Jonathan Tornberg

Professor Hodges

INLS 490.

11/7/18

INLS 490 Project 2 Report:

Threat Model for Silverspot Theater at University Mall

In recent years, movie theaters have become notorious for high prices. From tickets to concession prices, going to see a new movie can be an incredibly expensive venture for anyone let alone broke college students. For this reason, many movie goers have resorted to watching movies illegally online or, as this report will outline, finding ways to see movies in the physical theater for free or for a discounted rate. While this is certainly a threat for theaters across the country, this threat model will be made with a particular emphasis on the Silverspot Movie Theater at the University Mall in Chapel Hill, North Carolina. Due to its location right off of the University of North Carolina at Chapel Hill's campus, this theater is a hotspot for students and residents alike to come and view recently released films. Of course, this also means that it is a hotspot for students looking to view recently released movies for free. Listed below (Appendix A) is some background information on the theater, its location, and its pricing ("Silverspot Cinema".

Nighttime Showings	
Adult	$14.75
Senior 65+	$11.77
12 and Under	$9.30
Student	$10.11

Matinee Showings	
Adult	$11.77
Senior 65+	$10.40
12 and Under	$8.40

Location: 201 S Estes Dr. #100, Chapel Hill, N.C. 27514

In order to determine potential threats to security at the Silverspot theater, I utilized the STRIDE approach to threat modeling. This model works under the assumption that there are six primary ways that hackers or other malicious actors work to get into unsuspecting systems: spoofing, tampering, repudiation, information disclosure, denial of service, and escalation of privilege. Each of these methods suggest a unique form of attack that can rely on technical skills, social engineering, or a combination of the two. Additionally, each form of attack provides a threat to the CIA (confidentiality, integrity, and availability) triad by accessing confidential or proprietary information. Shown below is a threat model that lists potential vulnerabilities at the Silverspot Theater utilizing the STRIDE approach.

Threat Type	Potential Threats	CIA Violation(s)
Spoofing	• Attend movie with an outdated or fake one card or university ID • Impersonate mall/theater employee • Purchase theater concessions and attempt to sneak past the usher by claiming that I left ticket in theater • Utilize the ticket of another patron who purchased the ticket online • Use another patron's payment (i.e. using their credit card)	Confidentiality Integrity
Tampering	• Falsify a receipt or ticket • Utilize an old or outdated receipt or ticket • Hack into another users' account and use their data to purchase a move ticket • Shut down the payment system at Silverspot	Confidentiality Integrity Availability
Repudiation	• Call credit card company to dispute the charge from the theater • Call the theater company to dispute their charge for a ticket	Integrity
Information Disclosure	• Bribe a theater employee into giving me their employee discount • Bribe a theater employee into giving me another patron's account information	Confidentiality Integrity
Denial of Service	• Sneak in amongst a large group of paying customers	Integrity
Escalation of Privilege	• Pretend to be an executive from Silverspot reviewing the theater • Pretend to be an executive from the mall reviewing the theater	Integrity

As this table shows, there is a wide array of potential vulnerabilities at this theater with some (i.e. shutting down the payment system, hacking into users' accounts, or impersonating a Silverspot executive) having a higher damage potential than others. That being said, I see two vulnerabilities that have a far lower barrier of entry in terms of preparation and a far higher potential to occur on a more frequent basis. These two vulnerabilities, which I will discuss in this threat model, are: 1) attempting to utilize a spoofing attack by purchasing theater concessions and attempting to sneak past the usher by claiming that I left my ticket in the theater and 2) attempting a tampering attack by hacking into another users' account on Fandango (through a social engineering attack or otherwise) and purchasing a ticket with their account. Although these attacks may not have the same level of overall risk for Silverspot as the others, their potential frequency could result in a large-scale loss of revenue over an extended period of time. In addition, this report will also address possible remediations to these two vulnerabilities by considering the Center for Internet Security's Top 20 Controls and how they might relate to a social engineering attack of this kind ("CIS Controls", 2018).

Vulnerability 1:

Spoofing Attack by Purchasing Concessions and Sneaking Past Usher

In addressing the first vulnerability, there are assumptions that we must make. Primarily, we are working under the understanding that the concession booth is placed at the entrance prior to the usher stand. Additionally, we are assuming that there is only one usher placed at the main entrance to all of the theaters rather than multiple spread throughout the building as is sometimes the case during high traffic times. Another important factor to

consider with these attacks is that the movie-goer is not getting away without any payment as concessions are pricey for the average movie goer and an important driver of revenue for Silverspot.

In terms of approaches to carrying out this attack, there are two obvious options. In both instances, it would make sense for the attacker to purchase a large concession that will be clearly visible to the usher such as a large bucket of popcorn or a large soda. These give the appearance to the usher that the attacker has their hands' full or at least is willing to spend a significant amount of money on the concession. Listed below is a step-by-step approach to carrying out these two variations of a spoofing attack:

Approach 1: **Talk with Usher**	**Approach 2:** **Walk past Usher**
1. Purchase a large concession item 2. Approach usher with the large concession item clearly visible 3. Appear to be in a hurry or otherwise distracted by something (i.e. children, phone, or conversation) 4. Explain to usher that you have already entered the theater but left your ticket in the theater by accident 5. If usher is skeptical about claim, attempt to make a scene with loud noises, threaten to call manager	1. Purchase a large concession item 2. Walk on the opposite side of the usher into the theater area with the large concession item clearly visible on the side of the usher. 3. Preferably, wait for the usher to be busy with a line of other movie-goers giving him/her their tickets 4. Appear to be confident in your movement, know which theater you are going into beforehand and make a direct path towards it 5. If the usher does stop you, carry forward with the methodology lined out in approach 1

For both of these approaches, the burden is being placed entirely on the usher to be skeptical enough to check every passerby's ticket, or at the least to require them to come back from the theater to have their tickets checked. Although the burden of proof ultimately

remains on the movie-goer to provide their tickets, there is a potential that the usher may not feel comfortable asking the movie-goer to provide their ticket in order to maintain customer satisfaction. Furthermore, if the Silverspot Theater is understaffed or if the usher is generally apathetic about their work and the integrity of the ticket model, there is a high potential for this attack to be successful.

Because this vulnerability is fairly simple to exploit for attackers, this should be of primarily concern for Silverspot. Therefore, I have developed two primary remediation methods that could be utilized. The first and most simple solution would not require any expenses on the part of Silverspot. In this solution, the usher booth would be placed before the concession stand so that patrons are required to go past the usher and show their ticket prior to purchasing concessions. Although simple, this approach would successfully remediate both attack approaches as it forces all patrons to come into direct contact with the usher prior to purchasing the concession all while allowing patrons to easily leave the theater to come back and purchase more.

If this first approach is not possible, another potential solution that would primarily address approach 2 could be to put a sort of funnel system or turnstile in place that would require paying movie-goers and attackers alike to show their ticket to the usher before proceeding. Of course, the risk with this approach is that Silverspot would again be reliant on the usher to check each patrons' ticket. Furthermore, management would have to agree that ushers have the right to ask movie-goers to come back to the booth with their ticket if they leave it in the theater. Another concern with this remediation is usability and accessibility. For disabled patrons who are wheelchair-bound or otherwise handicapped, a turnstile could

prevent a challenge. There is also a potential for a line to build up which could frustrate paying customers.

Vulnerability 2:

Tampering Attack by Using Another Customer's Fandango Account

The second vulnerability that I will discuss is significantly more complex and technical in nature. Additionally, because of Silverspot's reliance on industry standard third-party ticket providers like Fandango, they inherently lose a degree of control over the chain of custody for the ticket as well as for their patron's information. As a result, any remediation suggested in this report would likely require a reworking of Fandango's contract with Silverspot and would therefore not be as immediate as the remediations in vulnerability 1. Listed below are two attack methods that hackers could use to get ticket information, one requiring technical expertise and the other requiring relatively simple social engineering:

Approach 1: **Steal Fandango users' credentials by creating a fake Fandango login page and spoofing a website's DNS**	**Approach 2 (assumes ability to obtain basic knowledge of victim, i.e. name, date of birth, etc.):** **Call Fandango and claim to have lost access to e-mail associated with account**
1. Utilize the "Site Cloner" function within the social engineering toolkit* to create a fake login page 2. Enter your IP address and the link to fandango.com 3. Launch an apache web server forwarded to port 80 to work as the web server where the attack will happen 4. Set up a configuration file that will forward the connections to your spoofed site 5. Track the user's login information in a harvester file. *Steps for cloning attack from hackingguides.com (Alexander, 2017)	1. Retrieve basic information about victim (either a friend or someone who you know has a Fandango account) 2. Call Fandango's helpline and ask which e-mail they have on file for your account 3. Explain to them frantically how you lost access to that account 4. Ask if there's any way for the representative to change the account's e-mail address to one that you have access to 5. Reset the account password with your new access and purchase a ticket with the payment information stored on their account

In terms of remediation, these approaches require different levels of technical and psychological expertise and vary in their potential severity. Approach 1, the more technical of the two, has the potential to pose a far greater threat to Fandango than Silverspot, but still may lead to bad publicity for Silverspot. In order for Silverspot to prevent such an attack, it is important they have a thorough understanding of Fandango's cyber security protocol and that their contract ensures compliance with the Center for Internet Security's top 20 controls ("CIS Controls", 2018). Unfortunately, if a patron were to fall victim to a malicious web server of this kind, the majority of the process is out of Fandango's control. With that being said, there are some precautionary measures that Silverspot ensures Fandango takes. Most importantly, compliance with control 16 (account monitoring and control) would be a critical step ("CIS Controls", 2018). By implementing multi-factor authentication, both the device logging into the website as well as the device utilized for multi-factor authentication would have to be utilizing the same malicious web server. While not perfect, a proper implementation of multi-factor authentication should minimize the risk associated with an attack of this kind.

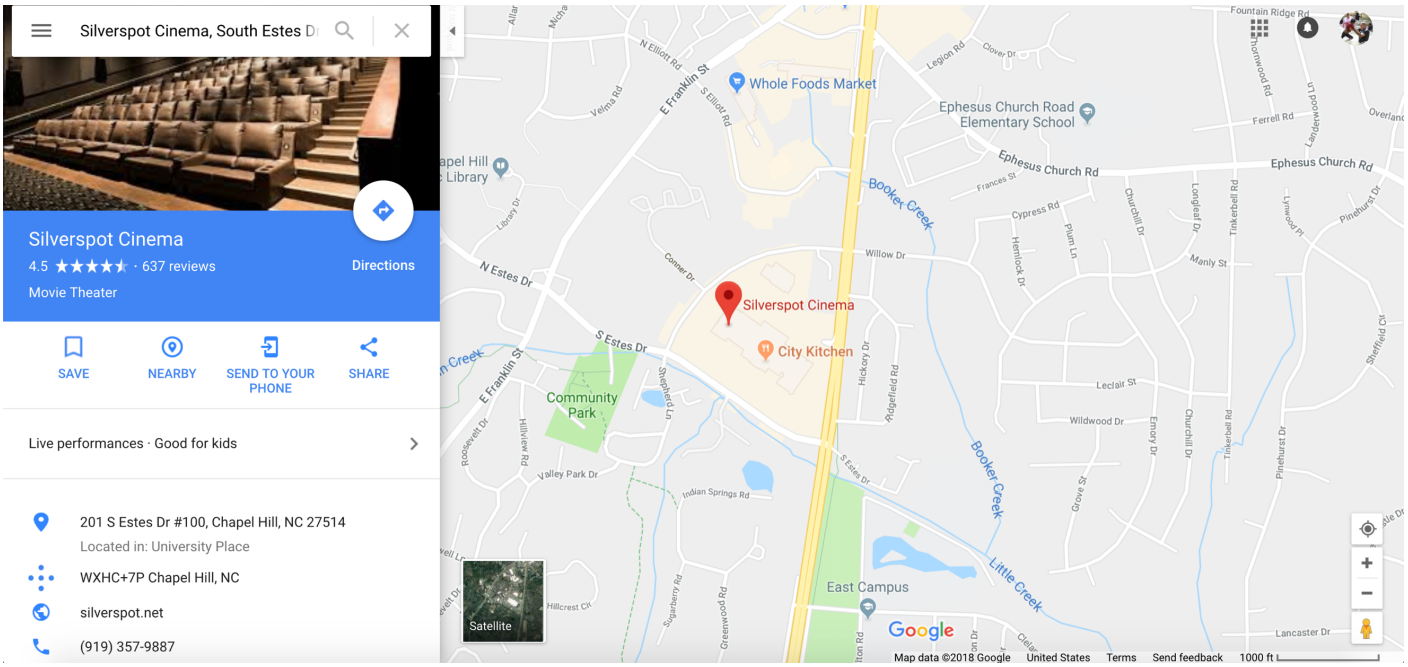
Finally, in regards to the second attack method, Silverspot will need to ensure that Fandango has properly trained their call-center employees to handle such situations. This training, as outlined in CIS control 17 (implement a security awareness and training program). Primarily by training their employees on "how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls" ("CIS Controls", 2018). By properly training staff to be wary of callers who do not have any of their personal information at hand, proper remediation steps can be taken only in cases where the caller can confirm that they are in fact who they claim to be. In combination with CIS control 4 (controlled use of

administrative privileges) would limit the ability to reset passwords or e-mails to only staff who have been properly trained to spot such an attack (“CIS Controls”, 2018).

Ultimately, would be nearly impossible to mitigate these vulnerabilities while still ensuring a usable and accessible interface for paying customers. That being said, proper training of ushers and other staff in addition with some physical boundaries should ensure a higher level of difficulty for those trying to sneak past. Furthermore, ensuring that Fandango and other third-party vendors are in compliance with the CIS controls should mitigate the majority of the risk associated with any technical or cyber attacks.

Appendix

A)


Silverspot Cinema, South Estes D
Silverspot Cinema
4.5 · 637 reviews
Movie Theater
Directions
SAVE
NEARBY
SEND TO YOUR PHONE
SHARE
Live performances · Good for kids
201 S Estes Dr #100, Chapel Hill, NC 27514
Located in: University Place
WXHC+7P Chapel Hill, NC
silverspot.net
(919) 357-9887
Whole Foods Market
Ephesus Church Road Elementary School
Ephesus Church Rd
Silverspot Cinema
City Kitchen
Community Park
East Campus
Booker Creek
Little Creek
Satellite
Google
Map data ©2018 Google
United States
Terms
Send feedback

Works Cited

Alexander. “Cloning Websites to Steal Usernames and Passwords.” *Hacking Guides*, Hacking Guides, 3 Aug. 2017, hackingguides.com/cloning-websites/.

“CIS Controls.” *CIS Control 20: Penetration Tests and Red Team Exercises*, Center for Internet Security, 2018, www.cisecurity.org/controls/.

“Silverspot Cinema.” *Silverspot*, Silverspot Cinema, www.silverspot.net/Ticketing/ssSelectMovie.aspx?cinemaId=0000000004.