Attack surface

The **attack surface** of a software environment is the sum of the different points (for "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.[1][2] Keeping the attack surface as small as possible is a basic security measure.[3]

Contents

Elements of an attack surface

Worldwide digital change has accelerated the size, scope, and composition of an organization's attack surface. The size of an attack surface may fluctuate over time, adding and subtracting assets and digital systems (e.g. websites, hosts, cloud and mobile apps, etc). Attack surface sizes can change rapidly as well. Digital assets eschew the physical requirements of traditional network devices, servers, data centers, and on-premise networks. This leads to attack surfaces changing rapidly, based on the organization's needs and the availability of digital services to accomplish it.

Attack surface scope also varies from organization to organization. With the rise of digital supply chains, interdependencies, and globalization, an organization's attack surface has a broader scope of concern (viz. vectors for cyber attacks). Lastly, the composition of an organization's attack surface consists of small entities linked together in digital relationships and connections to the rest of the internet and organizational infrastructure, including the scope of third-parties, digital supply chain, and even adversary-threat infrastructure.

An attack surface composition can range widely between various organizations, yet often identify many of the same elements, including:

- Autonomous System Numbers (ASNs)
- IP Address and IP Blocks
- Domains and Sub-Domains (direct and third-parties)
- SSL Certificates and Attribution
- WHOIS Records, Contacts, and History
- Host and Host Pair Services and Relationship
- Internet Ports and Services
- NetFlow
- Web Frameworks (PHP, Apache, Java, etc.)

- Web Server Services (email, database, applications)
- Public and Private Cloud

Understanding an attack surface

Due to the increase in the countless potential vulnerable points each enterprise has, there has been increasing advantage for hackers and attackers as they only need to find one vulnerable point to succeed in their attack.[4]

There are three steps towards understanding and visualizing an attack surface:

Step 1: Visualize. Visualizing the system of an enterprise is the first step, by mapping out all the devices, paths and networks.[4]

Step 2: Find indicators of exposures. The second step is to correspond each indicator of a vulnerability being potentially exposed to the visualized map in the previous step. IOEs include "missing security controls in systems and software".[4]

Step 3: Find indicators of compromise. This is an indicator that an attack has already succeeded.[4]

Surface reduction

One approach to improving information security is to reduce the attack surface of a system or software. The basic strategies of attack surface reduction include the following: reduce the amount of code running, reduce entry points available to untrusted users, and eliminate services requested by relatively few users. By having less code available to unauthorized actors, there tend to be fewer failures. By turning off unnecessary functionality, there are fewer security risks. Although attack surface reduction helps prevent security failures, it does not mitigate the amount of damage an attacker could inflict once a vulnerability is found.[5]

See also

- Vulnerability (computing)
- Computer security
- Attack Surface Analyzer
- Vector (malware)
- Vulnerability Management
- Vulnerability Scanner

References

1. "Attack Surface Analysis Cheat Sheet" (https://web.archive.org/web/20161223133056/https://www.owasp.org/index.php?title=Attack_Surface_Analysis_Cheat_Sheet&oldid=156006). Open Web Application Security Project. Archived from the original (https://www.owasp.org/index.php?title=Attack_Surface_Analysis_Cheat_Sheet&oldid=156006) on 23 December 2016. Retrieved 30 October 2013.

2. Manadhata, Pratyusa (2008). *An Attack Surface Metric* (http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf) (PDF). Archived (https://web.archive.org/web/20160222045620/http://reports-archive.adm.cs.cmu.edu/anon/2008/CMU-CS-08-152.pdf) (PDF) from the original on 2016-02-22. Retrieved 2013-10-30.
3. Manadhata, Pratyusa; Wing, Jeannette M. "Measuring a System's Attack Surface" (https://www.cs.cmu.edu/afs/cs/usr/wing/www/publications/ManadhataWing04.pdf) (PDF). Archived (https://web.archive.org/web/20170306210801/http://www.cs.cmu.edu/afs/cs/usr/wing/www/publications/ManadhataWing04.pdf) (PDF) from the original on 2017-03-06. Retrieved 2019-08-29.
4. Friedman, Jon (March 2016). "Attack your Attack Surface" (https://web.archive.org/web/20170306025153/https://www.skyboxsecurity.com/sites/default/files/Attack%20Surface%20Visualization.pdf) (PDF). *skyboxsecurity.com*. Archived from the original (https://www.skyboxsecurity.com/sites/default/files/Attack%20Surface%20Visualization.pdf) (PDF) on March 6, 2017. Retrieved March 6, 2017.
5. Michael, Howard. "Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users" (http://msdn.microsoft.com/en-us/magazine/cc163882.aspx). Microsoft. Archived (https://web.archive.org/web/20150402070607/https://msdn.microsoft.com/en-us/magazine/cc163882.aspx) from the original on 2 April 2015. Retrieved 30 October 2013.
