Bisrat Asefaw

CSS 310 (Cybersecurity and IA)

Prof. William W. Lidster

Spring 2021

About the company

Netflix is a top content platform and production company founded by Reed Hastings and Marc Randolph in Scotts, Valley California. The headquarter business revolves around components of original programming and is known for its subscription-based model that provides customers all over the world to stream movies and television episodes over the internet. Occupations surviving this company revolves around streaming technologists, business analytics, marketing, accounting, and IT supervisors.

Netflix has grown a huge amount over a decade. In 2001 Netflix had fewer than half a million subscribers, now with the financial growth throughout the years Netflix now has 73.94 million paying subscribers based in the US and Canada. User bases in the US and Canada accounts for a 36.3% share of global Netflix subscribers. Netflix offers three streaming plans which revolve in Basic, Standard, and premium, starting from $9 per month then ending at $18. With the increased subscribers in the US, the age group is from 35-44 years, as it continues to be the largest segment by 24% (*Netflix Revenue and Usage Statistics* 2021). This paper is going to discover insights about Netflix, its complexities, third party services, and three main threats that could have the maximum impact on the company's revenue and the vulnerability of the system.

.

About Security

Netflix protects its content from illegal leaking and distribution through the technology called multi-DRM (Digital Rights Management) and Forensic watermarking (Kim, *How Netflix protects its content-Part 1* 2019). As explained in the article *How Netflix Protect its Content,* "The functions of DRM are divided into encryption and decryption of contents and encryption key management" (P. 2). Forensic Watermarking is defined as a "field of a technology called digital watermarking. Digital watermarking refers to the technology of inserting and managing confidential information such as copyright information in various digital data such as photographs and videos" (Kim, *How Netflix protects its content-Part 1* 2019). The DRM is used by copyright holders to control the use of digital material. The functions used to encrypt DRM are preventable for the usage of encryption and decryption of certain contents to contain brief information for the company's database. The encryption key and the usage of the right information are transmitted separately from the content. There are many DRM solutions towards protecting Netflix's platform because it is used to prevent unauthorized use of digital content such as e-books, sound recordings, and videos, which allows only substantiate users to the content for an authorized period. When the content service provider or copyright provider found illegal distributed content, it will detect the watermark, track the user, and stop the user from using the service.

Systems, Applications, and Data

Netflix utilizes systems, applications, and data necessary to provide its customers need on watching a high-quality movie and provides a delivery system to place customer DVD orders. This is the core of the company's operation. Below is a list of applications, systems, and data that represent the major component of Netflix.

Employee Information such as contact information, employee actions, pay rates and bonuses, the number of years employed by Netflix and their position all of which are maintained by BambooHR. BambooHR is a third party company that maintains information about each employee, except health information. Employee health and insurance information is maintained by a third party health organization.

Netflix subscribers' information includes customer name, date of birth, home address, phone number, and billing information. This is information is managed on an internal storage database like DynamoDB and Cassandra (Form 10-K, 2010).

Multimedia broadcasting information such as movies, TV shows including the website "Netflix.com" is maintained in the cloud by a third party organization called Amazon webserver (AWS S3). Since Netflix requires a storage solution that is easily scalable, reliable, and highly available and AWS S3 provides those functionalities (How Netflix Protects Its Content, 2019). This provides high-speed and quality video streaming.

For Application Systems Netflix created a system design amplification that can direct a system of distributed servers that deliver pages and web content to a user based on the geographic locations of the user. This designed system is called Content Delivery Network (CDN).

Third Parties and Third Party Services

Netflix utilizes the services of third party cloud computing providers, more specifically, Amazon Web Services, as well as content delivery networks such as Level 3. Netflix utilizes the services of third party cloud computing providers, more specifically, Amazon Web Services, as well as content delivery networks such as Level 3 Communications, to help in efficiently streaming TV shows and movies.

Netflix utilizes DVD rental outlets and kiosk services such as Blockbuster and Redbox and provides delivery through US postal service for fast process and delivery of DVDs to US citizens.

Netflix utilizes Clover for credit and debit card payment processing. Any transaction and payments of subscribers are done through the third party organization, Clover. Maintains basic information about customers and customers card information.

The company uses internet services from internet providers for streaming the website "Netflix.com" including cable providers, such as Time Warner and Comcast; direct broadcast satellite providers, such as DIRECTV and Echostar; and telecommunication providers such as AT&T and Verizon (Form 10-K, 2010).

For providing more movie and TV-show choices to their customer, Netflix works with Apple iTunes, Amazon Prime, Hulu.com, and YouTube. For Entertainment purposes, Netflix utilizes services provided by video retailers such as Amazon.com online shopping and Best Buy.

Threat Analysis

As defined in the introduction section of this paper, the Netflix environment is mainly defined in the cloud (AWS) for storing and processing data, mainly movie and TV shows. Another business that helps increase Netflix revenue is delivering DVD to customers that use private cloud storage to save and process customer orders.

One of the primary threats to the organization would be any threat that can disrupt customers from accessing the Netflix website through the https://Netflix.com. A typical Threat would be a Worm that can instantiate a distributed denial of service (DDoS) attack to the server. A Worm is

a type of malware that “spreads copies of itself from computer to computer... it doesn’t need a software program to cause damage” (What is a computer worm and how does it work?). DDoS is a website or server attack that “will send multiple requests to the attacked web resource – with the aim of exceeding the website’s capacity to handle multiple requests” ...and makes it unavailable by flooding it with too much traffic (NortonLifeLock, what is a DDoS attack?). If Netflix.com is flooded with ping requests that are aimed to disrupt its functionality, subscribers will struggle to access media content. This could cause an increase in the number of unsatisfied customers with the business provided, causing more users to unsubscribe and this may cause Netflix revenue to suffer.

Another threat to the organization is attacks that could reduce video quality or accessibility of movies or tv shows that are broadcast through Netflix.com. A typical threat to this type of disruption could be a ransomware attack. Ransomware is a type of malware that “encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption” (Ransomware Guidance and Resources). The article cybersecurity watch posted by imagining communications states that, “new season of the highly popular Orange Is the New Black were stolen and then made available through a file-sharing site after Netflix refused to meet the hacker’s demands” (Cybersecurity watch: Top Five takeaways from Netflix Hack 2021). This clearly can negatively affect the trust between Netflix and movie production companies. Hence, the number of unsubscribes can increase due to the reduction of ordinal movies, causing Netflix revenue to decrease.

A third threat to the organization could be attacks that disrupt the delivery of DVD players to customers in time. A typical threat to this type of environment would be a trojan virus. A trojan is a malware attack that is a "malicious code or software that looks legitimate but can take control of your computer" (What is a trojan? Is it a virus or is it malware?). Once trojan malware is installed in the organizations operating system the attacker can control any activities that are performed by Netflix. In the case of the Netflix DVD delivery system, attackers could alter the destination address of customers or any information that helps to deliver the item in time. This could reduce the number of customers that shop DVDs from Netflix, which in turn might reduce Netflix revenue.

Corresponding Vulnerability of Netflix

This section examines vulnerabilities that the above-mentioned main threats of Netflix could exploit. Since Netflix revenue depends on the number of subscribers and growth of subscribers, the company's effort is to work on providing a movie service that is trusted by its customers. Below will be the system vulnerabilities that corresponds directly to the threats that are mentioned above that are worms that could be used for DDoS attack, ransomware, and trojan virus.

As corresponding to the DDOS attack that could disrupt the availability of Netflix website host (Netflix.com), a type of vulnerability that could be exploited is System configuration. A system configuration is that "security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities" (*Cyber Essentials Controls: Secure Configuration*). The system should be configured in a way that will

detect unauthorized software from running on the environment or the network. Hence it should also stop the execution of the worm as soon as it enters the environment in order to prevent the website from down for hours. Disruption of the service causes a decrease in customer satisfaction which in turn can cause a decrease in the number of service subscribers and revenue.

Similarly, a corresponding vulnerability of the Netflix environment that could be exploited by ransomware and cause disruption of video quality and availability of original movies can be due to improper configuration of the system. System configuration maintains, "what types and models of devices are installed and what specific software is being used to run the various parts of the computer system" (Techopedia, 2016). The system is supposed to recycle malicious malware software before it executes and performs the attack. The system should be patched regularly in order to prevent new emerging malware attacks. Hackers are always in search of underlying vulnerability when a new patch is released. If the hacker can successfully attack before the system is properly patched, there could be a high risk of breach.

A system configuration is a vulnerability that can be exploited by hackers to perform a trojan virus attack to disrupt the proper delivery of DVDs from the Netflix warehouse. The system should be configured and patched to avoid the execution of unauthorized softwire that could provide full control of the system to attacker (*Cyber Essentials Controls*). The Trojan virus creates a back door and allows the hackers to have full control of the system. Netflix system should stop the execution and/or operation of the virus. As the attackers have full control of the system, they can alter the delivery system. If customer's DVD orders got delayed or lost during delivery, their satisfaction could decrease and hence Netflix revenue could decrease.

Summary

To sum up, Netflix is a movie and tv-show broadcasting company that also relies on selling DVDs to customers throughout the U.S. to increase its revenue. The organization values satisfaction of customers from high-video quality streaming, and smooth and fast delivery of DVDs. Netflix's typical threats are Worms that might be used for DDoS attacks, Ransomware, and Trojan. These attacks can be performed through Netflix's system that is poorly configured.

References:

AWS. (n.d.). *The Courage of Innovation: A Conversation with Vernā Myers, VP of Inclusion Strategy at Netflix*. Amazon Web Services, Inc. Retrieved April 8, 2021, from https://aws.amazon.com/solutions/case-studies/netflix/

"Netflix Revenue and Usage Statistics (2021)." *Business of Apps*, 9 Mar. 2021, www.businessofapps.com/data/netflix-statistics/.

Kim, Daniel. "How Netflix Protects Its Content - Part 1." *Medium*, PallyCon, 21 June 2019, https://medium.com/pallycon/how-netflix-protects-contents-part-1-a40508ed0001

L, N. (2018, September 8). *NETFLIX system design - Narendra L*. Medium. https://medium.com/@narengowda/netflix-system-design-dbec30fede8d

Netflix, Inc. (2010, December 31). *Form 10-K*. UNITED STATES SECURITIES AND EXCHANGE COMMISSION. https://www.sec.gov/Archives/edgar/data/1065280/000119312511040217/d10k.htm

Written by Steve Weisman for NortonLifeLock. (n.d.). *What is a DDoS attack?* Norton. https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html.

What is a computer worm and how does it work? (n.d.). https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html.

Ransomware Guidance and Resources. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/ransomware.

Cybersecurity watch: Top Five takeaways from Netflix Hack. (2021, March 19). Retrieved April 26, 2021, from https://imaginecommunications.com/blog/cybersecurity-watch-top-five-takeaways-netflix-hack/

Written by Alison Grace Johansen for NortonLifeLock. (n.d.). What is a trojan? Is it a virus or is it malware? Retrieved April 26, 2021, from https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html#:~:text=A%20Trojan%20horse%2C%20or%20Trojan,or%20file%20to%20trick%20you.

Cyber Essentials Controls: Secure Configuration. IT Governance. (n.d.). https://www.itgovernance.co.uk/secure-configuration#:~:text=Secure%20configuration%20refers%20to%20security,criminal%20hackers%20look%20to%20exploit.

Techopedia. (2016, November 11). *What is System Configuration (SC)? - Definition from Techopedia*. Techopedia.com. https://www.techopedia.com/definition/12448/system-configuration-sc#:~:text=System%20configuration%20is%20a%20term,entire%20system%20and%20its%20boundaries.