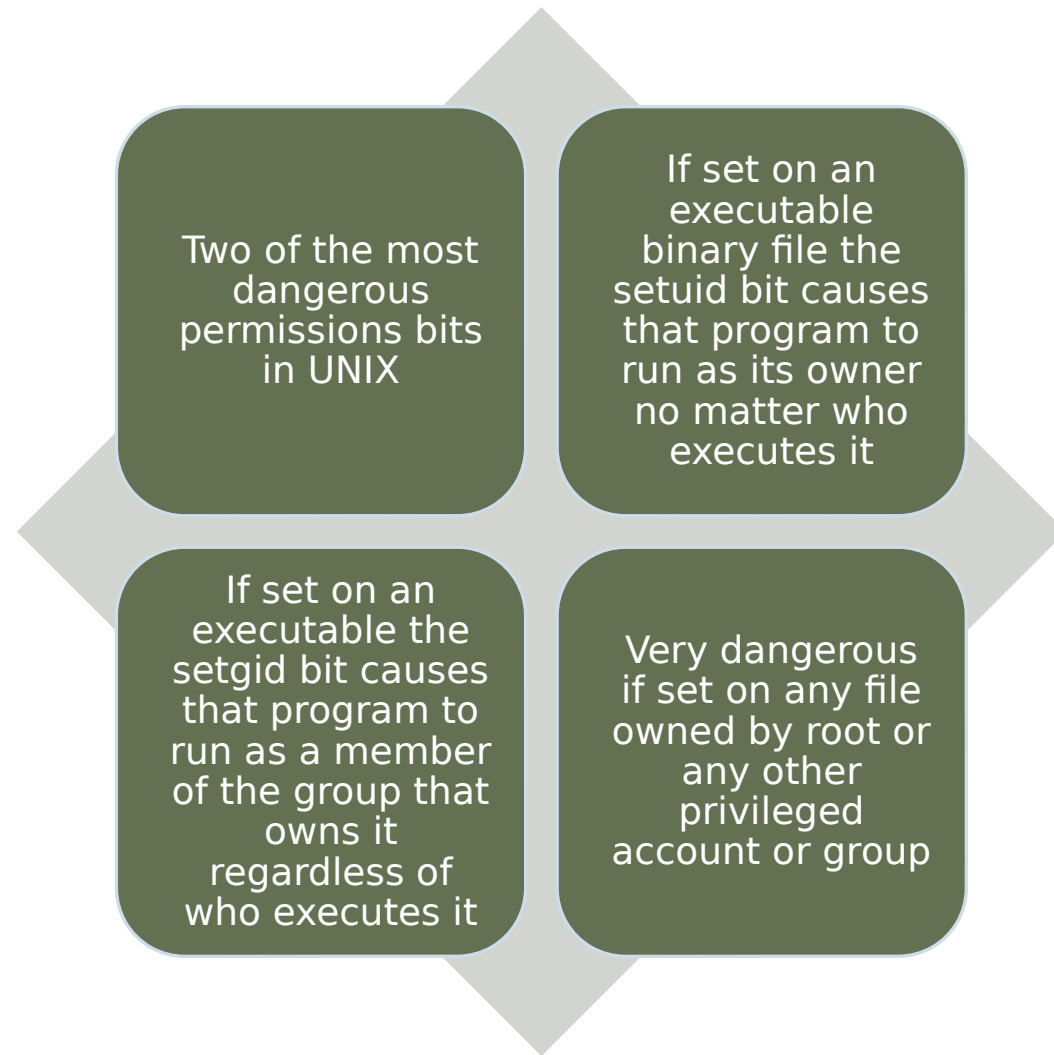


Execute translates to “use anything within or change working directory to this directory”

If a user or group has execute permissions on a given directory the user or group can list that directory’s contents, read that directory’s files, and change its own working directory to that directory

If a user or group does not have execute permissions on a given directory it will be unable to list or read anything in it, regardless of the permissions set on the things inside

# Directory Permissions



# Setuid and Setgid

# Numeric Modes

---

Internally Linux uses numbers to represent permissions

Consists of four digits

- As you read left to right these represent special permissions, user permissions, group permissions, and other permissions

Each permission has a numeric value and the permissions in each digit-place are additive

- The digit represents the sum of all permission-bits you wish to set

Basic numeric values are 4 for read, 2 for write, and 1 for execute

- These values represent bits in a binary stream and are therefore all powers of 2
- If user permissions are set to “7” this represents 4(value for read) plus 2 (the value for write and 1 (the value for execute)



- For example, the numeric mode 3000 translates to

"setgid set, sticky-bit set, no other permissions set"

- <https://chmodcommand.com/chmod-777/>

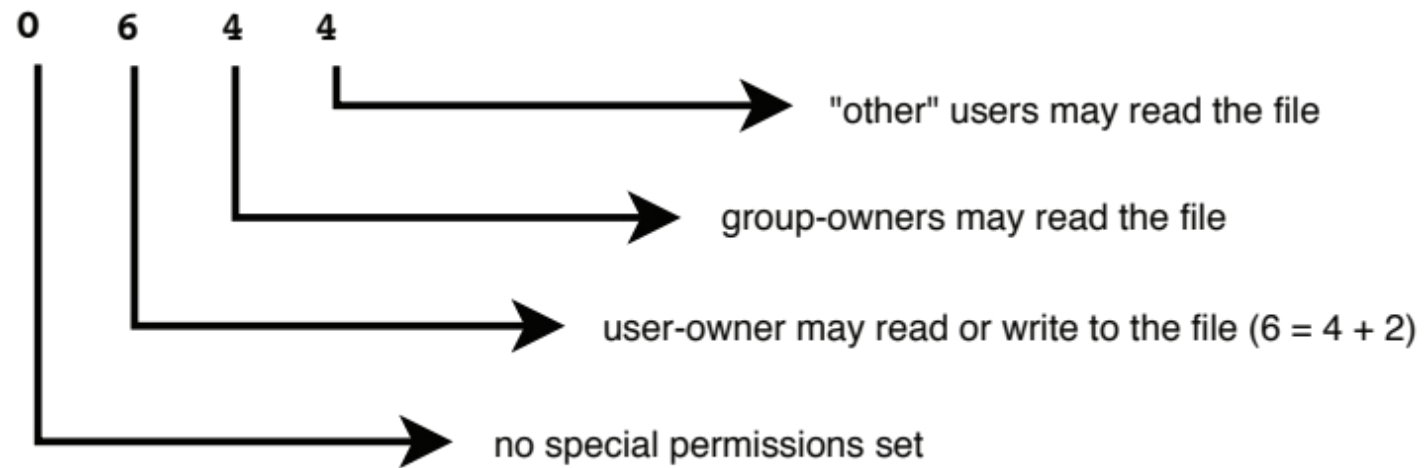
- 4 stands for setuid,
- 2 stands for setgid,
- 1 stands for sticky-bit

# Special Permissions

---

# Example

---



**Figure 25.2 Permissions on mycoolfile**

# Linux Vulnerabilities

---

Some common vulnerabilities in default Linux installations (unpatched and unsecured) have been:

- Buffer overflows
- Race conditions
- Abuse of programs run “setuid root”
- Denial of service (DoS)
- Web application vulnerabilities
- Rootkit attacks

# OS Installation: Software Selection and Initial Setup

---

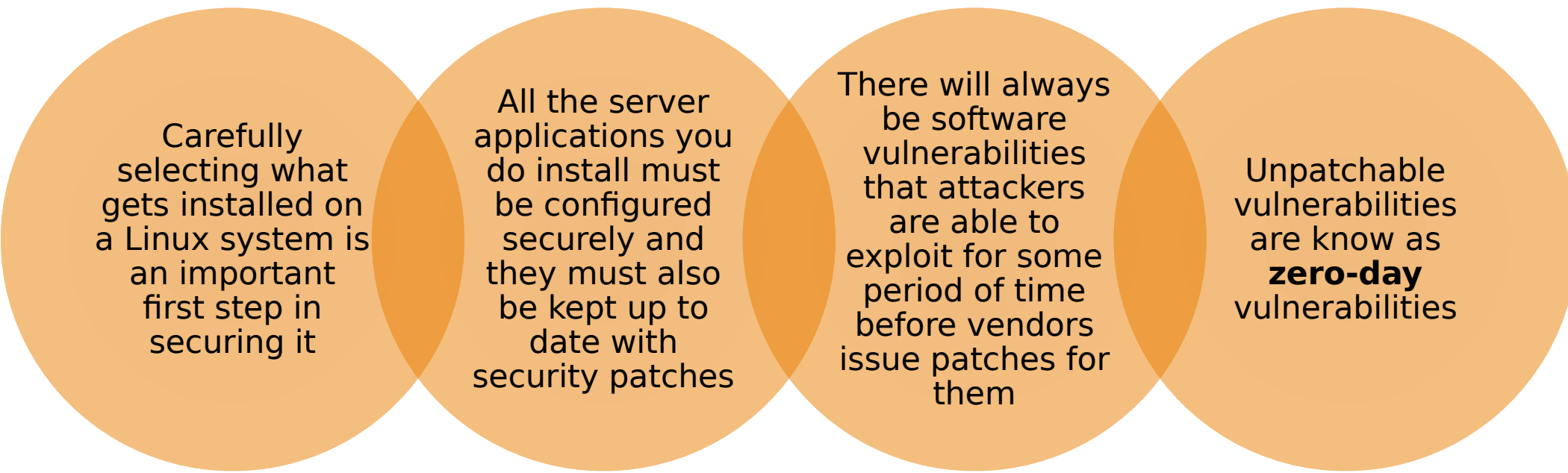
Linux system security begins at operating system installation time

Here is a list of software packages that should seldom, if ever, be installed on hardened servers, especially Internet-facing servers:

- X Windows System
- RPC Services
- R-Services
- inetd
- SMIP Daemons
- Telnet and other cleartext-logon services

# Patching

---



Carefully selecting what gets installed on a Linux system is an important first step in securing it

All the server applications you do install must be configured securely and they must also be kept up to date with security patches

There will always be software vulnerabilities that attackers are able to exploit for some period of time before vendors issue patches for them

Unpatchable vulnerabilities are known as **zero-day** vulnerabilities

# Antivirus Software

---

**Historically Linux hasn't been nearly so vulnerable to viruses as other operating systems**

**Most Linux system administrators have tended to rely on keeping up to date with security patches for protection against malware**

**Worms have historically been a much bigger threat against Linux systems than viruses**

**Viruses typically abuse the privileges of whatever user unwittingly executes them**

**As Linux's popularity continues to grow we can expect Linux viruses to become much more common**

# User Management

---

The guiding principles in Linux user account security are:

- Be very careful when setting file and directory permissions
- Use group memberships to differentiate between different roles on your system
- Be extremely careful in granting and using root privileges

Command review:

- `chmod` command sets and changes permissions for objects belonging to existing user and groups
- `useradd`, `usermod`, and `userdel` are used to create, modify, and delete user accounts
- `groupadd`, `groupmod`, and `groupdel` commands are used to create, modify, and delete group accounts

# Password Aging

---



**Maximum and minimum lifetime for user passwords**

**Set globally in the files `/etc/login.defs` and `/etc/default/useradd`**

**Passwords should have a minimum age to prevent users from rapidly cycling through password changes in attempt to reuse old passwords**

**If maximum age is too long the odds of passwords being exposed before being changed will increase, however if too short users may get frustrated with having to change their passwords frequently, leading to mistreatment of their password**

**Defunct user accounts should be disabled or deleted promptly**



# Root Delegation: su and sudo

---

- The fundamental problem with Linux and UNIX security is that permissions and authority on a given system boil down to “root can do anything, users can’t do much of anything”

## su

- Provided you know the root password, you can use the su command to promote yourself to root from whatever user you logged in as

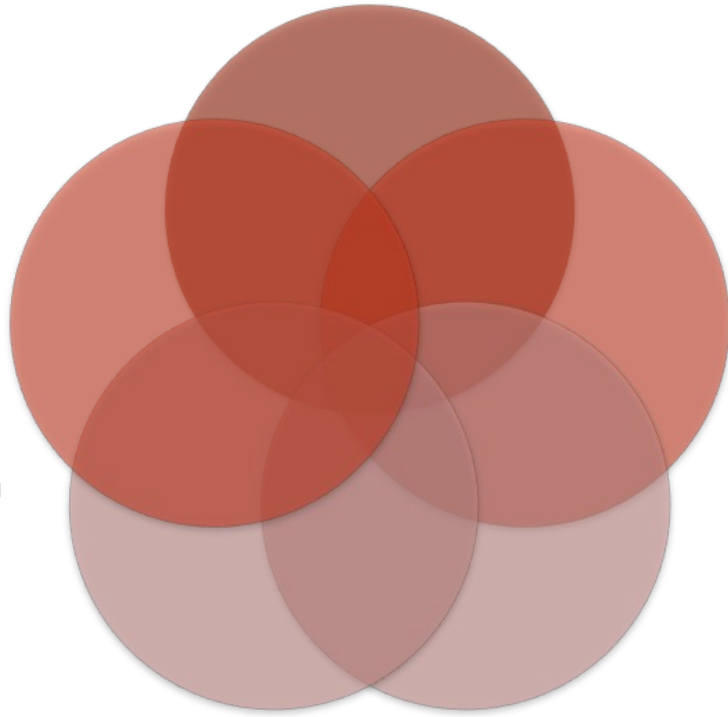
## sudo

- Short for “superuser do”
- Standard package on most Linux distributions
- Allows users to execute specified commands as root without actually needing to know the root password

Can only tell you about  
bad things that have  
already happened

System log daemons  
receive log data from a  
variety of sources, sort  
by facility and severity,  
and then write the log  
messages to log files

On Linux systems system  
logs are handled either  
by the Berkeley Syslog  
daemon in conjunction  
with the kernel log  
daemon or by the  
Syslog-NG



Isn't a  
proactive control

Helps ensure that in the  
event of a system breach  
or failure, system  
administrators can more  
quickly and accurately  
identify what happened

# Loggin g

---

# Windows Security – Fundamental Architecture

---

Anyone who wants to understand Windows security must have knowledge of the basic fundamental security blocks in the operating system

Some of the components in Windows that make up the fundamental security infrastructure are:

- The Security Reference Monitor (SRM)
- The Local Security Authority (LSA)
- The Security Account Manager (SAM)
- Active Directory (AD)
- Authentication Packages
- WinLogon and NetLogon

# Windows Security – Fundamental Architecture

---

## The Security Reference Monitor (SRM)

- This kernel-mode component performs access checks, generates audit log entries, and manipulates user rights (also called privileges)
- Ultimately every permission check is performed by the SRM
- Most modern operating systems include SRM type functionality that performs privileged permission checks
- SRMs tend to be small in size so their correctness can be verified

## The Local Security Authority (LSA)

- Resides in a user-mode process named lsass.exe and is responsible for enforcing local security policy in Windows
- It also issues security tokens to accounts so they log on to the system
- Security policy includes:
  - Password policy (such as complexity rules and expiration times)
  - Auditing policy (which operations on what objects to audit)
  - Privilege settings (which accounts can perform privileged operations)

# Windows Security – Fundamental Architecture

---

## The Security Account Manager (SAM)

- Is a database that stores accounts data and relevant security information about local principals and local groups
- When a user logs on to a computer using a local account the SAM process takes the logon information and performs a lookup against the SAM database
- If the credentials match the user can log on to the system
- The SAM file is binary rather than text, and passwords are stored using the MD4 hash algorithm
- On Windows Vista and later, the SAM stores password information using a password-based key derivation function (PBKCS) which is substantially more robust against password guessing attacks than MD4

## Active Directory (AD)

- Microsoft's LDAP directory included with Windows Server 2000 and later
- All currently supported client versions of Windows, including Windows XP and Windows 7, can communicate with AD to perform security operations including account logon
- A Windows client will authenticate using AD when the user logs on to the computer using a domain account rather than a local account

# Windows Security – Fundamental Architecture

---

## Local versus Domain Accounts

- A networked Windows computer can be in one of two configuration: either domain joined or in a workgroup
- When a computer is domain joined users can gain access to that computer using domain accounts, which are centrally managed in AD
- They can also log on using local accounts but local accounts may not have access to domain resources such as networked printers, Web servers, e-mail servers, etc.
- When a computer is in a workgroup only local accounts can be used, held in the SAM
- A domain has the major advantage of being centrally managed and as such is more secure, users' accounts can be disabled centrally rather than on all individual computers, and security policies are also centrally managed when using AD
- The only advantage of using local accounts is that a computer does not need the infrastructure required to support a domain using AD
- In a workgroup (collection of computers connected to one another using a network) the machines use only local accounts
- The difference between a workgroup and a domain is simply where accounts are authenticated
- A workgroup has no domain controllers, authentication is performed on each computer, and a domain authenticates accounts at domain controllers running AD

# Windows Security Basics

---

Before a user can log on to a Windows network a domain administrator must add the user's account information to the system (includes the user's name, account name, and password)

After the administrator has entered this information Windows creates an account for the user in the domain controller running Active Directory

Each user account is uniquely represented by a Security ID (SID)

SIDs are unique within a domain and every account gets a different SID

# Privileges in Windows

---

Privileges are essentially system-wide permissions assigned to user accounts

Some privileges are deemed “dangerous”, which means a malicious account that is granted such a privilege can cause damage

Examples of dangerous privileges include:

- Act as part of operating system privilege
  - This is the most dangerous privilege in Windows and is granted only the Local System account; even administrators are not granted this privilege
- Debug programs privilege
  - This privilege basically means a user can run any code he or she wants in any running process
- Backup files and directories privilege
  - Any process running with this privilege will bypass all access control list checks



# Access Control List (ACL)

---

## Windows has two forms of ACL:

- Discretionary ACL (DACL)
  - Usually what most people mean when they say ACL
  - Grants or denies access to protected resources in Windows such as files, shared memory, named pipes, etc.
- System ACL (SACL)
  - Used for auditing
  - In Windows Vista used to enforce mandatory integrity policy

## Two important things to keep in mind about access control in Windows:

- There is no implied access
- When a Windows application accesses an object, it must request the type of access the application requires

Objects that require protection are assigned a DACL (and possibly a SACL) which includes the SID of the object owner (usually the object creator) as well as a list of ACEs

## ACEs

- Access control entries
- Each ACE in the DACL determines access; and an ACE can be an allow ACE or a deny ACE
- Includes a SID and an access mask (an access mask could include the ability to read, write, create, delete, modify)

# Access Control

---

- When a user account attempts to access a protected object the operating system performs an access check
- It compares the user account and group information in user's token and the ACEs in the object's ACL
- If all requested operations are granted, then access is granted, otherwise the user gets an access denied error status

# Windows Vulnerabilities

---

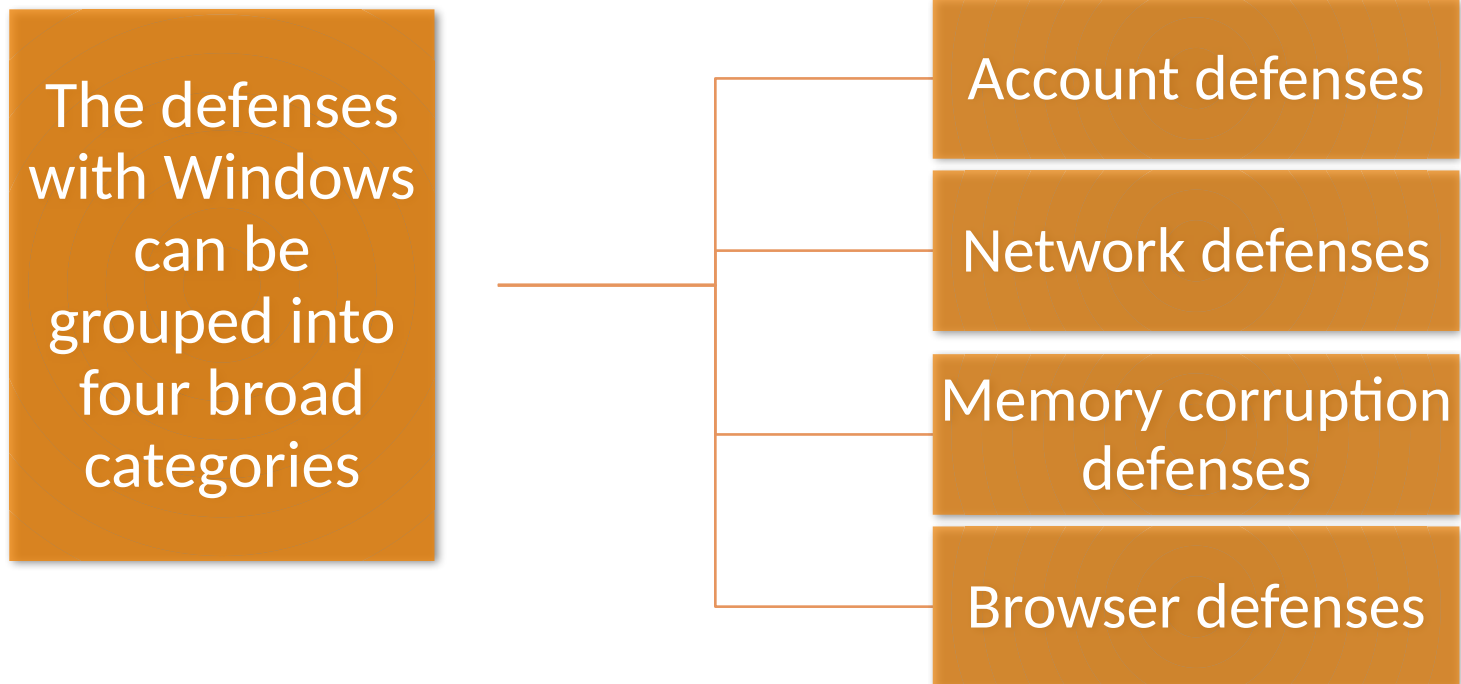
After 2001 Microsoft decided to change its software development process to better accommodate secure design, coding, testing, and maintenance requirements with the goal of reducing the number of vulnerabilities in all Microsoft products

## Security Development Lifecycle core requirements

- Mandatory security education
- Secure design requirements
- Threat modeling
- Attack surface analysis and reduction
- Secure coding requirements and tools
- Secure testing requirements and tools
- Security push
- Final security review
- Security response

# Windows Security Defenses

---



# Account Defenses

---

- Principle of least privilege dictates that users should operate with just enough privilege to get the tasks done, and no more
- Windows XP and Windows Server 2003 add a feature named "Secondary Logon" which allows a user account to right click an application, select "run as....", and then enter another user account and password to run the application
- Restricted token is a thread token with privileges removed and/or SIDs marked as deny-only SIDs
- User Account Control (UAC)
  - When a user wants to perform a privileged operation, the user is prompted to enter an administrator's account name and password
  - If the user is an administrator, the user is prompted to consent to the operation
  - Often referred to as "over the shoulder logon"

# Network Defense - Firewall

---

All versions of Windows since XP have included a built-in software firewall

The version included with XP was limited in that:

- It was not enabled by default
- Its configuration was limited to blocking only inbound connections on specific ports
- Changes in XP SP2
- Option to open a port to the Internet --- but only on the local subnet --- in order for users with multiple computers in the home to share files and print documents
- The firewall is enabled by default
- Changes in Vista and later
- The firewall is a fully integrated component of the rewritten TCP/IP networking stack
- The firewall supports optionally blocking outbound connections

# Further Security Measures

---

## Heap randomization

Designed to take some of the predictability away from the attacker

When a heap is created the start of the heap is offset by 0-4 MB

This feature is new to Windows Vista

## Image randomization

When the operating system boots, it starts up in one of 256 configurations (in other words, the entire operating system is shifted up or down in memory when it is booted)

This makes the operating system less predictable for attackers and makes it less likely that an exploit will succeed

## Service restart policy

In Vista, Microsoft set some of the critical services to restart only twice, after which the service will not restart unless the administrator manually restarts the service

This gives the attacker only two attempts to get the attack to work

# Browser Defenses

---

A malicious Web page could take advantage of many possible attack vectors

- Code and data makes for a rich and productive end-user environment but it is hard to secure
- Web browsers can also render various multimedia objects; many file formats are rendered by helper objects called MIME handlers

## ActiveX opt-in

- New feature added by Internet Explorer
- Essentially unloads ActiveX controls by default, and when a control is used for the first time, the user is prompted to allow the control to run

## Protected mode

- When this default configuration is used Internet Explorer runs at low integrity level, making it more difficult for malware to manipulate the operating system, which operates at a medium or higher integrity level

## ASLR and DEP

- Current versions of Internet Explorer also enable these by default



# Browser Defenses (cont.)

---

It is important to point out that Protected Mode, DEP and ASLR only help mitigate against memory corruption vulnerabilities, they do not help protect against Phishing attacks or common web-specific vulnerabilities such as cross-site scripting (XSS)

Microsoft added defenses to Internet Explorer to help address these issues

- First, a cross-site scripting detection logic to help detect and prevent some classes of XSS
- The second defense is a phishing filter --- when a user visits a web site, the site's URL is sent to a service that determines if the site is a known phishing or malware distribution site and the user is warned if the site is suspicious
- A final defense to help prevent users being tracked is a privacy-enhancing mode named InPrivate mode, which does not persist cookies or site history