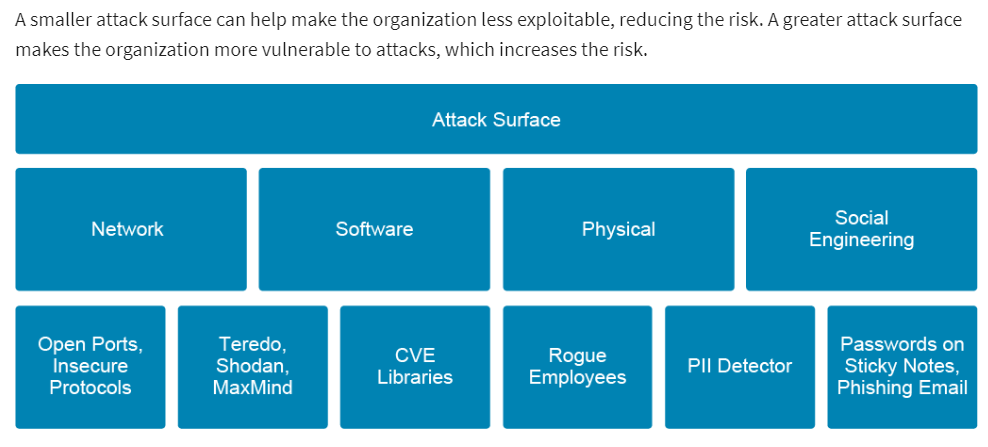
1. Attack surface



Attack surfaces can be divided in to the following four categories:

* The **network** attack surface comprises all vulnerabilities that are related to ports, protocols, channels, devices (smart phones, laptops, routers, and firewalls), services, network applications (SaaS), and even firmware interfaces. For example, some network protocols are inherently more insecure than others as they pass data over the network unencrypted. These protocols include Telnet, FTP, HTTP, and SMTP. Many Network File Systems, such as NFS and SMB, pass information over the network unencrypted. Remote memory dump services, such as netdump, also pass the contents of memory over the network unencrypted. Memory dumps can contain passwords or, even worse, database entries and other sensitive information. Other services, such as **finger** and **rwhod**, reveal information about users of the system. Network printers are also the target of a wide array of attacks from hackers because the operating system driver, management tools, and the printer’s software make them vulnerable. Printers can be attacked via the web-based administrative interface, SMTP, FTP, and SNMP.
* The **software** attack surface is the complete profile of all functions in any code that is running in a given system that is available to an unauthenticated user. An attacker or a piece of malware can use various exploits to gain access and run code on the target machine. The software attack surface is calculated across many different kinds of code, including applications, email services, configurations, compliance policy, databases, executables, DLLs, web pages, mobile apps, device OS, and so on. Unpatched software, such as Java, Adobe Reader, and Adobe Flash, also provide greater software attack surface because they are widely used. Publicly known cybersecurity vulnerabilities are listed in CVE libraries. Common CVE identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization’s security tools.
* The **physical** attack surface is composed of the security vulnerabilities in a given system that are available to an attacker in the same location as the target. The physical attack surface is exploitable through inside threats such as rogue employees, social engineering ploys, and intruders who are posing as service workers. External threats include password retrieval from carelessly discarded hardware, passwords on sticky notes, and physical break-ins. Also, consider a scenario where an intruder steals or downloads the information from an entire drive and extracts the target data in the future.

Note: While the network and software attack surface categories are generally agreed upon within the IT industry, the other categories are more loosely defined. For example, you may see overlap between the physical and social engineering categories or references to social engineering as an attack vector within the physical attack surface.

* The **social engineering** attack surface usually takes advantage of human psychology: the desire for something free, the susceptibility to distraction, or the desire to be liked or to be helpful. A few examples of human social engineering attacks are fake calls to IT, where the attacker is posing as an employee to get a password; or media drops where an employee might find a flash drive in the parking lot, and when they use that device, they inadvertently execute automatic running code leading to a data breach. Socially engineered Trojans provide another method of attack. An end user browses to a website that is usually trusted, which prompts the end user to run a Trojan. Most of the time the website is a legitimate, innocent victim that has been temporarily compromised by hackers. Another very popular method is an APT attacker sends a very specific phishing campaign, which is known as spear-phishing, to multiple employees' email addresses. The phishing email contains a Trojan attachment, which at least one employee is tricked into running. After the initial execution and first computer takeover, an APT attacker can compromise an entire enterprise in a short time.

1. Attack Vectors

An attack vector is a path or route by which an attack was carried out. Examples of attack vectors include malware that is delivered to users who are legitimately browsing mainstream websites, spam emails that appear to be sent by well-known companies but contain links to malicious sites, third-party mobile applications that are laced with malware that are downloaded from popular online marketplaces, and insiders using information access privileges to steal intellectual property from employers.

Common security threats include the following:

* **Reconnaissance:** The attacker attempts to gather information about targeted computers or networks that can be used as a preliminary step toward a further attack seeking to exploit the target system. For example, what operating system is on the target systems? Is there a firewall? Which ports are available? Which content management system (CMS) does the system run? There are also sources of information such as Facebook, Twitter, and Google that can be used to gather information about organizations or persons that are being targeted.
* **Known vulnerabilities:** The attacker finds weaknesses in hardware and software and then exploits those vulnerabilities.Several online resources publish information about vulnerabilities that have been discovered in different systems. Often, a proof-of-concept attack code will be provided with the vulnerability disclosure. Each platform has its own strengths and weakness. Once the target system is identified, it is simply a matter of trying out the different attacks for the targeted system to see which attacks work.
* **SQL injection:** This attack works by manipulating the SQL database queries that the web application sends. An application can be vulnerable if it does not sanitize user input properly, or uses untrusted parameter values in database queries without validation. According to research from U.S.-based cloud service provider Akamai in its State of The Internet report, SQL injection attacks accounted for 65 percent of web-based attack vectors from November 2017 to March 2019. In its report, Akamai noted that “The growth of SQLi as an attack vector over the last two years should concern website owners. In the first quarter of 2017, SQLi accounted for 44% of application layer attacks. This actually represented a rather large drop from the previous baseline, which was historically slightly over 50%."
* **Phishing:** The attacker sends out spam email to thousands of recipients. The email contains a link to a malicious site that has been set up to look like, for instance, a regular bank’s site. When the user enters their credentials in the login form, it actually is captured by the malicious site and then used to impersonate that user on the real site. Spear phishing is another variation of the phishing attack, in which the attacker usually targets specific persons. The RSA breach in 2011, which resulted in unspecified data that are related to their SecurID product being stolen, started with a spear phishing attack.
* **Advanced Persistent Threat:** An advanced persistent threat (APT) is a covert cyber attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network, and remains undetected for a significant period. Between infection and remediation, the hacker will often monitor, intercept, and exfiltrate sensitive data from the network. APTs intend to exfiltrate or steal data, and not cause a network outage, cause a denial of service, or infect systems with malware. APTs often use social engineering tactics or exploit software vulnerabilities, and usually target organizations with high value information.
* **Malware:** Short for malicious software, malware may be computer viruses, worms, Trojan horses, dishonest spyware, and malicious rootkits.
* **Weak authentication:** These exploits occur because of poorly designed or poorly implemented authentication mechanisms. Weak authentication usually means one or more of the following: weak, guessable passwords are allowed, no lockout enforcement after a specific number of invalid login attempts, or the password reset methods are not secure.

Other common threats, such as security misconfiguration, cross-site scripting, cross-site request forgery, and HTTP header manipulation, have not been included in the list above.