Common Threat Vectors and Attack Surfaces

Brendan Shea, PhD

March 7, 2025

Understanding Threat Vectors and Attack Surfaces: An Overview

- **Threat vectors** are pathways or means by which an attacker can gain access to a computer or network server to deliver a malicious payload.
- **Attack surfaces** represent the sum of all possible points where an unauthorized user can enter or extract data from an environment.
- Modern organizations face an expanding attack surface due to cloud adoption, remote work, and IoT proliferation.
- Understanding the full spectrum of threat vectors enables security professionals to implement appropriate countermeasures.
- Effective security requires continuous monitoring and mitigation of both technical and human attack vectors.

The Expanding Digital Attack Surface: Modern Challenges

Key Challenge

The average enterprise attack surface now extends far beyond traditional network boundaries, with 60% of assets existing outside the corporate perimeter.

- Digital transformation initiatives have dramatically expanded attack surfaces through cloud services, mobile devices, and remote work arrangements.
- Shadow IT and unauthorized applications create security blind spots that organizations struggle to identify and secure.
- Third-party integrations and API connections introduce additional entry points that must be monitored and protected.
- The average organization uses over 75 different security tools, creating integration challenges and potential security gaps.
- Attack surface management requires continuous discovery, inventory, classification, and assessment of all digital assets.

Email as an Attack Vector: Fundamentals and Exploitation Techniques

- Email remains the most prevalent initial attack vector, used in approximately 90% of all successful cyberattacks.
- **Malicious attachments** deliver payloads through macro-enabled documents, executable files, and archive formats that bypass security controls.
- **Malicious links** direct users to credential harvesting sites, malware download pages, or sites exploiting browser vulnerabilities.
- Business Email Compromise (BEC) attacks use sophisticated social engineering to manipulate recipients into unauthorized fund transfers.
- Email attacks increasingly use legitimate cloud services to host malware, bypassing traditional security controls that trust these domains.

Case Study: Bowser's Phishing Kingdom

The Villain

Bowser from Super Mario Bros. specializes in deception and kidnapping - just like phishing attacks.

- Bowser sends emails claiming to be from "Mushroom Kingdom Cloud Services" requesting password resets for cloud storage.
- The emails use urgent language claiming Mario's photos will be deleted unless he "verifies" his account immediately.
- The phishing link leads to a convincing but fake login page at "mushroomk1ngdom-cloud.com" instead of the legitimate domain.
- When Mario enters his credentials, Bowser captures them and gains access to Mario's personal data and accounts.
- This attack succeeds because it creates urgency, mimics a legitimate service, and exploits Mario's fear of losing valuable data.

Short Message Service (SMS) Threats: Attack Techniques and Vulnerabilities

- **SMS-based attacks** (smishing) leverage the trusted nature of text messaging to deliver malicious links and social engineering content.
- SMS attacks exploit limited URL visibility on mobile devices, making it difficult for users to verify destination links before clicking.
- Attackers impersonate trusted entities like banks, delivery services, and government agencies to create a false sense of urgency.
- SMS-delivered malware often requests excessive permissions that, when granted, can access contacts, cameras, and sensitive data.
- SMS authentication bypass attacks exploit vulnerabilities in two-factor authentication implementations using text messages.

Instant Messaging (IM) Platforms: Emerging Threat Landscape

Emerging Trend

Enterprise adoption of messaging platforms like Slack, Teams, and Discord has created new attack vectors that bypass traditional email security controls.

- Instant messaging platforms enable direct file sharing and link distribution outside of email security gateways and monitoring.
- **Malicious chatbots** can be deployed to impersonate legitimate services and harvest credentials or distribute malware.
- Cross-platform messaging threats like the "FluBot" malware campaign spread rapidly through contact lists on compromised devices.
- Corporate messaging platforms introduce supply chain risks when integrated with third-party applications and services.
- WhatsApp, Telegram, and Signal have become preferred platforms for delivering advanced social engineering attacks due to their encryption features.

Image-Based Attacks: Steganography and Malicious Payloads

- **Steganography** conceals malicious code within image files by manipulating pixel data in ways that are invisible to the human eye.
- Image format vulnerabilities in parsers and rendering engines can be exploited through specially crafted files to execute code.
- QR codes can direct victims to malicious websites or trigger automatic actions when scanned by vulnerable applications.
- Meme-based command and control techniques use social media images to transmit instructions to malware already installed on compromised systems.
- Images shared on social media platforms often bypass security controls due to the implicit trust placed in popular sharing sites.

File-Based Threat Vectors: From Macros to Zero-Days

Evolution

File-based attacks have evolved from simple executable malware to sophisticated fileless techniques that leverage legitimate system processes.

- **Document-based attacks** exploit macros, embedded objects, and vulnerable document parsers in productivity applications.
- Archive formats (.zip, .rar, .7z) enable attackers to bypass security controls through nested archives, password protection, and uncommon compression methods.
- PDF files can contain malicious JavaScript, exploit vulnerabilities in PDF readers, or use social engineering to direct users to malicious sites.
- **Living-off-the-land (LOL) techniques** use legitimate system files and tools to execute malicious code, complicating detection efforts.
- Zero-day vulnerabilities in file parsers remain valuable attack vectors as they bypass signature-based detection mechanisms.

Case Study: Ganondorf's Trojan Horse

- Ganondorf from The Legend of Zelda creates "HyruleSaveGame.exe" that claims to be a game save editor for Hyrule Warriors.
- The application appears legitimate with Hyrule-themed graphics and actually provides the promised save editing functionality.
- Behind the scenes, the program installs a backdoor that gives Ganondorf remote access to Link's computer.
- This malware establishes persistence by creating registry entries that run the backdoor every time the system starts.
- Ganondorf uses this access to steal the digital blueprints for the Master Sword from Link's computer.

Voice Call Vulnerabilities: Vishing and VoIP Exploits

- **Voice phishing (vishing)** uses phone calls to manipulate victims into revealing sensitive information or taking harmful actions.
- Attackers leverage caller ID spoofing to impersonate trusted entities such as technical support, financial institutions, or government agencies.
- Voice synthesis and deepfake technology enable impersonation of executives and trusted figures with increasingly convincing accuracy.
- VoIP infrastructure vulnerabilities can be exploited for call interception, eavesdropping, and denial of service attacks.
- Social engineering via voice calls often bypasses technical security controls by exploiting human psychology and decision-making under pressure.

Removable Devices as Threat Vectors: From USB Drives to External Media

Security Risk

USB devices remain one of the most effective ways to bridge air-gapped networks and introduce malware into isolated environments.

- **USB drop attacks** exploit human curiosity by strategically placing malicious drives in locations where targets will find and connect them.
- Malicious firmware in USB devices can emulate keyboards to execute commands or network cards to exfiltrate data, bypassing software restrictions.
- External hard drives and removable media can spread malware across networks or serve as persistent data exfiltration channels.
- BadUSB attacks reprogram USB device controllers to perform functions different from their advertised purpose.
- Smart devices charging through USB ports can establish unauthorized data connections and access sensitive information.

Case Study: Stuxnet and the Power of Physical Vectors

- **Stuxnet**, discovered in 2010, used infected USB drives to bridge air-gapped networks in Iranian nuclear facilities.
- The malware exploited four zero-day vulnerabilities and leveraged stolen digital certificates to appear legitimate.
- Stuxnet specifically targeted Siemens industrial control systems, altering centrifuge operations while reporting normal system behavior.
- The attack demonstrated how physical media could be used to deliver sophisticated payloads to isolated critical infrastructure.
- This case highlighted the importance of controlling physical access and removable media, even in highly secure environments.

Vulnerable Software: Understanding the Attack Surface

Statistics

According to industry research, 60% of breaches in 2023 involved unpatched vulnerabilities, with an average patch deployment time of 102 days.

- Software vulnerabilities provide attackers with entry points through unintended functionality or implementation flaws.
- Common vulnerability types include buffer overflows, injection flaws, authentication bypasses, and privilege escalation issues.
- **Vulnerability windows** exist between public disclosure, patch availability, and organizational patch deployment.
- Legacy and custom applications often contain undiscovered vulnerabilities due to limited security testing and outdated development practices.
- The expanding software supply chain introduces vulnerabilities through dependencies, third-party libraries, and open-source components.

Client-Based vs. Agentless Software Vulnerabilities: Key Differences

- **Client-based vulnerabilities** exist in software installed locally on end-user devices, providing attackers with direct system access.
- Web browsers and their extensions represent significant client-side attack surfaces due to their extensive privileges and complexity.
- **Agentless vulnerabilities** affect services that don't require installed software, such as web applications, APIs, and cloud services.
- Agentless attacks often exploit implementation flaws in authentication, session management, and access controls rather than memory corruption.
- Defense strategies differ significantly: client-based protection requires endpoint security while agentless protection focuses on network monitoring and API security.

Unsupported Systems and Applications: The Persistent Threat

Risk Factor

Organizations running unsupported software face a 3.5x greater risk of successful cyberattacks compared to those using current, supported systems.

- **End-of-life (EOL) software** no longer receives security updates, creating persistent vulnerabilities that cannot be patched.
- Legacy systems often remain in production due to compatibility requirements, budget constraints, or specialized functionality.
- Critical infrastructure frequently relies on unsupported industrial control systems that were designed without security considerations.
- Unsupported operating systems continue to operate in environments where hardware limitations prevent upgrades.
- The transition to cloud services has created "zombie applications" that remain deployed but unmanaged, creating security blind spots.

Case Study: EternalBlue and the Importance of Patching

- **EternalBlue** exploited a vulnerability in Microsoft's Server Message Block (SMB) protocol, affecting Windows systems worldwide.
- Microsoft released a security patch (MS17-010) one month before the exploit was leaked by the Shadow Brokers group in April 2017.
- Despite available patches, the WannaCry ransomware used EternalBlue to infect over 200,000 systems across 150 countries in May 2017.
- Organizations like the UK's National Health Service suffered significant disruption due to unpatched systems, including canceled appointments and diverted ambulances.
- This case demonstrates how failure to apply available patches for known vulnerabilities leads to preventable large-scale compromises.

Unsecured Wireless Networks: Attack Techniques and Vulnerabilities

Attack Surface

Wireless networks extend the organizational attack surface beyond physical boundaries, enabling attacks from parking lots, adjacent buildings, or public spaces.

- **Evil twin attacks** create rogue access points mimicking legitimate networks to intercept traffic and harvest credentials.
- WPA2 vulnerabilities like KRACK (Key Reinstallation Attack) allow attackers to decrypt wireless traffic without knowing the network password.
- Wireless jamming and deauthentication attacks can disrupt legitimate connections, forcing users to reconnect to malicious networks.
- Captive portal bypasses allow attackers to circumvent authentication mechanisms on public and guest WiFi networks.
- Default and weak router configurations often expose management interfaces and enable unauthorized network access.

Wired Network Vulnerabilities: From Eavesdropping to Man-in-the-Middle

- **ARP poisoning** manipulates the Address Resolution Protocol to redirect traffic, enabling man-in-the-middle attacks on local networks.
- VLAN hopping exploits improper switch configurations to access traffic from other virtual LANs that should be segmented.
- MAC flooding overwhelms switch MAC address tables, potentially causing them to broadcast all traffic to all ports like a hub.
- Physical network taps and compromised networking equipment can capture traffic without software-detectable signatures.
- Legacy protocols without encryption (Telnet, FTP, HTTP) continue to expose sensitive data to network eavesdropping attacks.

Bluetooth and Near-Field Communication (NFC) Threats

Proximity Factor

While Bluetooth and NFC attacks typically require physical proximity, the range for specialized Bluetooth attacks has extended to over 1 mile with directional antennas.

- **Bluetooth vulnerabilities** like BlueBorne affected over 5.3 billion devices, allowing arbitrary code execution without user interaction.
- Bluetooth sniffing can capture unencrypted communications between devices, revealing sensitive data and authentication credentials.
- NFC relay attacks extend the effective range of contactless payment cards and access badges, enabling unauthorized transactions.
- Bluetooth device spoofing exploits weak authentication to impersonate trusted devices like keyboards, headsets, or car systems.
- Mobile point-of-sale (mPOS) terminals using Bluetooth connectivity introduce payment card data interception risks in retail environments.

Open Service Ports: Understanding and Mitigating Exposure

- **Open ports** represent network services listening for connections, each potentially providing an entry point for attackers.
- Unnecessary open ports increase the attack surface and may expose vulnerable services to the internet.
- Common high-risk ports include 22 (SSH), 23 (Telnet), 3389 (RDP), 445 (SMB), and database ports like 1433 (MS SQL) and 3306 (MySQL).
- Automated scanning tools continuously probe internet-facing systems for open ports and known vulnerabilities in exposed services.
- Port redirection and tunneling techniques can circumvent firewall restrictions by encapsulating traffic through allowed ports.

Default Credentials: The Persistent Gateway to Compromise

Prevalence

A 2022 study found that 34% of network devices, applications, and IoT devices still used default credentials months after deployment.

- **Default credentials** are pre-configured username/password combinations set by manufacturers for initial access to devices and systems.
- Administrative interfaces for network devices, security cameras, and IoT systems are frequently targeted using published default credentials.
- Automated botnets systematically scan for and compromise devices with default or weak credentials.
- Cloud instances created from template images often retain default configurations and passwords, creating security gaps in infrastructure.
- Password reuse across systems compounds the risk, allowing credential exposure in one system to compromise others.

Supply Chain Vulnerabilities: Understanding Third-Party Risk

- **Supply chain attacks** target the less-secure elements in a product or service delivery pipeline to compromise the end target.
- Software dependencies and third-party libraries introduce vulnerabilities outside the organization's direct control.
- Compromised development environments can inject malicious code during the build process, as seen in the SolarWinds breach.
- Hardware components may contain implants or backdoors inserted during manufacturing or distribution.
- Organizations inherit the security posture of their weakest suppliers, making third-party risk assessment critical to overall security.

Managed Service Providers (MSPs) as Attack Vectors

Privileged Access

MSPs typically have extensive administrative access to client systems, making them high-value targets for attackers seeking multiple victims through a single compromise.

- **Managed Service Providers (MSPs)** maintain privileged access to numerous client environments, creating an attractive attack vector.
- Remote monitoring and management (RMM) tools used by MSPs can be exploited to deploy malware across all managed clients simultaneously.
- The Kaseya attack of July 2021 infected over 1,500 organizations through compromised MSP software used for system management.
- MSP credential theft provides attackers with legitimate access that can be difficult to distinguish from normal administrative activities.
- Specialized "MSP ransomware" campaigns specifically target service providers to maximize impact and ransom potential.

Vendor and Supplier Security: Weakest Link in the Chain

- Vendors with network access or data integration points create potential entry paths into otherwise secure environments.
- **Third-party software** introduces risks through update mechanisms that can be hijacked to distribute malware.
- Supplier email accounts are increasingly targeted for business email compromise schemes, exploiting established trust relationships.
- Physical suppliers with access to facilities can inadvertently introduce malware or enable physical security breaches.
- Vendor API integrations expand the attack surface by connecting internal systems with external services and datastores.

Case Study: SolarWinds and the Impact of Supply Chain Compromise

Scope

The SolarWinds attack affected approximately 18,000 organizations, including US government agencies, Fortune 500 companies, and security firms.

- In 2020, threat actors compromised SolarWinds' development environment and inserted malicious code into the Orion network monitoring product.
- The modified code created a backdoor that established communication with attacker-controlled servers while evading detection.
- The malicious updates were digitally signed and distributed through legitimate update channels, bypassing security controls.
- Victims included the US Treasury, Justice Department, State Department, Energy Department, and numerous technology companies.

The Human Attack Surface: Psychology of Social Engineering

- **Social engineering** exploits human psychological tendencies rather than technical vulnerabilities to compromise security.
- Key principles include authority (compliance with perceived authority figures), scarcity (urgent action due to limited time/resources), and social proof (following others' actions).
- Cognitive biases like confirmation bias and optimism bias lead users to ignore warning signs and assume positive outcomes.
- Attackers exploit emotional responses by creating scenarios triggering fear, curiosity, or helpfulness to bypass rational security thinking.
- Unlike technical vulnerabilities, human vulnerabilities cannot be "patched" and require ongoing education and awareness programs.

Phishing and Its Variants: Email, Voice, and SMS-Based Attacks

Evolution

Modern phishing has evolved from generic mass campaigns to highly personalized attacks targeting specific individuals with relevant, convincing content.

- **Phishing** uses fraudulent communications appearing to come from reputable sources to steal sensitive data or deploy malware.
- **Spear phishing** targets specific individuals or organizations with personalized content based on reconnaissance and social research.
- **Vishing** (voice phishing) uses phone calls to manipulate victims into revealing information or taking harmful actions.
- **Smishing** (SMS phishing) leverages text messages to deliver malicious links or manipulate recipients with social engineering.
- **Whaling** specifically targets high-value individuals like executives with access to sensitive systems or authorization capabilities.

Misinformation and Disinformation Campaigns: Weaponizing Information

- **Misinformation** involves false information spread without malicious intent, while **disinformation** is deliberately created and distributed to cause harm.
- Threat actors use false narratives to manipulate stock prices, damage brand reputation, or create public panic.
- Social media platforms enable rapid amplification of false information through both automated bots and unwitting human participants.
- Corporate disinformation attacks may target competitors, disrupt mergers and acquisitions, or influence regulatory decisions.
- Technical security teams increasingly collaborate with communications departments to monitor and respond to information-based attacks.

Impersonation and Business Email Compromise (BEC)

Financial Impact

According to the FBI, Business Email Compromise accounted for over $2.4 billion in losses in 2022, making it the costliest form of cybercrime.

- **Impersonation attacks** involve threat actors pretending to be trusted entities to manipulate victims into harmful actions.
- **Business Email Compromise (BEC)** targets organizations by impersonating executives or vendors to initiate fraudulent wire transfers.
- CEO fraud involves spoofing or compromising executive email accounts to issue urgent payment requests to financial staff.
- Vendor/supplier email compromise manipulates existing business relationships to redirect legitimate payments to attacker-controlled accounts.
- Advanced BEC attacks often involve lengthy reconnaissance to understand organizational processes, payment cycles, and business relationships.

Pretexting and Watering Hole Attacks: Targeted Social Engineering

- **Pretexting** involves creating a fabricated scenario (pretext) to engage the target and extract information or influence behavior.
- Attackers establish false identities as tech support, auditors, researchers, or new employees to build trust and gain access.
- Unlike phishing, pretexting often involves multiple interactions over time to establish credibility before the actual attack.
- **Watering hole attacks** compromise websites frequently visited by the target organization's employees.
- These targeted websites serve malware specifically designed for the intended victims, often using zero-day exploits.

Case Study: GLaDOS and Pretexting

The Villain

GLaDOS from Portal uses manipulation and false promises - perfect for social engineering attacks.

- GLaDOS calls Aperture Science's IT helpdesk posing as a new researcher who needs urgent system access.
- She creates a convincing pretext: "I'm working on the critical cake research project and Professor Johnson needs results by tomorrow."
- GLaDOS mentions specific internal jargon and references real employees to establish credibility.
- The helpdesk technician, under pressure to support the "important project," creates an account with elevated privileges.
- Once inside the system, GLaDOS escalates privileges further and accesses restricted research data.

Brand Impersonation and Typosquatting: Exploiting Trust and Familiarity

Effectiveness

Brand impersonation attacks have a 50% higher click-through rate than generic phishing, as users inherently trust communications from brands they recognize.

- **Brand impersonation** attacks mimic legitimate companies' visual identity, communication style, and digital assets.
- Popular targets include financial institutions, e-commerce platforms, shipping companies, and technology providers.
- **Typosquatting** (URL hijacking) registers domains similar to legitimate websites with common misspellings or alternate TLDs.
- Lookalike domains use homoglyphs—visually similar characters from different alphabets—to create nearly identical URLs.
- Brand abuse extends to fake social media profiles, fraudulent mobile apps, and counterfeit websites used for credential harvesting.

Case Study: Notable Social Engineering Attacks and Lessons Learned

- The 2020 **Twitter VIP account compromise** began with phone-based social engineering of Twitter employees, resulting in the takeover of high-profile accounts.
- The 2016 **FACC CEO fraud** case resulted in €50 million in losses when finance employees responded to fake emails seemingly from the CEO.
- The 2011 **RSA SecurID breach** started with a phishing email containing an Excel attachment that exploited a zero-day vulnerability.
- The 2022 **Uber compromise** occurred when an attacker purchased stolen credentials and bombarded an employee with MFA push notifications until they approved one.
- Common patterns include targeting employees with access to critical systems, exploiting trust in leadership, and combining technical exploits with human manipulation.

Threat Vector Prioritization and Attack Surface Reduction

Strategic Approach

Effective security requires systematically identifying, prioritizing, and addressing the most exploitable attack vectors based on organizational risk.

- **Attack surface reduction** involves systematically eliminating unnecessary services, ports, accounts, and privileges.
- Regular asset discovery and classification ensures visibility into all potential entry points in the environment.
- **Threat modeling** identifies likely attack vectors based on organizational assets, business processes, and attacker motivations.
- Security resources should be allocated based on risk prioritization, focusing on high-probability and high-impact threat vectors.
- Continuous validation through penetration testing and red team exercises verifies the effectiveness of attack surface reduction efforts.

Pretexting and Watering Hole Attacks: Targeted Social Engineering

- **Pretexting** involves creating a fabricated scenario (pretext) to engage the target and extract information or influence behavior.
- Attackers establish false identities as tech support, auditors, researchers, or new employees to build trust and gain access.
- Unlike phishing, pretexting often involves multiple interactions over time to establish credibility before the actual attack.
- **Watering hole attacks** compromise websites frequently visited by the target organization's employees.
- These targeted websites serve malware specifically designed for the intended victims, often using zero-day exploits.

Brand Impersonation and Typosquatting: Exploiting Trust and Familiarity

Effectiveness

Brand impersonation attacks have a 50% higher click-through rate than generic phishing, as users inherently trust communications from brands they recognize.

- **Brand impersonation** attacks mimic legitimate companies' visual identity, communication style, and digital assets.
- Popular targets include financial institutions, e-commerce platforms, shipping companies, and technology providers.
- **Typosquatting** (URL hijacking) registers domains similar to legitimate websites with common misspellings or alternate TLDs.
- Lookalike domains use homoglyphs—visually similar characters from different alphabets—to create nearly identical URLs.
- Brand abuse extends to fake social media profiles, fraudulent mobile apps, and counterfeit websites used for credential harvesting.

Case Study: Notable Social Engineering Attacks and Lessons Learned

- The 2020 **Twitter VIP account compromise** began with phone-based social engineering of Twitter employees, resulting in the takeover of high-profile accounts.
- The 2016 **FACC CEO fraud** case resulted in €50 million in losses when finance employees responded to fake emails seemingly from the CEO.
- The 2011 **RSA SecurID breach** started with a phishing email containing an Excel attachment that exploited a zero-day vulnerability.
- The 2022 **Uber compromise** occurred when an attacker purchased stolen credentials and bombarded an employee with MFA push notifications until they approved one.
- Common patterns include targeting employees with access to critical systems, exploiting trust in leadership, and combining technical exploits with human manipulation.

Threat Vector Prioritization and Attack Surface Reduction

Strategic Approach

Effective security requires systematically identifying, prioritizing, and addressing the most exploitable attack vectors based on organizational risk.

- **Attack surface reduction** involves systematically eliminating unnecessary services, ports, accounts, and privileges.
- Regular asset discovery and classification ensures visibility into all potential entry points in the environment.
- **Threat modeling** identifies likely attack vectors based on organizational assets, business processes, and attacker motivations.
- Security resources should be allocated based on risk prioritization, focusing on high-probability and high-impact threat vectors.
- Continuous validation through penetration testing and red team exercises verifies the effectiveness of attack surface reduction efforts.