NETWORK SECURITY

Complete Study Notes

ITEC 5010 - Network Security Course

Simplified Guide for Easy Understanding

Week 1: Understanding TCP/IP and OSI Layers

What is the OSI Model?

The OSI (Open Systems Interconnection) model is like a map that shows how computers talk to each other. It has 7 layers, and each layer does a specific job. Think of it like a post office system where your letter goes through different departments before reaching its destination.

The 7 Layers of OSI Model:

Layer	Name	What It Does	Example
7	Application	Where you interact with programs	Web browsers, Email
6	Presentation	Translates data into readable format	Encryption, JPEG, MP3
5	Session	Manages connections between computers	Video calls, Login sessions
4	Transport	Makes sure data arrives correctly	TCP, UDP
3	Network	Finds the best path for data	IP addresses, Routers
2	Data Link	Moves data between nearby devices	MAC addresses, Switches
1	Physical	The actual cables and signals	Cables, WiFi signals

What is TCP/IP Model?

TCP/IP is a simpler model with only 4 layers. It's what the internet actually uses today. While OSI is like a detailed blueprint, TCP/IP is the real building that was constructed.

Layer	Name	Similar OSI Layers	What It Does
4	Application	Layers 5, 6, 7	All user applications and services
3	Transport	Layer 4	Reliable data delivery (TCP/UDP)
2	Internet	Layer 3	Routing data across networks (IP)
1	Network Access	Layers 1, 2	Physical connection and local delivery

Key Differences:

- OSI has 7 layers, TCP/IP has 4 layers
- OSI is theoretical, TCP/IP is practical
- OSI was created by ISO, TCP/IP by DARPA
- TCP/IP is what the internet uses today

Week 2: Cloud-Enabling Technologies

What is Cloud Computing?

Cloud computing means using computers and storage that are somewhere else (in data centers) instead of on your own computer. It's like renting instead of buying. You can access these resources through the internet whenever you need them.

Key Cloud Technologies:

1. Virtualization: This is the foundation of cloud computing. It allows one physical computer to act like many separate computers. Think of it like dividing a big house into multiple apartments - same building, but each apartment is independent.

2. Virtual Machines (VMs): These are like fake computers running inside real computers. Each VM thinks it's a complete computer with its own operating system, but it's actually sharing the physical hardware with other VMs.

3. Containers: These are lighter than VMs. They package an application with everything it needs to run, but they share the operating system. Think of containers like lunch boxes - each contains different food, but they're all carried in the same bag.

4. APIs (Application Programming Interfaces): These are like translators that allow different software programs to talk to each other. They make it possible for your phone app to communicate with cloud servers.

Types of Cloud Services:

Type	What You Get	Example	Who Manages What
IaaS (Infrastructure)	Virtual computers, storage, networks	Amazon EC2, Microsoft Azure	You: Apps, Data Provider: Hardware
PaaS (Platform)	Development tools and environment	Google App Engine, Heroku	You: Apps Provider: Everything else
SaaS (Software)	Ready-to-use applications	Gmail, Dropbox, Office 365	Provider: Everything You: Just use it

Benefits of Cloud Computing:

- **Cost Savings:** Pay only for what you use, no need to buy expensive equipment
- **Scalability:** Easily increase or decrease resources as needed
- **Accessibility:** Access your data from anywhere with internet
- **Reliability:** Professional data centers with backup systems
- **Automatic Updates:** Software stays current without your effort

Week 3: WAN and LAN Networks

What is a LAN?

LAN stands for Local Area Network. It's a network that covers a small area like your home, office, or school building. All devices are close together and usually connected with cables or WiFi. Think of it like a neighborhood where everyone knows each other.

LAN Characteristics:

- **Coverage:** Small area (one building or campus)
- **Speed:** Very fast (100 Mbps to 10 Gbps)
- **Ownership:** Usually owned by one organization
- **Cost:** Lower setup and maintenance costs
- **Examples:** Home WiFi, office network, school computer lab

What is a WAN?

WAN stands for Wide Area Network. It connects LANs that are far apart, like connecting offices in different cities or countries. The internet is the world's largest WAN. Think of it like highways connecting different cities.

WAN Characteristics:

- **Coverage:** Large area (cities, countries, worldwide)
- **Speed:** Slower than LAN (varies greatly)
- **Ownership:** Usually involves telecom companies
- **Cost:** Higher costs for long-distance connections
- **Examples:** The Internet, company networks across cities

Network Devices:

Device	What It Does	Where Used
Switch	Connects devices in a LAN Sends data to specific devices	Within office/home
Router	Connects different networks Finds best path for data	Connects LAN to internet
Firewall	Blocks unauthorized access Protects network security	Between internet and LAN
Access Point	Provides WiFi connectivity Extends wireless coverage	Throughout buildings
Modem	Converts digital to analog signals Connects to ISP	Home/office internet connection

Week 4: Wide Area Networks and Service Quality Metrics

Understanding WAN Technologies:

Wide Area Networks use different technologies to connect distant locations. The main types include dedicated lines (like private highways), shared networks (like public roads), and internet-based connections (like using Google Maps to find routes).

WAN Connection Types:

1. Leased Lines: A dedicated, private connection between two locations. It's like having your own private road - expensive but guaranteed speed and security.

2. MPLS (Multi-Protocol Label Switching): A efficient way to direct data across networks using labels instead of addresses. Like having express lanes on a highway.

3. VPN (Virtual Private Network): A secure tunnel over the public internet. It's like sending a locked box through regular mail instead of hiring an armored truck.

4. SD-WAN (Software-Defined WAN): Uses software to manage multiple connection types intelligently. Like having a smart GPS that automatically chooses the best route.

Service Quality Metrics:

These are measurements that tell us how well a network is performing. Just like you might measure a car's performance by speed, fuel efficiency, and reliability, we measure networks using these metrics:

Metric	What It Means	Good vs Bad	Impacts
Bandwidth	How much data can travel at once	Good: 100+ Mbps Bad: <10 Mbps	Download speeds, video quality
Latency	Delay in data transmission	Good: <50ms Bad: >150ms	Gaming, video calls, responsiveness
Jitter	Variation in latency	Good: <30ms Bad: >100ms	Call quality, streaming smoothness
Packet Loss	Percentage of lost data	Good: <1% Bad: >5%	Connection drops, retransmissions
Uptime	Time network is available	Good: >99.9% Bad: <95%	Service reliability, business continuity

SLA (Service Level Agreement):

An SLA is a contract between a service provider and customer that defines expected service quality. It's like a warranty for your network service. It usually includes:

- Guaranteed uptime percentage (e.g., 99.9%)
- Maximum response time for support
- Performance guarantees
- Penalties if standards aren't met
- Procedures for reporting problems

Week 5: Information Systems Security Policy

What is a Security Policy?

A security policy is a set of rules that tells everyone in an organization how to protect information and systems. Think of it like the rules of your home - no shoes inside, lock the doors at night, don't talk to strangers. But for computers and data.

Why Do We Need Security Policies?

• **Protect sensitive information** from being stolen or leaked
• **Prevent security breaches** and cyber attacks
• **Ensure everyone knows** what they should and shouldn't do
• **Meet legal requirements** and industry regulations
• **Reduce risks** and potential losses

Key Components of a Security Policy:

1. Access Control: Who can access what information
- User accounts and passwords must be strong
- Different people have different permission levels
- Remove access when employees leave

2. Password Policy: Rules for creating and using passwords
- Minimum 8-12 characters
- Mix of letters, numbers, and symbols
- Change passwords regularly
- Don't share passwords with others

3. Acceptable Use Policy: What you can and can't do
- Work computers are for work purposes
- Don't visit suspicious websites
- Don't download unauthorized software
- Don't share company information publicly

4. Data Classification: Labeling information by sensitivity
- Public: Anyone can see (company brochures)
- Internal: Only employees (company policies)
- Confidential: Only specific people (salaries)
- Secret: Highly restricted (trade secrets)

5. Incident Response: What to do when something goes wrong
- Report suspicious activity immediately
- Don't try to fix security problems yourself
- Contact IT security team
- Document what happened

Common Security Threats:

Threat	What It Is	How to Protect
Phishing	Fake emails trying to steal information	Check sender, don't click suspicious links
Malware	Harmful software (viruses, trojans)	Use antivirus, don't download from unknown sources
Ransomware	Locks your files and demands money	Regular backups, security updates
Social Engineering	Tricking people into giving information	Be skeptical, verify identities
Insider Threats	Employees misusing access	Monitor activities, limit access

Best Practices for Everyone:

1. **Lock your computer** when you step away
2. **Don't write down passwords** on sticky notes
3. **Be careful with USB drives** - they can contain viruses
4. **Update software** when prompted
5. **Use different passwords** for different accounts
6. **Think before you click** on links or attachments
7. **Report anything suspicious** immediately
8. **Protect physical documents** - shred sensitive papers

Week 6: Strategic Mobility and Security

What is Mobile Security?

Mobile security is about protecting smartphones, tablets, and laptops from threats. Since we use these devices everywhere - at work, at home, in coffee shops - they need special protection. It's like having a guard for your phone that travels with you.

Why Mobile Security is Important:

• Phones contain personal and work information
• We use them for banking, shopping, and email
• They connect to many different WiFi networks
• Easy to lose or have stolen
• We use them for two-factor authentication

Mobile Security Threats:

1. Lost or Stolen Devices: If someone finds your phone, they might access your data. Solution: Use screen locks, remote wipe features, and encryption.

2. Malicious Apps: Apps that look normal but steal your data or damage your device. Solution: Only download from official app stores, check reviews and permissions.

3. Unsecured WiFi: Public WiFi networks at cafes or airports can be monitored by hackers. Solution: Use VPN when on public WiFi, avoid sensitive transactions.

4. Phishing: Fake text messages or calls trying to steal information. Solution: Don't click links in unexpected messages, verify sender identity.

5. Outdated Software: Old versions have known security holes. Solution: Always install updates when available.

Mobile Device Management (MDM):

MDM is software that helps companies manage and secure employee devices. It's like a remote control center for all company phones and tablets. MDM can:
• Enforce security policies automatically
• Install and update apps remotely
• Track device location if lost
• Remotely wipe data if device is stolen
• Separate work and personal data
• Generate security reports

BYOD (Bring Your Own Device):

BYOD means using your personal phone or laptop for work. It has benefits and risks:

Benefits	Risks	Solutions
Employees prefer their own devices	Company data on personal devices	Use MDM software
Cost savings for company	Mixing work and personal data	Create separate work profiles
Higher employee satisfaction	Security not controlled by IT	Require security software
Better productivity	Lost/stolen personal devices	Remote wipe capability

Week 7: Security Incident Response

What is a Security Incident?

A security incident is any event that threatens the security of information systems. It could be a virus infection, data breach, hacking attempt, or even a lost laptop. Think of it like a fire alarm - when it goes off, you need to act quickly and correctly.

Types of Security Incidents:

- **Data Breach:** Unauthorized access to sensitive information
- **Malware Infection:** Virus or ransomware on systems
- **Denial of Service:** Making systems unavailable to users
- **Unauthorized Access:** Someone using systems without permission
- **Physical Security:** Theft of equipment or unauthorized entry
- **Social Engineering:** Tricking employees into breaking security

Incident Response Process:

When a security incident happens, follow these steps:

Step 1: Preparation (Before Incident)
- Create incident response plan
- Form incident response team
- Set up monitoring tools
- Train employees on procedures
- Have contact lists ready

Step 2: Detection and Analysis
- Identify that an incident occurred
- Determine the type and severity
- Collect initial evidence
- Document everything you see
- Alert the security team

Step 3: Containment
- Stop the incident from spreading
- Isolate affected systems
- Create backups of evidence
- Implement temporary fixes
- Continue monitoring

Step 4: Eradication
- Remove the cause of incident
- Delete malware or close security holes
- Reset compromised passwords

• Patch vulnerable systems
• Verify threat is eliminated

Step 5: Recovery
• Restore systems to normal operation
• Test that everything works
• Monitor for signs of problems
• Gradually return to full service
• Verify security controls are working

Step 6: Lessons Learned
• Hold a review meeting
• Document what happened and why
• Identify what went well and what didn't
• Update security policies
• Improve defenses to prevent recurrence

Incident Severity Levels:

Level	Description	Example	Response Time
Critical	Severe impact, major systems down	Ransomware attack, major data breach	Immediate (<1 hour)
High	Significant impact, some systems affected	Virus outbreak, unauthorized access	Urgent (<4 hours)
Medium	Moderate impact, limited scope	Suspicious activity, minor policy violation	Same day (<24 hours)
Low	Minimal impact, no immediate threat	Failed login attempts, spam emails	Next business day

What NOT to Do During an Incident:

- Don't panic or act without thinking
- Don't try to fix it yourself if you're not trained
- Don't turn off systems without approval
- Don't delete logs or evidence
- Don't discuss the incident publicly
- Don't assume the problem is solved without verification

Week 8: Cloud System Management, Patch Management, and Backup

Cloud System Management:

Managing cloud systems means making sure your cloud resources work properly, stay secure, and don't waste money. It's like being the manager of an apartment building - you need to maintain the property, collect rent, and keep tenants happy.

Key Cloud Management Tasks:

1. Resource Monitoring: Watching how cloud resources are used
• Check CPU, memory, and storage usage
• Monitor network traffic
• Track application performance
• Set up alerts for problems

2. Cost Management: Controlling cloud spending
• Turn off unused resources
• Choose right-sized instances
• Use reserved instances for steady workloads
• Monitor and analyze spending

3. Security Management: Protecting cloud resources
• Configure firewalls and access controls
• Encrypt sensitive data
• Monitor for suspicious activity
• Regular security audits

4. Compliance Management: Meeting regulatory requirements
• Understand applicable regulations
• Implement required controls
• Maintain audit logs
• Generate compliance reports

Patch Management:

Patches are updates that fix bugs and security problems in software. Patch management is the process of keeping all software up-to-date. Think of it like getting your car serviced regularly to prevent breakdowns.

Why Patching is Critical:

• **Security:** Many cyber attacks exploit known vulnerabilities that patches fix
• **Stability:** Patches fix bugs that cause crashes or errors
• **Performance:** Updates often improve speed and efficiency

• **Compliance:** Regulations may require current software versions
• **Compatibility:** Keep software working with other systems

Patch Management Process:

Step	What to Do	Why It Matters
1. Inventory	List all systems and software	Know what needs updating
2. Assessment	Evaluate new patches	Understand what patch fixes
3. Testing	Test patches in safe environment	Prevent patch from breaking things
4. Approval	Get management approval	Ensure business readiness
5. Deployment	Install patches on systems	Apply the actual fix
6. Verification	Confirm patches work correctly	Ensure success
7. Documentation	Record what was done	Track history and compliance

Backup and Recovery:

Backups are copies of your data saved in a different location. They protect against data loss from accidents, hardware failures, or cyber attacks. It's like having a spare key to your house - you hope you never need it, but you're glad it's there.

The 3-2-1 Backup Rule:

This is the gold standard for backups:
• **3** copies of your data (original + 2 backups)
• **2** different types of media (hard drive, cloud, tape)
• **1** copy stored off-site (different physical location)

Types of Backups:

Type	What It Backs Up	Speed	Storage Used
Full Backup	Everything, every time	Slow	High
Incremental	Only what changed since last backup	Fast	Low
Differential	Everything since last full backup	Medium	Medium
Mirror	Exact copy at this moment	Medium	High

Disaster Recovery Plan:

A disaster recovery plan explains how to restore systems after a major problem. It should include:
• **Recovery Time Objective (RTO):** How quickly you need to be back up
• **Recovery Point Objective (RPO):** How much data you can afford to lose
• **Backup locations:** Where backups are stored
• **Recovery procedures:** Step-by-step instructions
• **Contact information:** Who to call in an emergency
• **Testing schedule:** Regular drills to ensure plan works

Week 9: Security Strategies - Data and Cloud Monitoring

What is Security Monitoring?

Security monitoring is like having security cameras for your network. It watches everything that happens on your systems, looking for suspicious activity. Instead of watching for burglars, it watches for hackers, malware, and other threats.

Why We Need Monitoring:

- **Early Detection:** Find problems before they cause damage
- **Compliance:** Meet regulatory requirements for logging
- **Investigation:** Understand what happened during incidents
- **Prevention:** Identify and block threats in real-time
- **Performance:** Track system health and efficiency

What to Monitor:

1. Network Traffic:
- Who is connecting to your network
- What data is being transmitted
- Unusual patterns or volumes
- Blocked connection attempts

2. User Activity:
- Login and logout times
- Failed login attempts
- Files accessed and modified
- Privilege escalation attempts

3. System Performance:
- CPU and memory usage
- Disk space and I/O
- Application response times
- Error rates and crashes

4. Security Events:
- Antivirus alerts
- Firewall blocks
- IDS/IPS alerts
- Configuration changes

Monitoring Tools:

Tool Type	What It Does	Example Use

SIEM (Security Information and Event Management)	Collects and analyzes security logs from all systems	Detect coordinated attack across multiple systems
IDS/IPS (Intrusion Detection/ Prevention System)	Monitors network for malicious activity and can block it	Stop known attack patterns in real-time
Log Management	Centrally stores and searches logs	Investigate what happened during incident
Cloud Monitoring	Tracks cloud resource usage and security	Monitor AWS, Azure, or GCP services

Data Protection Strategies:

1. Encryption: Scrambling data so only authorized people can read it
• Encrypt data at rest (stored on drives)
• Encrypt data in transit (moving across network)
• Use strong encryption algorithms (AES-256)

2. Data Loss Prevention (DLP): Preventing sensitive data from leaving
• Monitor email for sensitive information
• Block unauthorized file transfers
• Alert when confidential data is shared

3. Access Controls: Limiting who can access data
• Principle of least privilege
• Regular access reviews
• Multi-factor authentication

4. Data Classification: Labeling data by sensitivity
• Automatically tag sensitive data
• Apply appropriate protections
• Track data movement

Cloud Security Best Practices:

1. Shared Responsibility Model:
Understand that cloud security is shared between you and the cloud provider:
• Provider secures: Physical infrastructure, virtualization layer, network
• You secure: Your data, applications, user access, configurations

2. Identity and Access Management:
• Use strong passwords and MFA
• Create separate accounts for different purposes
• Regularly review and remove unused accounts
• Implement role-based access control

3. Network Security:
• Configure virtual firewalls (security groups)
• Use VPNs for remote access
• Segment networks into separate zones
• Monitor network traffic

4. Data Protection:
• Enable encryption by default
• Use cloud provider's backup services
• Implement versioning for important data
• Regular data backups to different regions

5. Compliance and Governance:
• Enable logging and monitoring
• Implement compliance frameworks
• Regular security assessments
• Document configurations and changes

Common Cloud Security Mistakes:

• Leaving storage buckets publicly accessible
• Using default or weak passwords
• Not enabling MFA on admin accounts
• Failing to encrypt sensitive data
• Not monitoring for unusual activity
• Ignoring security updates and patches
• Granting excessive permissions
• Not having backups or disaster recovery plan

Week 10: Addressing Regulatory Cloud Imperatives

What is Regulatory Compliance?

Regulatory compliance means following laws and rules that apply to your industry. Different industries have different rules about how to protect data. It's like following building codes when constructing a house - you must meet certain standards to be legal.

Why Compliance Matters:

- **Legal Requirement:** Breaking rules can result in fines or lawsuits
- **Customer Trust:** Shows you take security seriously
- **Business Opportunity:** Some customers require compliance
- **Risk Reduction:** Compliance standards reduce security risks
- **Reputation:** Avoid negative publicity from violations

Major Compliance Frameworks:

Framework	Who It Applies To	Key Requirements
GDPR (General Data Protection Regulation)	Companies handling EU citizens' data	• Data privacy by design • Right to be forgotten • Data breach notification • Consent management
HIPAA (Health Insurance Portability Act)	Healthcare organizations in the US	• Protect patient health info • Encryption requirements • Access controls • Audit trails
PCI DSS (Payment Card Industry Standard)	Organizations processing credit card payments	• Secure network • Encrypt card data • Vulnerability management • Access control
SOC 2 (Service Organization Control)	Service providers handling customer data	• Security controls • Availability measures • Confidentiality • Privacy protection
ISO 27001	Any organization wanting certification	• Risk assessment • Security policies • Access control • Incident management

Cloud Compliance Challenges:

1. Data Location: Where is data stored physically?
- Some laws require data stays in specific countries
- Cloud providers have data centers worldwide

• You need to know and control data location

2. Data Access: Who can access the data?
• Cloud provider employees might have access
• Need clear agreements on access controls
• Implement encryption to protect from unauthorized access

3. Vendor Management: Third-party risks
• Cloud provider must also be compliant
• Review vendor security practices
• Get appropriate certifications and audit reports

4. Change Management: Cloud services change frequently
• New features might affect compliance
• Stay informed about cloud provider changes
• Re-assess compliance when services change

Steps to Achieve Compliance:

Step 1: Understand Requirements
• Identify which regulations apply to you
• Read and understand the requirements
• Consult with legal and compliance experts
• Document your understanding

Step 2: Assess Current State
• Review existing security controls
• Identify gaps in compliance
• Document current practices
• Prioritize issues to address

Step 3: Implement Controls
• Deploy required security measures
• Update policies and procedures
• Train employees on requirements
• Configure systems appropriately

Step 4: Document Everything
• Keep records of all security measures
• Document policies and procedures
• Maintain audit trails
• Track compliance activities

Step 5: Monitor and Test
• Regular security assessments
• Penetration testing
• Vulnerability scanning
• Review and test disaster recovery

Step 6: Continuous Improvement
• Regular compliance reviews
• Update controls as threats evolve
• Stay current with regulation changes
• Learn from incidents and audits

Cloud Provider Certifications to Look For:

When choosing a cloud provider, verify they have relevant certifications:
• **SOC 2 Type II:** Security, availability, and confidentiality
• **ISO 27001:** Information security management
• **PCI DSS:** If processing payments
• **HIPAA compliance:** For healthcare data
• **FedRAMP:** For US government work
• **Industry-specific certifications:** Relevant to your field

Data Sovereignty:

Data sovereignty means data is subject to the laws of the country where it's stored. This is important because:

- Different countries have different privacy laws
- Some data must stay within specific borders
- Cloud data can be stored anywhere globally
- You need to control and know data location
- Use cloud provider's region selection features

Summary: Key Takeaways

Network Fundamentals:

• OSI model has 7 layers, TCP/IP has 4 layers
• Each layer has specific responsibilities
• Understanding layers helps troubleshoot problems
• TCP/IP is what the internet actually uses

Cloud Technologies:

• Cloud computing provides on-demand resources
• Three main service types: IaaS, PaaS, SaaS
• Virtualization and containers enable cloud computing
• Cloud offers flexibility and cost savings

Network Infrastructure:

• LANs connect local devices, WANs connect distant networks
• Network devices include switches, routers, and firewalls
• Quality metrics measure network performance
• SLAs define expected service levels

Security Policies:

• Security policies define acceptable behavior
• Include access control, password, and acceptable use policies
• Everyone must understand and follow policies
• Regular training keeps people aware

Mobile Security:

• Mobile devices need special security considerations
• MDM helps manage company devices
• BYOD requires careful planning and policies
• Encrypt devices and use strong authentication

Incident Response:

• Incidents happen - preparation is key
• Follow structured response process
• Document everything during incidents
• Learn from incidents to prevent recurrence

System Management:

• Keep all systems patched and updated
• Regular backups prevent data loss
• Follow the 3-2-1 backup rule
• Test disaster recovery plans regularly

Monitoring and Protection:

• Monitor all systems for suspicious activity
• Use encryption to protect sensitive data
• Implement defense in depth strategy
• Cloud security is a shared responsibility

Regulatory Compliance:

• Understand which regulations apply to you
• Implement required security controls
• Document all compliance activities
• Regular assessments ensure ongoing compliance
• Choose compliant cloud providers

Final Thoughts:

Network security is not just about technology - it's about people, processes, and technology working together. The key principles are:

• **Defense in Depth:** Use multiple layers of security
• **Least Privilege:** Give minimum access needed
• **Continuous Monitoring:** Always watch for threats
• **Regular Updates:** Keep systems current
• **User Education:** Train people on security
• **Incident Preparation:** Plan for problems
• **Compliance:** Follow applicable regulations

Remember: Security is an ongoing process, not a one-time event. Stay vigilant, keep learning, and always prioritize protecting your data and systems.