Caleb M Lemmons

Benjamin Blakely

Cpr-E 234

Mar. 25, 2022

With malicious activity on the internet skyrocketing, people are becoming increasingly more aware of the necessities of cyber security. Attackers getting more sophisticated leaves security professionals backed into a corner. Methods of threat modeling for varying organizations have been established to include set guidelines to work with and avoid vulnerable and elementary means of protection. In an industrial control systems environment, threat modeling tactics are even more necessary. The Saudi Arabian Aramco Oil Company is the world's largest oil and gas company and deals with important yet highly dangerous machinery like oil pumps on a refinery plant. Aramco's abundant assets and high-level machinery put a sizable target on their heads. With threat modeling frameworks like the ATT&CK and STRIDE frameworks, Security professionals are better equipped to spot possible threats in different mechanisms of an organization's network. The assistance of the CAPEC and ATT&CK framework is not finished when each threat is found. Each potential threat found has varying possibilities of threat actors, vectors, and impacts. When used in its entirety, these frameworks guide organizations to a substantially secure environment.

The basic ideology behind threat modeling centers around the items an organization is trying to protect as well as whom they are protecting against. The place to start would be the STRIDE framework. This framework is a guideline used to help identify potential threats and makes for a good starting point in the active threat modeling process. The STRIDE framework finds the initial potential threats to worry about, and with frameworks like the ATT&CK and CAPEC, cyber security professionals can classify those threats found in the STRIDE model through categories of attack patterns and tactics a cybercriminal could potentially use. When dealing with valuable goods on an international level, a threat of attack becomes more of a risk factor. When tampered with, industrial control system environments can be very dangerous for people on site. Attacks on an ICS put an organization at risk of losing millions of dollars and dozens of potential deaths from oil spills, gas leaks, and plant explosions. There are many ways an attacker could pose a threat, but the STRIDE framework allows you to simply choose potential threats that seem worthy of consideration.

Spoofing was a major risk factor to consider because of the varying and subtle ways attackers deploy these tactics. Spoofing is the impersonation of another user to trick a victim into allowing unwanted access and violates the authentication property. Spoofing methods range from impersonating technical support to showing up as a delivery guy. Spoofing also relates closely to

phishing attacks. Whaling an executive through a fake company email and spear phishing as a third party ally all classify as phishing which lies under the umbrella of spoofing. Spoofing is a common tactic and should be addressed in an organization's security policies. Though dangerous, spoofing is just a means of gaining access; problems begin to skyrocket when access is gained.

Attackers with access are looking to control a network or the opposite, which are both unfortunate outcomes. Industrial control systems in the oil and gas industry hold availability second to none on the CIA triad. These companies rely on oil and gas production, and if an oil pump or a refinery machine is down, they lose a substantial amount of money. With attacks like denial of service that target availability, attackers are able to do major damage. Aramco's dependency on the availability of oil production is why a denial of service attack would be detrimental to the company. The last and most versatile threat I found worth consideration was tampering with data. Like spoofing, tampering with data is an umbrella term with many subcategories and vectors to dissect. This stage shows that an attacker already has some access, which could be an insider to the company. Tampering with data breaks the Integrity aspect of the CIA triad and is a base for other threats like escalation of privilege and ransomware. Tampering with data or assets in an oil plant could cause machine malfunctions, damages, or worse. Different ways of tampering with system information can be classified into covert and overt damages. Covert damages refer to minor or hardly noticeable changes to a system like changing configurations or shutting down the operations of a crucial piece of machinery. Cover damages can be more of an annoyance to deal with because of their hard to detect nature, but on the other hand, overt damages are louder attacks that are, in turn, more powerful.

In this threat modeling process, it is important to first dissect potential threats and the subcategories that resonate as threats to the organization. We can easily determine potential threat actors, vectors, and assets at risk for a specific threat by first settling on what assets are along with possible breach points. When viewing potential spoofing tactics, threat actors are less clear than usual because of the popularity of spoofing in the cyber world. Phishing emails and other more interactive forms of attack have been the most exploited in recent times. It would be most common for competitors or unaffiliated third parties to attempt such an attack. A competitor trying to gain access to disclosed information is not unlikely, but at the same time, an increase in the usage of this cybercrime makes it hard to pinpoint specific threat actors that may be responsible. These threat agents' attempts to engage in deceptive interactions include phishing and taking advantage of valid accounts and trust relationships. Spoofing is a constant threat to organizations like Aramco, and breaches could be a big setback. Possible technical impacts include the escalation of privilege, which leads to a compromised network leaving it at risk for more brutal tactics like ransomware attacks or simply the leaking of private company data. Spoofing in itself could be a minor problem with the right detection but can also lead to further destruction if an attacker is left undetected, as stated above. Damages like these could cost major asset loss and would leave a company down in funds to rebuild and for future mitigation. Anyone with decent cyber knowledge could perform spoofing attacks, and it is important to note that gaining further access and privileges differs from a spoofing attack.

However, tampering with the integrity of a system or network resonates more with the escalation of privileges because you need access to a powerful user like an administrator in order to view and tamper with configurations and information. Actors most able to pursue this method of attack are insider personnel. The main agent in question would be a disgruntled employee with the knowledge and access to system information. Other actors include partners or service providers with malicious intent. These threat actors share insider access and have the ability to possibly manipulate data structures and system resources inside the network or on hacked assets given by malicious providers. Various methods range from direct source manipulation to the injection of malicious software through USB. These actors exploit valid accounts and hardware additions; providers exploit and compromise the supply chain. Actions of this caliber could result in broken systems, information loss along with the impacts of a spoofing attack. In this case, an oil plant could be at risk of gas leaks, or explosion of a plant causing deaths as well as loss in assets and costs for repair. Similar impacts can be seen in a denial of service threat. As a more overt method of attack, cyber terrorists and malicious or neglected clients tend to be the common threat actors. By overloading a systems processing and storage, these cybercriminals exploit existing functionality in network systems. These can be administered through countless methods including phishing links and is a very common form of attack.

Fully dissecting security and possible threats for a large company would be near impossible without a guide. With the combined help of the ATT&CK, CAPEC, and STRIDE frameworks, we were able to classify important potential threats surrounding the basis of Aramco's investment in the oil and gas industry. The potential threats discovered were then broken down into specific cases that seem to pose the biggest threat in this scenario. Then, the threats are classified by potential threat agents, vectors, and impacts on the company. The second half of the threat modeling process can be viewed as a way to conclude the modeling process and begin implementation. Aramco is already an established company and has strong cyber security practices. Initiations of action against threats include security tactics like the least privilege principle and detection systems like IDS and SIEM systems which are necessary for such a big organization.

References

Attack.mitre.org. 2015. *MITRE ATT&CK®*. [online] Available at: <https://attack.mitre.org/> [Accessed 8 April 2022].

Blakely, B., 2022. *L19 Threat Modeling*.

Capec.mitre.org. 2021. *CAPEC - CAPEC List Version 3.7*. [online] Available at: <https://capec.mitre.org/data/index.html> [Accessed 8 April 2022].

Hernan, Lambert, S., n.d. *Uncover Security Design Flaws Using The STRIDE Approach*. [online] Web.archive.org. Available at: <https://web.archive.org/web/20191211174549/https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach> [Accessed 8 April 2022].

Hewko, A., 2021. *STRIDE Threat Modeling: What You Need to Know*. [online] SoftwareSecured. Available at: <https://www.softwaresecured.com/stride-threat-modeling/> [Accessed 8 April 2022].

Kamal, M., 2019. *ICS Layered Threat Modeling*. [ebook] SANS, pp.1-4. Available at: <https://www.sans.org/white-papers/38770/> [Accessed 8 April 2022].

Pipikaite, A., 2021. *What the cyber-attack on the US oil and gas pipeline means and how to increase security*. [online] World Economic Forum. Available at: <https://www.weforum.org/agenda/2021/05/cyber-attack-on-the-us-major-oil-and-gas-pipeline-what-it-means-for-cybersecurity/> [Accessed 8 April 2022].