Cybersecurity Basics & Attack Surface Analysis

Executive Summary

This document provides a comprehensive overview of cybersecurity fundamentals, attack surface analysis, threat actors, and practical security considerations for modern digital systems. It covers the CIA triad, various types of attackers, common attack surfaces, OWASP Top 10 vulnerabilities, and real-world application security mapping.

Table of Contents

Confidentiality

Ensuring information is accessible only to authorized individuals.

Real-World Examples:

- Banking: Encryption of account details, PIN protection, secure HTTPS connections
- Social Media: Private messages, restricted profiles, two-factor authentication
- Healthcare: HIPAA-protected patient records, encrypted medical data

Integrity

Maintaining accuracy and trustworthiness of data throughout its lifecycle.

Real-World Examples:

- Banking: Transaction validation, checksums for fund transfers, audit trails
- E-commerce: Order data consistency, inventory management, price verification
- Academic Records: Tamper-proof transcripts, digital signatures on certificates

Availability

Ensuring systems and data are accessible when needed.

Real-World Examples:

- Banking: 24/7 ATM access, online banking uptime, disaster recovery plans
- Social Media: Platform reliability during high-traffic events, CDN distribution
- Emergency Services: Always-available dispatch systems, redundant communications

2. Types of Attackers

Script Kiddies

- Motivation: Curiosity, entertainment, ego
- Capability: Low technical skill, uses pre-built tools
- Example: Running Metasploit modules without understanding them
- Typical Targets: Unsecured websites, IoT devices with default credentials

Insider Threats

- Motivation: Financial gain, revenge, espionage, negligence
- Capability: High-level access, knowledge of internal systems
- Example: Disgruntled employee stealing customer data
- Typical Targets: Proprietary data, financial records, source code

Hacktivists

- Motivation: Political/social ideology, public attention
- Capability: Moderate to high technical skills
- Example: DDoS attacks on government websites for protest
- Typical Targets: Government sites, corporate pages, political organizations

Nation-State Actors

- Motivation: Espionage, political advantage, military advantage
- Capability: Advanced persistent threats (APTs), significant resources
- Example: Stuxnet worm targeting Iranian nuclear facilities
- Typical Targets: Critical infrastructure, government agencies, defense contractors

Organized Cybercriminals

- Motivation: Financial profit
- Capability: Sophisticated operations, business-like structure
- Example: Ransomware-as-a-service operations
- Typical Targets: Healthcare organizations, financial institutions, corporations

3. Common Attack Surfaces

Web Applications

- Vulnerabilities: SQL injection, XSS, CSRF, insecure authentication
- Examples: E-commerce sites, web portals, online banking interfaces
- Attack Vectors: Input fields, cookies, session tokens, file uploads

Mobile Applications

- Vulnerabilities: Insecure data storage, weak encryption, code tampering
- Examples: Banking apps, social media apps, productivity tools
- Attack Vectors: Local storage, inter-app communication, insecure APIs

APIs (Application Programming Interfaces)

- Vulnerabilities: Broken object level authorization, excessive data exposure
- Examples: REST APIs, GraphQL endpoints, microservices
- Attack Vectors: API endpoints, authentication tokens, rate limiting bypass

Network Infrastructure

- Vulnerabilities: Unpatched systems, misconfigurations, weak protocols
- Examples: Routers, switches, firewalls, VPNs
- Attack Vectors: Open ports, default credentials, protocol weaknesses

Cloud Infrastructure

- Vulnerabilities: Misconfigured storage buckets, insecure IAM policies
- Examples: AWS S3 buckets, Azure containers, Google Cloud storage
- Attack Vectors: Publicly accessible resources, weak access controls

Human Element (Social Engineering)

- Vulnerabilities: Lack of awareness, trust, urgency manipulation
- Examples: Phishing emails, pretexting, baiting
- Attack Vectors: Email, phone calls, physical media

4. OWASP Top 10 (2025) Critical Vulnerabilities

Top 10:2025 List

1. A01:2025 - Broken Access Control
2. A02:2025 - Security Misconfiguration
3. A03:2025 - Software Supply Chain Failures
4. A04:2025 - Cryptographic Failures
5. A05:2025 - Injection
6. A06:2025 - Insecure Design
7. A07:2025 - Authentication Failures
8. A08:2025 - Software or Data Integrity Failures
9. A09:2025 - Security Logging and Alerting Failures
10. A10:2025 - Mishandling of Exceptional Conditions

5. Daily Applications Attack Surface Mapping

Email (Gmail/Outlook)

Attack Surfaces:

- Phishing links in emails
- Malicious attachments
- Weak password recovery
- Session hijacking

Protections:

- Spam filters
- Two-factor authentication
- Link scanning
- Encryption in transit

WhatsApp/Messaging Apps

Attack Surfaces:

- Media file exploits
- Backup interception
- Social engineering through messages
- Web client vulnerabilities

Protections:

- End-to-end encryption

- Security code verification
- Block/report features
- Ephemeral messages

Banking Applications

Attack Surfaces:

- Man-in-the-middle attacks
- Screen recording malware
- SIM swapping
- Fake banking apps

Protections:

- Biometric authentication
- Transaction signing
- Device binding
- Real-time fraud monitoring

Social Media (Instagram/Facebook)

Attack Surfaces:

- Malicious links in DMs
- Third-party app permissions
- Location data exposure
- Fake profiles/scams

Protections:

- Privacy settings
- Login approvals
- Suspicious activity alerts
- Content reporting

6. Data Flow & Attack Points

Data Flow Diagram:

User → Browser/App → Network → Server → Database

Stage 1: User Input

- Data: Credentials, form data, queries
- Attack Points: Keyloggers, phishing pages, social engineering
- Security Controls: User education, antivirus software, secure input validation

Stage 2: Application Layer

- Data: Processed input, session tokens
- Attack Points: Input validation bypass, session hijacking, client-side attacks (XSS)
- Security Controls: Input sanitization, secure session management, Content Security Policy

Stage 3: Network Transmission

- Data: Encrypted/plaintext packets
- Attack Points: Eavesdropping, man-in-the-middle, DNS spoofing
- Security Controls: TLS/SSL encryption, VPNs, certificate pinning

Stage 4: Server Processing

- Data: Business logic processing
- Attack Points: SQL injection, command injection, server misconfigurations
- Security Controls: Web Application Firewalls, parameterized queries, least privilege principle

Stage 5: Database Storage

- Data: Structured persistent data
- Attack Points: Direct database access, SQL injection, backup theft
- Security Controls: Encryption at rest, database activity monitoring, regular audits

7. Summary

Cybersecurity is fundamentally about protecting information systems through the CIA triad principles: ensuring confidentiality (only authorized access), integrity (data remains unaltered), and availability (accessible when needed).

Attackers range from low-skilled script kiddies to highly sophisticated nation-state actors, each with different motivations and capabilities. Understanding these threat actors helps in designing appropriate security controls.

The attack surface has expanded significantly with digital transformation, now including web and mobile applications, APIs, cloud infrastructure, networks, and even the human element through social engineering.

The OWASP Top 10 provides a crucial framework for understanding the most critical web application vulnerabilities, with broken access control, cryptographic failures, and injection attacks being consistently dangerous.

Daily applications we use—email, messaging, banking, and social media—each have unique attack surfaces that require specific security measures. Understanding the data flow from user to database reveals multiple potential attack points at each stage, emphasizing the need for defense-in-depth strategies.

Effective cybersecurity requires a layered approach combining technical controls, secure development practices, continuous monitoring, and user education to protect against evolving threats in our increasingly digital world.

Recommendations for Implementation:

1. Implement defense-in-depth with multiple security layers
2. Regularly update and patch all systems and applications
3. Conduct security awareness training for all users
4. Perform regular vulnerability assessments and penetration testing
5. Follow the principle of least privilege for access control
6. Encrypt sensitive data both at rest and in transit
7. Maintain comprehensive logging and monitoring systems
8. Develop and test incident response plans regularly
9. Implement secure coding practices throughout development lifecycle
10. Conduct regular security audits and compliance checks

References

- OWASP Foundation. (2021). OWASP Top 10 Web Application Security Risks
- NIST Cybersecurity Framework
- ISO/IEC 27001 Information Security Management
- Google Cybersecurity Blog
- IBM Security Intelligence Reports
- Verizon Data Breach Investigations Report (2023)

Document Information:

- Author: Narendran P.P
- Date: Generated on 2026-01-15