Cybersecurity Magic:
Parallel Structures of Design by Hackers and Magicians

Samuel Sagan
Honors Thesis
Science, Technology, and Society Program
Stanford University
May 31, 2018

Advisor: John Willinsky, May 2018

STS Honors Program Director: Kyoko Sato, May 2018
Abstract

Almost half of the American public has been a victim of a major cyber-hacking incident and cyber-crime now tops the Gallup Poll’s list as the crime Americans worry about the most. (Pagliery 2014; Riffkin 2017) Yet for many Americans, their vulnerability to hacking seems mysterious. How can so much cyber-crime occur when so many technical efforts are devoted to preventing it? One possible answer to this question might be that cyber-hackers take advantage of common human psychological traits that make us all vulnerable to deception and misdirection. The ability to take advantage of such human vulnerabilities is part of the art of deception in many realms, such as espionage, warfare, politics, theatre, and especially in performance magic. What are the similarities and differences between the process used by cyber-criminals to design their hacking attacks and the process used by magicians to design their magic tricks? I investigated these connections by collecting primary sources and interviewing a small number of magicians, “white hat hackers,” and individuals from the national security intelligence community to discover how they design their activities to take advantage of individuals’ common human vulnerabilities and new technology vulnerabilities. I present multiple case studies and then compare specific magic tricks with specific cybersecurity exploits, demonstrating how the design processes used by hackers have inherent structural similarities to those used by magicians. Furthermore, this research demonstrates the value in demystifying the design processes of hackers and magicians to produce better cybersecurity.
### Table of Contents

**Introduction**...4

**Chapter 1: Literature Review**...15

**Chapter 2: Research Methodology**...31

**Chapter 3: Magicians and Hackers: Applying the Frameworks**...38

**Chapter 4: Conclusion**...53
Introduction

Three years ago, I noticed that my professor, Herb Lin, had “poor magician” listed as an avocational skill in his biography on CISAC’s (Center for International Security and Cooperation) website. Having performed as a magician for close to a decade, I decided to attend Professor Lin’s office hours to discuss this hobby of his. After we met to discuss our mutual interests in Magic and Technology, Professor Lin proposed that we conduct a research project comparing methods between hackers and magicians. Together, we designed a performance/lecture in which I would perform a magic trick and then Professor Lin and I would discuss relevant cybersecurity issues regarding the methodology or principles behind the trick that I had just performed. This lecture was conducted multiple times for professors, students, Congressional staffers, and reporters. Below is a link to the first performance:

https://www.youtube.com/watch?v=zqgpaiK1xh8

Once I decided that I was conducting a Science, Technology, and Society Honors thesis, I looked into the underlying motivations and discoveries of this initial project to see whether there was further analysis to make. The project with Herb Lin simply compared similar methods used between cybersecurity individuals and magicians. After closer analysis, I realized that these similarities were not just coincidental, and that it’s possible that cybersecurity individuals and magicians actually use strikingly parallel structures when designing their exploits.

Questions and Roadmap

Through the previous project with Herb Lin, we know that magicians and hackers use similar methods of distraction and misdirection to conduct their exploits. However, how far does this correlation go? To what extent can inherent structural parallels be demonstrated between the
development and execution of cybersecurity and magic exploits? Is the relationship simply analogous or do the parallels with magic help uncover the thinking behind the methods of cyber-crime? Through the past iteration of this project and the conclusions drawn from this thesis, I have discovered that the design and ideation process behind magic tricks and cybersecurity exploits share intrinsic parallel structures.

This initial conception of this thesis was informed by Barton Whaley’s 1982 article in the *Journal of Strategic Studies*, titled “Towards a General Theory of Deception.” In this journal article, Whaley compares magicians to military planners, but claims that the theory developed through this comparison could be applied to “diplomats, counter-espionage officers, politicians, businessmen, con artists, charlatans, hoaxers, practical jokers, poker players, gambling cheats, football quarterbacks, fencers, actors, artists, mystery story writers, or you or I in our everyday lives” (Whaley, 1982). Whaley does not include hackers or cybersecurity professionals, because these fields were in their infancy in 1982. In this thesis, I will both extend and test some of his theoretical ideas by applying his theories to the modern worlds of hacking and cybersecurity.

Whaley writes that “all modern magicians recognize that magic is applied psychology” (Whaley, 1982). Cyber-hackers and scholars analyzing any field of deception should recognize that cybersecurity is often applied psychology as well. Whaley provides a quote from a magician: “David Devant’s motto: Give me a good "effect" and I'll find a way to do it” (Whaley, 1982, 190). This thesis is informed by this motto, as aim to discover whether the “way to do it” is a consistent between magicians and hackers.

Magicians and hackers use similar methodology to design their exploits. However, are these similarities surface level, or are there inherent structural similarities between the design of a magic trick and a hack? This thesis aims to answer that question through analysis of existing
literature on magic, cybersecurity, and deceptive warfare and analysis of primary sources regarding the design process of particular magic tricks or cybersecurity exploits. Through my research, I have discovered similarities and parallels between magic and hacking, due to the fact that both are deceptive practices and exploit the same vulnerabilities.

This thesis is divided into five chapters. In the introduction, I discuss the inception of this project and the realization that it could be taken further than in the initial project conducted during my sophomore year and discuss my personal design process for a magic trick. Chapter 1 provides a literature review of various academic and popular sources connecting deception in the fields of magic, cybersecurity and in some cases, military security. In Chapter 2, I use the context provided by the literature review to present two case studies, aimed at showing the reader specific examples of magic tricks directly paralleling cybersecurity exploits. Then, I develop my “Characterizing the Primary Exploit of a Trick and Hack” and my “Framework to the Conception and Execution of Magic Tricks and Cybersecurity Exploits,” and provide example narratives to put these frameworks into a real-world context. In Chapter 3, I use this established framework to breakdown and analyze both primary published sources and new interview sources and see how they fit within the framework that I have constructed. Finally, in Chapter 4, I discuss the takeaways and discoveries of this project within a wider context. Before diving into my literature review, I will provide three narrative examples of the design processes of magic tricks and one brief case study of a cybersecurity hack. I provide these examples to enable reader to see some elements of design in magic and cyber-hacking.

Designing Magic Tricks

Below are three examples of the design process behind magic tricks. The first two discuss personal examples of magic tricks that I have designed with a Human Vulnerability in mind,
while the third follows a magician designing a trick with a technological vulnerability in mind. In the first two narratives, I am occupying the role of a Human Vulnerability magician, while in the third narrative Alan Rorrison is occupying the role of a Technological Vulnerability Magician.

The first example narrative will follow my personal process for designing a trick, specifically how I designed my own “Ambitious Card Routine.” The premise of an ambitious card routine at the base level is as follows: a card is selected, the card is memorized and placed into the center of the deck, the magician reveals that the card has risen to the top of the pack. Every magician is supposed to come up with his or her own method for performing this trick or some variation of it.

When I sought out to design my own ambitious card routine, I wanted to make it new and exciting, but had no idea of how to revamp a trick and almost every magician knows, many of whom have their own variations. I realized that while the other magicians’ tricks were drastically different in style, execution and sleight of hand, the “punchline” of the trick remained constant, the card appears on the top of the pack. Since this “punchline” was so ingrained into every version the trick, I realized that magicians and even some spectators are anticipating the punchline, ultimately removing some of the surprise of the trick. I decided that my method of performing this trick would have change the ending of this trick to exploit the audience’s preconceptions of the trick.

Once I knew that I wanted to change the punchline of the trick, I had to figure out a punchline that didn’t destroy the integrity of the effect. The origins of the name of this trick are relatively apparent when you see it performed: an ambitious card is placed in the middle of a deck and repeatedly appears on the top through its ambition. How could I portray an “ambitious
card” with a unique punchline? I came up with the idea to change the “ambition” of the card, so instead of jumping to the top of the pack, the card flips face up in the center of the pack.

Once I had decided how my trick would be different, I had to discover the method behind the ultimate execution of the trick. Since my punchline was so drastically different from the original idea, I couldn’t rely on the same sleights that other ambitious card routines did. I researched sleight of hand that had never been used in ambitious card routines to repurpose them for my ambitious card routine. The primary piece of sleight of hand that I ended up using was Aaron Fischer’s Gravity Half Pass, as taught in his book *Paper Engine*. (Fisher, 2012)

The practice period for this particular trick was much like how I practiced new tricks in high school, by attempting to fool my siblings. Since my siblings have seen me performing magic for years, their critical magic eyes are much more discerning than an average audience. These performances function as a refining period, where I can work through problems and perfect my sleight of hand.

The execution of this trick was two-fold. First, I wanted to show non-magicians this trick. Second, I wanted to show magicians this trick. While non-magicians were impressed by the trick, magicians found it much more intriguing.

Non-magicians saw this trick for its face value, not knowing any of the context behind it and why it was different from other ambitious card routines. Magicians, however, understood the context of the trick and were blown away by it. Since magicians knew the premise going in, the fact that I changed the premise made magicians much more excited by the trick. With this trick, I was toying with the magicians’ expectations, taking advantage of their prior knowledge of most ambitious card tricks by surprising them with a novel and unexpected twist.
I have continued to perform this trick for both magicians and non-magicians. My initial observation has continued with every performance. Since part of the initial conception of this trick was build up then exploit the expectations of magicians specifically, I’d say that this trick has continued to show me that expectations are a fantastic window of opportunity to a magical exploitation.

The second example narrative will again follow my personal process for designing a trick, but in this case, this a new trick that I designed while working on this project, making sure to record all the steps that I took in designing this trick. The trick starts with a card getting selected by an audience member, signed, then replaced in the pack. I reveal a card, that I claim is their selected and signed card. Upon the revelation that my selection was incorrect, I give the spectator the incorrect card to hold on to. Then, I find their original card in the deck, and reveal that it has a small corner torn off. I ask them to tear up the incorrect card in their hand and in between the layers of paper making up that playing card, is the matching missing corner of the original card.

I perform many tricks that involve tearing playing cards in half, and at every performance the act of tearing a card shocks the audience. I realized that under pretenses set up by a “card trick,” the audience rarely expects a card to be destroyed during a trick. I had the idea that if the destruction of a card is the ultimate reveal of the trick, the audience will be shocked not only by the magic trick itself, but also by the act of tearing up the card.

Once I knew that I wanted to exploit this expectation, I had to work out how to exploit this expectation. I discovered that with great care and caution, I could peel back the layers of a playing card, creating a pocket between the layer with the back design printed on it and the layer
with the value of the card printed on it. I realized that I could glue these layers back together with a small object (i.e. the corner of a playing card) embedded in the card itself.

The biggest piece of misdirection integral for this trick, is not showing the audience that the corner of the card is already missing from the start of the trick. I worked through multiple complex pieces of sleight of hand to accomplish this, when I realized that simple covering the corner of the card with two fingers when showing the card to the audience and getting it signed was entirely effective in convincing the audience that the card was full. This also plays into the audience expectation, since they are not expecting a card to be torn or missing a piece during this trick so far.

I conducted my dry-run of this trick (performing in front of an audience for the first time), with my Thesis Advisor, Professor John Willinsky. Luckily, he observed a slight mistake that I made which ended up being integral to the effectiveness of the trick. When I performed this trick for Willinsky, I tore up the card myself, which caused him to suspect that I had planted the corner of the card in the torn pieces. I realized that the card must be torn by the audience member, for the trick to be fully effective.

The execution of this trick was conducting at an event at CoHo, a coffee shop and eatery located on Stanford Campus. This particular trick was set up as the finale of my act, so I spent 4 or 5 different tricks reading the audience and attempting understand how to best present the trick as to have the strongest impact. These initial tricks also serve as a vetting process for audience
volunteers, in which I can attempt to select the volunteer who will help execute the trick coherently and also provide an amusing reaction. The reaction to this trick was as expected and the audience enjoyed it profusely.

The third example narrative will breakdown the release of the Smoke by Alan Rorrison. Smoke is a device that allows the magician to “produce a cloud of smoke from [their] mouth, on command” (Rorrison and Bayme, 2010). Since I do not have the rights to reveal the methodology of the trick, all I will say about the nature of the trick is that it uses technology similar to that found in early electronic cigarettes.

The device was released to the public on August 6, 2010 by a magic company partnered with Rorrison called Theory11, but Rorrison must have spent significant time developing his initial idea into a product. (Rorrison and Bayme, 2010) According to Consumer Advocates for Smoke-Free Alternatives Association, electronic cigarettes were first introduced to American markets in 2006-2007. (CASAA, 2016) Presumably, Rorrison saw that this new technology, initially designed to help smokers quit, could be creatively repurposed to be used in magic.

Once Rorrison identified the technology that he wanted to use, he had to ideate and explore various ways that this new technology could be used in magic tricks. At the time that Rorrison was designing this product, there were other smoke products for magicians, such as Ultrasmoke 2000 and Pure Smoke. However, these devices allowed magicians to produce smoke from their sleeves, while Rorrison discovered a method to produce smoke from one’s mouth.

Rorrison’s next step was figuring out how to disguise the fact that he was using electronic cigarette technology. This was ultimately done by casing the technology inside a seemingly innocuous prop. Again, since I do not have the rights to reveal this trick, I will not go into more detail here.
The most innovative part of Rorrison’s release of this project was the fact that there was only one trick taught with the device. The trick taught was actually not very impressive and intentionally so. The trick was designed to highlight a very simple use of the product. Once the product was released, other magicians were encouraged to experiment with the device and come up with their own tricks using the product.

Releasing the product in this manner allows Rorrison to maintain the value of the trick by not exhausting the possibilities and applications of the product in promotional material. Incidentally, there is an economic parallel to cybersecurity here. There are cases of hackers and programmers selling Bots, or pieces of automated code for a particular function, to users for a variety of nefarious purposes. Much like Rorrison, hackers designing these bots do not have to show their own execution and instead allow others to use their tool to solve their own problems. For example, a student named Srijan Sharma, written about in Forbes “made $50,000 reselling sneakers” using various bots purchased online. (Heilweil, 2017) Sharma claims that he has “spent at least $2,000 on an assortment of bots to aid his business” (Heilweil, 2017).

In 2016, Rorrison released a follow up product, Smoke 2.0. According to Theory 11 “This new version also allows for bigger bursts of vapor,” since the technology behind electronic cigarettes has grown so much since the release of the initial product. (Rorrison, 2016)

**Case Study Comparison: Prepping the Battlefield**

This section compares one of the most clever and effective features of the now infamous Stuxnet program with a classic age-old card trick.

The Stuxnet program was a completely unpresented form of computer warfare, which, according to Kim Zetter, “Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment
the computers controlled” (Zetter, 2014). One factor that made the Stuxnet virus so effective was that it provided inaccurate equipment readouts, while slowly increasing the pressure in centrifuges, eventually causing them to fail. The accurate readouts were collected as the code lay malignant in the system. This code stayed in the system without actually executing any damages and only collected data. The feature of the malware that provided accurate readouts for the centrifuges is essential the program’s effectiveness, allow it to stay under the radar, while collecting data and “prepping the battlefield.” Once the data had been collected, the program spits the data back out allowing it to do copious damage before even being noticed.

The Teleporting Card Trick

While the concept and methodology behind this trick has probably existed for multiple generations, the method discussed here was popularized by Brian Brushwood, though his YouTube show Scam School.

The trick:

The magician has a card selected by an audience member. The card is committed to memory by the audience member, and then shuffled back into the pack. The selected card then appears in an impossible location, for example, under the spectator’s seat cushion.

The method:

For this trick, the magician uses a duplicate card. The magician must enter the room and place the card under the seat cushion before the audience has entered the room. The magician then uses sleight of hand to “force” the spectator to select the duplicate card from the pack. “Forcing” selection of a desired card is very common in magic and can be accomplished through dozens of different sleight of hand methods. The spectator must seem to have been picked at
random, that way they do not expect that there is anything important about the chair that they were sitting on. The magician must be able to make it appear that the everything is normal until he or she starts the trick. But if fact, the key to the vulnerability has already been placed under the spectator’s cushion.

Analysis:

This trick and this program are examples of what Herb Lin calls “prepping the battlefield” (Lin and Sagan, 2016). To “prep the battlefield” successfully, one must execute their hack or trick, before the victim or the audience is expecting to be deceived. If this is executed well, the preparation can stay hidden for a prolonged period of time.

These three narratives and the case study provided above serve several purposes for this thesis. First, these narratives serve as a way to introduce the readers to the world of magic, giving them context on the actual implementation of magic tricks from initial conception to execution. Second, through these narratives and case study, I would like the reader to gain some familiarity with the design process of a magician, since typically, non-magicians are not granted an insider view on these processes. Third, I want the reader to see in the case study that both magicians and hackers can use a similar methods and principles to help promote deception. Lastly, though this case study, I would like the reader to experience one of the ideas (presented in the initial lecture with Herb Lin), that inspired me to go forward with this project.
Chapter 1

Literature Review

While there have been writings connecting magical methods with cybersecurity, such as Maria Konnokova’s 2007 New York Times article, “Born to be Conned,” most of these kinds of articles essentially present magic as an analogous practice to hacking. Instead, my hypothesis is that the two practices are constructed and executed using parallel structures and thought processes. This literature review is divided into three sections: 1) a discussion on Kevin Mitnick and drawing connections with magic in select case studies, 2) an analysis of articles and books relating cybersecurity or espionage to certain elements of magic and 3) an analysis of texts written by magicians.

Kevin Mitnick

Kevin Mitnick’s two books The Art of Deception: Controlling the Human Element of Security, and The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers are collections of both fictional and genuine stories detailing Mitnick’s years of experience as a hacker. The main body of The Art of Deception is divided into eight different chapters, each outlining a different vulnerability: When Innocuous Information Isn’t; The Direct Attack: Just Asking for It; Building Trust; “Let Me Help You”; “Can You Help Me”; Phony Sites and Dangerous Attachments; Using Sympathy, Guilt, and Intimidation; and The Reverse Sting. While each of these chapters only analyzes a single vulnerability, Mitnick includes multiple case studies in each chapter, concluding each case study with an “Analyzing the Con” section.

This section of the literature review draws specific examples from Mitnick’s books and compares them to magic tricks in extensive case studies. Since Mitnick’s book does not
explicitly discuss magic methodology, these case studies are designed to provide both the structures behind Mitnick’s narratives and the necessary frameworks to compare these narratives to magic methodology. The magic tricks featured in this section are drawn from tricks that I have encountered in my ten plus years of performing magic. Since I personally perform many of these tricks, I have been able to develop intricate understandings of how these tricks successfully misdirect and control the audience’s attention. I have selected each of these tricks, because I have identified common structures and designs between the tricks and my research.

*Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker* is an autobiographical account of Mitnick’s exploits as a hacker. While this book is less formulaic than his others, it still provides insight into the methodology and principles behind Mitnick’s hacking. In fact, in the first few pages of this book, Mitnick cites visiting a magic shop regularly: “Magic was my original doorway into the art of deceiving people” (*Ghost in the Wires*, 4). It is interesting to note that Mitnick equates hacking (the subject of this book) and magic, qualifying them both under the category of “deceiving people.”

Mitnick goes on to discuss social-engineering, which he claims to have unintentionally discovered at a young age. Mitnick defines social-engineering as “the casual or calculated manipulation of people to influence them to do things that they would not ordinarily do. And convincing them without the least hint of suspicion” (*Ghost in the Wires*, 27). Interestingly, I was advised against using Mitnick’s work by Stanford Computer Science Professor, Keith Winstein, because he views Mitnick as a criminal not a hacker. Winstein is correct because Mitnick has served multiple stints in prison for cyber-criminal activities. However, I don’t believe his criminal actions should bar his ideas for the purpose of analysis in this thesis. In fact, his position as a genuine criminal makes his work even more relevant to the ideas explored in this thesis.
While his earlier books are extremely useful for the purposes of this thesis, *Ghost in the Wires* has significantly less analysis of particular cons and instead contains lengthy narratives less related to hacking and social-engineering. However, this book provides some of the context necessary to design my interviews, particularly the interviews with hackers. Since the book provides a look into Mitnick’s thought processes, it ended up being valuable for the early ideation towards the framework within this thesis.

In *The Art of Deception*, Mitnick discussed the social engineer’s ability to “Build Trust.” In this chapter, he breaks down the misconception that people who are susceptible to hacks are “stupid or [lacking] common sense” (Mitnick 2002, 41). One con that Mitnick describes here, focuses on the story of a hacker named Henry and his father.

**“Surprise Dad”**

The story presented here is presented to prove that “anyone, not just a [crooked] employee” has the capability to steal credit card information as long as they know the tactics. Essentially, Harry calls his dad’s favorite video store, and pretends to be an employee at another branch and says

“Are your [branch’s] computers working? Ours are up and down… I have one of your [branch’s] costumers here…. Look I’m holding up a line of costumers here. What’s the credit card number and expiration date?”

With this simple script, Harry is able to retrieve his father’s credit card information from a completely unsuspecting employee, who is none-the-wiser after the con has already occurred. Harry has to know only one name of a customer at first store, the name of the second store, and then he creates empathy with the clerk by pretending to be another clerk and sympathy by saying
that he is holding up a line of customers. Through limited information and some intuitive, he has become a trusted agent of sorts.

In his analysis of this con, Mitnick brings into question why we inherently trust people on the phone. In person, initial trust is typically built on appearance. Mitnick provides the examples of a “shabby stranger” and a stranger who is “nicely dressed, shoe shined, hair perfect with a polite manner and a smile” (Mitnick, 2002, p. 46). Obviously, we would trust the latter, however, especially over the phone, these snap judgements can be difficult to make accurately. Mitnick claims that even over the phone, “we judge these things and perhaps a dozen others unconsciously, in a flash, often in the first few moments of the conversation” (Mitnick, 2006, p. 46). In this case, the victim not looking for the “trick” at that point, and the trick is designed in a way to perfectly exploit that human vulnerability. The video store employee is not suspecting to be conned and therefore plays along perfectly into the hacker’s hands. Here, even if the victim gets suspicious, their suspicion formulates after the hack has already been fully executed.

**Cybersecurity, Espionage and Magic**

“Towards Science in Magic” is an article by Gustav Kuhn, Alym A. Amlani and Ronald A. Rensink in the *Trends in Cognitive Science Journal*, which details how magicians can portray apparently scientifically impossible tricks through three primary tools: “the ability to control attention, to distort perception, and to influence choice” (Kuhn et al., 2008). Gustav Kuhn and his co-authors give multiple examples detailing these three tools used by magicians. In their section detailing methods of misdirection or “the ability to control attention,” the authors note that “Magicians have found that control can also be achieved through repetition, or ‘off beat’ moments, which lead to a momentary relaxation (such as after a joke), during which the
spectrum's attentional ‘hold’ is relatively weak” (Kuhn et. al, 2008). Creating this low attention moment, can be conducted through either physical or psychological misdirection, or in some cases, both. According to the authors, “psychological misdirection controls spectators’ attention by manipulating their expectations…attentional orienting is determined by a person's goals and intentions” (Kuhn, et.al, 2008). Both methods of misdirection can be extremely effective, since the audience very rarely expects or anticipates either.

The authors also discuss “the ability to distort perception,” and “to influence choice” (Kuhn, et.al, 2008). These ideas are entangled due to the fact that influencing a choice requires the magician to “distort perception” in order to convince the audience that their choice was completely free and open. The authors discuss “the process by which your choice can be systematically influenced” (Kuhn, 2008), known in magicians’ terms as “forcing.” Since forcing requires the audience member to be unaware that their choice was influenced or forced, “such effects have potential for investigating the formation and distortion of human memory” (Kuhn, et. al., 2008). The topic of forcing was brought up during the CISAC Cybersecurity Magic Seminar, Stanford University 2016, during which Herb Lin equated forcing a playing card to a phony random number generator. Lin explains that much like the selected card is not truly a free choice, a random number generated by a hacked machine “is a ‘quote’ random number, that isn't really random [and] can be predicted” (Lin and Sagan, 2016, 15:20).

Although these methods can prove valuable to the scientist, care should be taken in using these techniques as a way of investigating the mind without destroying the necessary mysteries and secrets that give us so much joy. (Kuhn, et. al., 2008)

This closing statement from “Towards Science in Magic”, encapsulates one of the primary goals of this thesis: to show the value of magic methods in academic/scientific contexts without “destroying the necessary mysteries” of magic.
In her 2015 *New York Times* article, “Born to be Conned,” Maria Konnikova breaks down the idiom “you can’t cheat an honest man.” She shows that this statement is a prominent misconception with no grounding in evidence whatsoever. Konnikova first uses the example of the game “Three Card Monte,” also known as “Find the Lady.” It is important to note that in almost all cases, the “Three Card Monte” is a scam not a game. In fact, it is often described as “one of the most persistent and effective cons in history” (Konnikova, 2015). Konnikova then details the methodology used by con men, whom she describes as “exceptional judges of character” and “exceptional creators of drama” (Konnikova, 2015). The con’s persisting success is due to “a sort of narrative sweep that makes everything seem legitimate. Much like a talented hacker or even so a talented magician, “the power of a good con artist: the ability to identify your deepest need and exploit it.” (Konnikova, 2015).

Maria Konnikova’s 2016 book, *The Confidence Game*, also provides some useful analysis comparing the work of con artists to the work of magicians. Konnikova claims that “confidence games and magic tricks share the same fundamental principle: a manipulation of our beliefs” (Konnikova, 2016, 7). She tells the reader that both a successful con and a successful magic trick “[operate] at the most basic level of visual perception, manipulating how we see and experience reality” (Konnikova, 2016, 7). According to Konnikova “the best confidence games go under the radar” (Konnikova, 2016, 16) and can be repeated, much like how the best magic trick is one that can be “repeated ad infinitum” without the audience becoming “much more likely to discern the ruse” (Konnikova, 2016, 15).

In her 2014 *WIRED* article and subsequent book – *An Unprecedented Look at Stuxnet, The World’s First Cyber Weapon* – Kim Zetter analyzes the precedent, history and modern discourse surrounding the computer program designed to shutdown Iranian nuclear centrifuges,
eventually dubbed Stuxnet. While the United States and Israeli governments have not publicly acknowledged the program, Zetter cites multiple sources claiming to have worked on, or at least in close proximity to the Stuxnet program (originally called “Olympic Games”). Throughout her writing, Zetter discusses both cyber-espionage and human-espionage, the two necessary elements that allowed Stuxnet to not only infiltrate its target in Iran, but also spread across the world.

To get Stuxnet to its target machines, the attackers first infect computers belonging to five outside companies that are believed to be connected in some way to the nuclear program. The aim is to make each "patient zero" an unwitting carrier who will help spread and transport the weapon on flash drives into the protected facility and the Siemens computers. (Zetter, 2017)

In the passage above, Zetter discusses how the virus was to be snuck into the Iranian nuclear facility at Natanz. This furtive method of sneaking in the original Stuxnet code was necessary due to the fact that the computers in the facility were “air-gapped from the internet… [and] cannot be reached directly by the remote attackers” (Zetter, 2017). The use of a “patient zero” indicates that this government program was comfortable utilizing both cybersecurity methodology and espionage methodology. The patient zeros targeted by the Stuxnet virus were “trusted” because they were “trustworthy” that is they did not know that they were part of the hacking scheme. They were unwitting allies of the hackers.

**Deception and Military Affairs**

There is a precedent to the application of deception in security and cybersecurity. For example, *Cheating and Deception* by J. Bowyer Bell and Barton Whaley discusses uses of deception techniques as applied to war doctrine and espionage. It is interesting to note, that Whaley is a military historian who also wrote *Stratagem: Deception and Surprise in War*, as well as the previously discussed 1982 *Journal of Strategic Studies* article entitled “Toward a General
Theory of Deception” (Whaley, 2007; Whaley, 1982). Both of these works creatively analyze the use of deception in war and military security:

Magicians call this generally 'magic' or occasionally and privately 'deception' and specifically a 'trick' or 'illusion'. Soldiers and practitioners of intelligence call it 'deception'. Some military camouflagers call it 'strategic camouflage. (Whaley, 1982, 182)

By defining these terms, specifically redefining “deception” and its many monikers, Whaley creates a system in which deception can be discussed from both a magician’s and a soldier’s perspective. Whaley then continues comparisons in this manner reflecting on the parallel structures within magic and military strategy:

Magicians speak of the 'method', the means or procedure by which a trick is done, the part that must be hidden from the audience. Some also use the word 'dissimulation' itself. Military deception specialists call this variously 'cover', 'cover and concealment', or simply 'dissimulation', defining the latter as 'hiding the real'. Practitioners of intelligencers speak of 'cover' and 'covert'; and some camouflagers call it 'negative camouflage'. (Whaley, 1982, 183)

“Magicians repackage when they exchange costumes with an assistant in various 'substitution' illusions. A general may have a new unit in the line wear the distinguishing patches of the old to disguise the changeover. An admiral disguises a warship as a harmless freighter. General Dayan repackaged the opening stroke of the 1956 Sinai Campaign by publicly calling the seizure of the Mitla Pass a mere 'reprisal' to delay an all-out Egyptian counter-attack. (Whaley, 1982, 184)

Whaley conducts nine comparisons in this format with varying levels of broad applicability and specificity. However, each comparison serves to tell the reader that “deception is always possible; anything and any event is meat for the deception planner” (Whaley, 1982, 190) Whaley goes on to quote magician David Devant: “Give me a good "effect" and I'll find a way to do it” (Whaley, 1982, 190). This idea of the challenge of finding “a way to do it” ties directly into my theory of the Initial Conception, discussed in the next chapter.
According to magicians interviewed by Whaley and Bell, magicians use what they call a “trick brain, doublethink… [or] lateral thinking” (Bell and Whaley, 1991, 98). This “lateral thinking” simply means that to design effective magic tricks, magicians must be able to think in an atypical manner and see patterns and exploits that no one else does. They then cite cryptanalyst Major Herbert O. Yardley, who “referred to people who have the ability to think up ruses as ‘cipher brains.’” (Bell and Whaley, 1991, 98) B. Stewart Whaley, whom Bell and Whaley refer to as a “theorist of deception,” claims that “this devious or indirect mind is possessed by all deceivers whether they are magicians, psychics, con-artists, mystery writers, comedians, practical jokers, counterespionage officers, or military deception planners” (Bell and Whaley, 1991, 98). This idea of the “cipher brain” is incredibly intriguing since it is the first explicit example that I have found linking the thought processes of magicians to those of cybersecurity professionals. While Bell and Whaley do not explicitly mention cybersecurity when discussing the “cipher brain,” due to the fact that this book was written in 1991, before the field of cybersecurity existed. However, cybersecurity professionals can be grouped into Bell and Whaley’s category of “counterespionage officers.” To this point, hackers can also be grouped into “con-artists,” another group that Whaley identifies as prominent users of the “cipher brain.”

In their chapter titled “Magic,” Bell and Whaley discuss the archetype of a magician cheater, who is “unique among the cheaters” (Bell and Whaley, 1991, 129). This uniqueness stems from the fact that “the magician proclaims before all those he is about to deceive that he is going to do so” (Bell and Whaley, 1991, 129). This distinction among cheaters and magicians is quite prevalent in the magic community. Indeed, as James Randi has said “Magicians are the most honest people in the world; they tell you they're gonna fool you, and then they do it” (Weinstein and Measom, 2014). Randi is a retired stage magician who was featured on the
Tonight Show with Johnny Carson over 38 times, and is the founder of both The Committee for Skeptical Inquiry and The James Randi Educational Foundation. This statement made by him carries the exact same message as Bell and Whaley’s discussion of the “uniqueness” of the magician as a form of “cheater.” According to Bell and Whaley, the methodology behind magic and other forms of cheating and deception are “simple interplay,” however, “it is only the execution that demands skill” (Bell and Whaley, 1991, 130).

Bell and Whaley are adamant in their assertion that the underlying principles of magic are simple and easy to understand, while the execution and design are much more involved. Bell and Whaley quote Harry Blackstone, who is credited with inventing “The Floating Light Bulb.” The original light bulb for Blackstone’s trick, designed and constructed by Thomas Edison, himself, was memorialized in the Smithsonian in 1985. Bell and Whaley cite Blackstone saying, “Magic is nothing but pure psychology—applied in the right place” (Bell and Whaley, 1991, 130). After outlining various methods of misdirection used by magicians, they go on to discuss how magic starting as early as 1722, “magic [continues] to keep pace with technology” (Bell and Whaley, 1991, 139). They cite 18 cases of magicians using cutting edge technology to achieve their tricks, including a magician who in 1772 created a “magic lantern, the primitive prototype to the slide projector” and Robert-Houdin (Houdini’s name-sake) who used an electromagnet in a show in 1945. Intriguingly, Bell and Whaley claim that “few, if any magicians, however, deceive themselves that these new innovations do anything more that refresh a tired repertoire of effects” (Bell and Whaley, 1991, 142). Innovation and new technology “add nothing to the ancient psychological principles of deception and cheating” (Bell and Whaley, 1991, 142). This assertion ties Blackstone’s quote to the Yardley’s principle of the “cipher brain.” Blackstone specifically cites the “application” of psychological principles as being the important part to designing a
trick. The ability to discern when to use various psychological principles (by a magician, hacker or any other deceiver) could also be used as an indicator for someone who has a “cipher brain.”

Having sprung out of secretive government programs, modern day cybersecurity and hacking translates many of practices and methodologies from traditional espionage. This form of espionage particularly draws many practices and methodologies from magic. The Official CIA Manual of Trickery and Deception is probably the most explicit and blaringly obvious connection between espionage work and a magician’s handicraft. This book (originally written as a top-secret document in the 1950s) was recently released to the public. It is written as “step-by-step instructions to covert intelligence operatives in all manner of sleight of hand and trickery designed to thwart the Communist enemy” (Melton, 2010).

**Magicians**

This section of the literature review will discuss and analyze contemporary thinkers in the magic realm. Magicians have spent decades honing their craft and their insight into the principles of deception and misdirection could be integral progressing the discussion of this thesis.

According to Henry Gordon, the author of the foreword of Nathaniel Schiffman’s book *Abracadabra*, “Books based on [Magicians] principles are extremely rare” (Schiffman, 1997, 7). The chapter of this book titled “Foundations of Deception,” provides great scholarly analysis of deception as applied to magic tricks. Schiffman’s analysis focuses on proving or disproving common “theories” of magic and deception. The first of these theories is “the hand is quicker than the eye” (Schiffman, 1997, 15). Schiffman disproves this theory, citing psychologist Joseph Jastrow’s study in which “two great magicians of their time” were tested in “motor skills, sensory acuity and memory” (Schiffman, 1997, 15). One of the magicians in the study tested average in each of these categories, while the other “fell below the average population in such
factors” (Schiffman, 1997, 15). Schiffman goes on to claim that due to these average results, “clearly, something other than speed is at play here” (Schiffman, 1997, 15). Schiffman does provide an alternative explanation to this theory, declaring that “The hand is not invisible because it’s quicker than the eye—it’s invisible because the eye is distracted away from the hand at crucial moments” (Schiffman, 1997, 16). The second theory that Schiffman discusses is “The ‘Supernatural’ Theory,” in which an audience member believes that the magician “used psychic powers or metaphysical powers to produce their illusions” (Schiffman, 1997, 16). Interestingly, Schiffman debunks this theory by claiming that if a magician were to use supernatural powers, “there would be no point in the show” and that “the point of a magic show is that you don’t know how it’s done” (Schiffman, 1997, 16). Since the audience enters the show knowing that the magician will use “natural means,” the audience has “no idea how to explain it” (Schiffman, 1997, 16).

Beyond these initial discussions of “theories,” Schiffman discusses other “Foundations of Deception,” most notably, misdirection. Schiff details the methodology behind two different types of misdirection, “spatial misdirection” and “temporal misdirection” (Schiffman, 1997, 20). According to Schiff, “spatial misdirection” involves controlling the audience such that “while your attention is focused on one point in space, the action is happening at another point” (Schiffman, 1997, 18). However, Schiffman believes that this form of misdirection is a much less important tool in the magician’s arsenal when compared to “temporal misdirection… Misdirection in time” (Schiffman, 1997, 18). According to Schiffman, “One of the greatest achievements of the legacy of illusion is the almost complete cover-up of time misdirection. People know about space misdirection, but temporal misdirection has in a sense misdirected from the public’s eye” (Schiff, 1997, 18).
Schiffman’s very strongly advocates the utility of temporal misdirection in magic. The utilities of this form of misdirection are directly transmutable to forms of deception in cybersecurity and hacking. To further define temporal misdirection, Schiffman quotes Peter M. Nardi, “a magician and sociologist at Pitzer who shows his students magic tricks” (Schiffman, 1997, 23). According to Nardi, temporal misdirection works in magic because “the beginning and end of a trick is never clear.” Nardi provides the example of a coin trick in which sleight of hand is used to make a coin disappear. When the magician opens their hand to reveal that the coin has vanished, “what looks like the ending has already disappeared moments before… so the trick ended for you before, but for the audience it’s just ending now” (Schiffman, 1997, 24).

Director Christopher Nolan had an incredibly nuanced perspective on the methodology of magicians in his 2006 film The Prestige. Nolan not only centered this film’s plot around how magicians think and design their tricks, but also decided to require his actors to perform the sleight of hand on screen. By requiring every trick in this film to be genuinely performed on camera, Nolan relates to Schiffman’s theory of “the supernatural,” discussed on page 15 of this thesis. Much like Schiffman says magic can be less impactful when the audience believes that the performer “used psychic powers or metaphysical powers to produce their illusions,” (Schiffman, 1997, 16) magic portrayed in The Prestige would be less impactful if the audience believed that the tricks being performed were being done via camera trick. To successfully portray magic in this film, Nolan decided to bring a contemporary magic thinker into the film leading to “the involvement of Ricky Jay, one of the best magicians in the world and one of the finest playing card manipulators who ever lived” (Collis, 2006).

In a 1993 issue of The New Yorker, Mark Singer wrote a profile on his friend, Ricky Jay, whom Singer describes as “perhaps the most gifted sleight-of-hand artist alive” (Singer, 1993).
According to Singer, Ricky Jay has a “relentless passion for collecting rare books and manuscripts, art, and other artifacts connected to the history of magic, gambling, unusual entertainments, and frauds and confidence games” (Singer, 1993). However, rather than perform, Ricky Jay now “has devoted his energies mainly to scholarship and to acting in and consulting on motion pictures” (Singer, 1993). He appears in Christopher Nolan’s film *The Prestige* and served as a consultant for the film. While Jay rarely performs now, Marcus McCorison, a former president of the American Antiquarian Society, describes Jay as “a deeply serious scholar—I think he knows more about the history of American conjuring than anyone else” (Singer, 1993). Unlike most magicians, Jay’s fame is not limited to magicians’ circles. In fact, Steve Martin once described Ricky Jay as “the intellectual élite of magicians” (Singer, 1993). Interestingly, Jay “declines opportunities to perform for other magicians” because he despises events such as magic clubs and conventions where magicians “unabashedly seek to expropriate each other’s secrets” (Singer, 1993).

Darren Brown is an award-winning UK-based mentalist and illusionist. Mentalism is a type of performance magic, where the performer appears to have supernatural mental or intuitive skills. In his book *Tricks of the Mind*, Darren Brown provides dozens of tricks for his reader to learn and perfect. However, the most intriguing aspect of this book are the sections between the tricks, where Brown breaks down the psychology behind each of his tricks. Brown believes that
no level of technical skill can separate a good magician from a bad one, but instead that “it’s about entering a relationship with someone whereby you can lead him, deftly and economically, to experience an event as magical” (Brown, 2007, 34). The way in which Brown describes this relationship and the methodology to achieve it, seems to be very similar to the concept of the “cipher brain,” discussed above.

Brown delves deepest into the idea of the “cipher brain” in his section titled, Learning to Read People. The skills and methodologies discussed in this section very closely mirror some of the methodology taught in the CIA Manual of Trickery and Deception.

…in order to understand what behaviors are significant, one must first identify how a person normally behaves, in a less significant scenario… it is often crucial to first understand a person's normal behavior. (Brown, 2007, 226)

In this passage, Brown is specifically referring to how to read someone’s body language. However, this way of thinking can be extrapolated to apply to espionage or even cybersecurity. Interestingly, Brown breaks down the “common misconception…that people break eye-contact when they lie” (Brown, 226, 2007). In an example involving a student at a hypnosis show, Brown observed that he was able to deduce a lie, because “the time she lied was the only occasion that she kept eye-contact” (Brown, 227). Brown’s ability to observe this and then use this information to design a nearly foolproof magic trick seems to imply that he has what Major Herbert O. Yardley would call a “cipher brain.” While Brown may have more insight to particular mental phenomena due to his career as a mentalist than other magicians, this thesis will demonstrate the degree to which the thought processes used by magicians closely mirror or in some cases completely overlap with the methodology used by hackers and cybersecurity professionals to exploit and protect computer systems.
This thesis identifies and analyzes the common acts of deception and misdirection between cyber-criminals and magicians, specifically how these professions exploit human vulnerabilities. I detail the significance of these common acts in three distinct stages: conception, design/practice and execution. These cyber “tricks” are not new, but rather can be seen and understood through studying similar techniques used by magicians and conjurers. In fact, as far back as 1900, Norman Triplett studied “the psychology of conjuring deceptions” in order to combat what he called “sleight of hand artists” whose crimes were “obnoxious to law-abiding communities” (Triplett, 1900, 508).

To further analyze these three stages of both cyber-criminal and magic trick execution, I conducted interviews with members from two different groups: 1) magicians and 2) cybersecurity professionals and/or hackers. Hackers are set in a different category from cybersecurity professionals because in many cases the act of hacking is not criminal and should not be viewed as such. However, the actions and methodologies of hackers pulled from these interviews along with corroboration from cybersecurity professionals may provide insight into the actions and methodologies of cyber-criminals. If I am right, the structures and ideologies identified in these interviews should be parallel to structures and ideologies pulled from the interviews with magicians.
Chapter 2
Research Methodology

This chapter focuses on establishing the two frameworks that will be the basis for this analysis in this thesis. The first framework divides hacks and magic tricks into four categories based on the primary vulnerability being exploited. The second framework that I have designed provides structure for anecdotal narratives that provide context and understanding for the creative processes involved in the design of magic tricks and cyber-security exploits.

Framework of Analysis

The framework for the analysis for both magic and cybersecurity was developed with input for Professor John Willinsky and Professor Herb Lin. While I will attempt to place the contents of each interview into this framework, I do not expect that each interview will directly mirror my framework. The framework is designed to show the creative processes and design steps taken by magicians and hackers and the interviews will hopefully corroborate the framework and the ideas behind it. There are also many ideas that I would like to explore outside of this framework, such as the differences between automated and manual execution in hacks and magic tricks.

Characterizing the Primary Exploit of a Trick and Hack

Table 1: Matrix for Characterizing the Primary Exploit

<table>
<thead>
<tr>
<th></th>
<th>HUMAN</th>
<th>TECHNOLOGY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trick</td>
<td>Tricks in which the primary exploit is based on a human vulnerability</td>
<td>Tricks in which the primary exploit is based on a technological vulnerability</td>
</tr>
<tr>
<td>Hack</td>
<td>Hacks in which the primary exploit is based on a</td>
<td>Hacks in which the primary exploit is based on a</td>
</tr>
</tbody>
</table>
A further distinguishes between the types of tricks and hacks being discussed. Each trick or hack in the Results chapter will fall into human or a technological vulnerability (Table 2).

Table 2: The Chronological Conception and Execution of a Magic trick or Cybersecurity Exploit

<table>
<thead>
<tr>
<th>STAGES</th>
<th>HUMAN</th>
<th>TECHNOLOGY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Initial Conception</td>
<td>Observed Human Vulnerability</td>
<td>Observed new or previously unnoticed Technological Vulnerability or Possibility</td>
</tr>
<tr>
<td>2. Ideation</td>
<td>What are ways that this vulnerability can be exploited?</td>
<td>What are ways that this technology can be used by the magician or hacker?</td>
</tr>
<tr>
<td>3. Misdirection vs.</td>
<td>What steps must be taken to misdirect the audience away</td>
<td>What steps must be taken to disguise or hide the technology?</td>
</tr>
<tr>
<td>disguising</td>
<td>from the vulnerability being exploited</td>
<td></td>
</tr>
<tr>
<td>4. Practice</td>
<td>How should this be practiced, given that it should be</td>
<td>How much does the hack/trick rely on the technology and how intimately</td>
</tr>
<tr>
<td></td>
<td>practiced in “real” scenarios?</td>
<td>should the hacker/magician know the technology?</td>
</tr>
<tr>
<td>5. Dry-run</td>
<td>Dry-run to make sure that the human vulnerability can</td>
<td>Dry-run to make sure the technology works as expected in test conditions</td>
</tr>
<tr>
<td></td>
<td>be exploited as practiced in test conditions</td>
<td></td>
</tr>
<tr>
<td>6. Execution</td>
<td>Execution in the real world</td>
<td>Execution in the real world</td>
</tr>
<tr>
<td>7. Follow through</td>
<td>Make sure that the necessary steps were taken to hide</td>
<td>Make sure that the necessary steps were taken to cover up the technology</td>
</tr>
<tr>
<td></td>
<td>the vulnerability from audience/hacking victims</td>
<td>used</td>
</tr>
</tbody>
</table>

1. The Initial Conception
Every magic trick and every cybersecurity exploit has a point of initial conception. There must be moment when the individual discovers a vulnerability and sets on the path to discover how to exploit it. I believe that this initial conception can stem from two distinct types of vulnerabilities: 1) human 2) technological. It is definitely possible that someone could discover an exploit that uses both a human vulnerability and a new technology. However, I believe that in most cases, the initial conception would stem from one of these vulnerabilities and the other would be incorporated later in the Ideation or Design phases. I would also like to note here that there can be vulnerabilities in organizational systems. For example, Stanford’s course selection gives preference to majors. Feasibly, one could exploit this organizational system by declaring majors just to get into classes. However, for the purposes of this thesis, I will only be looking at technological and human vulnerabilities.

2. Ideation

Just because the magician or hacker has identified the vulnerability that they will exploit, they still must discover exactly how the will use this vulnerability to their own devices. In this phase, one must think of possible ways that this vulnerability could be exploited. By thinking of multiple uses, the magician/hacker can isolate the potentially most effective use.

3. Misdirection vs. Disguising

Once the magician/hacker has decided exactly how the exploit is going to be used, they must design the rest of the exploit. During this design process, the magician/hacker must figure out exactly how they will disguise the exploit. For a magician, this often consists of a design process that often includes “patter,” the carefully selected words that a magician uses to distract the audience. However, patter is only one example of misdirection, and a magician/hacker will often
use multiple layers of misdirection, including intricate finger movements or even costume choices to assure that their exploit is successful.

4. Practice

Practice is key in mastering any skill, but is extremely important when trying to learn a hack or a magic trick. Due to the strict scrutiny put on the magician by their audiences and on the hacker by their victims and the authorities, hackers and magicians must make sure that they practice their exploit until near perfection to avoid being caught or found out. It is also extremely important those following the first column of Figure 1 practice in “real” scenarios. For magicians, this typically means practicing for friends and family before rolling out the trick to a larger audience. However, for a hacker this practice could be executed in a myriad of ways, but it is most important that the human vulnerability be tested on real people. Technological exploits, by those following the second column of Figure 1 must also be practiced extensively. However, for the most part these exploits don’t need to be tested on humans, so the practice would involve learning as much as possible about the technology being used to best prepare for all possible failures on the part of the technology.

5. Dry-Run

The dry-run is a continuation of practice, but must be conducted under stricter test conditions. Once the magician or hacker has practiced sufficiently and is confident that they understand all the ins and outs of their exploit, they must do a last check under strict test conditions to assure that the exploit will be successful. If the dry-run is not successful, the magician or hacker would have to return to the previous steps to rework and redesign the exploit.

6. Execution
Once a successful dry-run has occurred, the magician or hacker will make plans for the actual execution. If the practice and dry-run were conducted well enough, there should be a relatively low chance of failure. Of course, there is the chance of failure with every exploit, but the practice and dry-run steps should be treated as a method to minimize this chance.

7. Follow Through

Just because the execution went well, doesn’t mean that the magician or hacker is off the hook from being discovered or found out. Many of elements that are part of the follow through must be taken or at least planned before the execution.

Example Narratives:

In the introduction of this thesis, I provided three example narratives with the goal of giving the reader tangible stories on the design process of a magic trick before getting into the deeper literature on both magic and cybersecurity. You may notice that the first two narratives fall into the first cell of row 1 in Table 1, while the third narrative falls into the second cell of row 1. You also may notice that each of these narratives almost directly mirrors The Chronological Conception and Execution of a Magic trick or Cybersecurity Exploit, provided in Table 2. In the next chapter of this thesis will apply these two tables to both first-hand interviews and primary sources.

Identifying the Interview Participants:

For this project, I aimed to have two sets of participants: 1) magicians and 2) cybersecurity individuals. Interestingly enough, I discovered that there was some overlap in these two categories. For magicians, I used my own network to reach out to magicians with varying skill sets in different types of magic. For cybersecurity professionals, I leveraged contacts through Professor Herb Lin and CISAC affiliate Whitfield Diffie. Whitfield Diffie is an award
winning American cryptographer, who upon the advice of Herb Lin, attending the first performance of the previous iteration of this project that Herb Lin and I conducted three years ago. I also managed to source contacts from Thomas Macaulay’s *Techworld* article, “7 White Hat Hackers You Should Know” (Macaulay, 2017).

Through emails and other contact methods (i.e. Facebook), I was able to find the participants for this study. However, since many of my contacts did not follow through or respond, I decided to bring in secondary sources, written by cyber-professionals as well to contribute to my research and arguments.

**Interview Protocol:**

The individuals involved in the interviews were given three options for participation:

1. In-person/phone/video interview conducted over 15-20 minutes.
2. Provide an anecdotal written account of a **HACK OR MAGIC TRICK**, providing as much detail on the design process of the trick as possible.
3. Fill out the questionnaire template below.

The goal of these interviews, regardless of the option selected, is to find parallel structures in the design of magic tricks and cybersecurity exploits.

**Cybersecurity Magic Survey**

1. For either a hack or a trick that you designed or that you have come to know intimately, please provide a brief description (including a name for it if there is one).
2. What initially led you to pursue this hack or trick?
3. Did it involve exploiting a vulnerability or a technology, and if so, how does the hack or trick take advantage of it?
4. How has the execution of the hack/trick in the real world differed from practice and/or dry runs of the hack/trick?
5. What steps are taken after the execution of the hack/trick to "cover your tracks"?
6. Are there other aspects about the origins or execution of the hack/trick that you would like to comment on, perhaps in comparison to another hack/trick?

While ideally, I would have liked to conduct in person interviews as often as possible, I found that I got more positive responses when giving the participants the option of writing up
their responses via email, either using the template provided or telling a narrative. The questionnaire was designed with the framework of analysis in mind.
Chapter 3
Magicians and Hackers: Applying the Frameworks

This chapter applies both my “Matrix for Characterizing the Primary Exploit” and “Chronological Conception and Execution of a Magic trick or Cybersecurity Exploit” to first-hand interviews and primary sources from both magicians and hackers. Throughout this chapter, I will be discussing the terms from the framework in relation to direct quotes from my sources and analyzing how the framework applies or doesn’t apply to each quote. This chapter will be organized by the designations defined in Table 1, provided again below.

Table 1: Matrix for Characterizing the Primary Exploit with Subject

<table>
<thead>
<tr>
<th></th>
<th>HUMAN</th>
<th>TECHNOLOGY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trick</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Herb Lin</td>
<td>3. Alex Stone</td>
<td></td>
</tr>
<tr>
<td>2. Teller</td>
<td>Tricks in which the primary exploit is based on a human vulnerability</td>
<td></td>
</tr>
<tr>
<td>Tricks in which the primary exploit is based on a human vulnerability</td>
<td>Tricks in which the primary exploit is based on a technological vulnerability</td>
<td></td>
</tr>
<tr>
<td><strong>Hack</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Herb Lin</td>
<td>8. Gustavus Simmons</td>
<td></td>
</tr>
<tr>
<td>Hacks in which the primary exploit is based on a human vulnerability</td>
<td>Hacks in which the primary exploit is based on a technological vulnerability</td>
<td></td>
</tr>
</tbody>
</table>

1. Human Exploit Tricks

Herb Lin

For the purposes of this project, I interviewed Professor Herb Lin on a magic trick that I have seen him perform multiple times. Professor Lin performs this trick at the beginning of many of his lectures to demonstrate “the power of false assumptions” (Lin, 2018). The trick involves
starting a presentation with a working lapel microphone and a turned off hand-held microphone. When Professor Lin begins this trick, he pretends to use the hand-held microphone and then dramatically reveals that he does not need it to project his voice through the speakers.

Professor Lin says that the initial conception of this trick involved “identifying [false assumptions] and taking advantage of them” (Lin, 2018). In this case, the false assumption is that since he is holding the hand-help microphone that must be the method by which his voice is being projected through the speakers. He emphasizes that for these false assumptions to be successfully exploited, they must be “perfectly natural assumptions” (Lin, 2018). These “perfectly natural assumptions” can be exploited in both magic and cybersecurity as Professor Lin’s interview will appear again in the next section.

**Teller**

On June 30th, 2017, the magician known as Teller, or the silent half of Penn and Teller appeared on NPR’s This American Life. In this piece, Teller discusses the multiple year long process of adapting a century old magic trick into a modern piece to be included in the Penn & Teller stage show in Las Vegas. The magician who designed this trick was named David P. Abbot and throughout his life “Houdini, Thurston, Keller, all the big names of magic would come to this guy's little house in Omaha, Nebraska to see [his] great shows” (Glass, 2018).

Teller obtained a copy of Abbot’s book and found a fantastical trick in which was “this golden ball, 6 inches across like a small cannonball, [which would] float around [Abbot’s] living room [and] was supposed to be one of the most beautiful routines in magic” (Glass, 2018). After perfecting Abbot’s version of the trick, Teller struggled to adapt the trick for his own show, until he had an accidental realization of how the trick could be changed.
[Teller] put the ball on a bench and lifted one end of the bench and then made the ball roll up the bench. And then later, he had this thought that the floating ball was actually more interesting to watch when it's not floating, when it's just this ball that's somehow alive and rolling around. It's weirder and it's more mysterious. It's less clear what's propelling it. (Glass, 2018)

Here, Teller has observed a human vulnerability, in which the non-floating ball subverts the audiences’ expectations and makes the trick “weirder” and “more mysterious.” There are multiple ways in which we are vulnerable to human deception, such as observational limitations, physical expectations and even emotional expectations. Here, Teller is exploiting the audience’s preconceptions of the physical expectations of the object. The ball does not obey the normal laws of physics as the audience would expect, therefore making the trick “weirder.” Teller says that this idea had never been conducted by any other magician, claiming that “no one had ever done a floating ball that didn't float” (Glass, 2018). After discovering this Human Vulnerability, Teller had to work out the technical moves:

The next step was to put something together into a routine, like an actual trick as it might be performed. This involved a tremendous amount of invention, making up all kinds of new moves on his own for the floating ball that does not float. (Glass, 2018)

The Ideation process for this trick involved a “tremendous amount of invention,” since many of the moves executed by Abbott in his original trick were not applicable to Teller’s new take on the trick. Teller practiced these moves and continued inventing new ones before showing the new trick to his performance partner, Penn Gillette. Teller says that he kept the performance hidden from Penn because “you can't look at a half-finished piece of magic and know whether it's good or not. It has to be perfect before you can evaluate whether it's good” (Glass, 2018).

Once Teller had perfected the “juggling” of the trick, “the mechanics of moving the ball around” (Glass, 2018), he moved onto the Dry-run phase in which he presented the trick to Penn. Penn strongly disliked the trick and said that it in fact made him “really, really, really wicked
uncomfortable” (Glass, 2018). Due to this unsuccessful dry run, Teller had to return to Ideation and find other ways to present the trick.

Upon the suggestion of magician James Thompson, Teller decided to “treat the ball like a trained dog” (Glass, 2018). In this new version of the trick “the plot of this is the dog trainer is getting the dog to jump through a hoop,” (Glass, 2018) rather unsuccessfully. This “plot” gives the audience something to follow and relate to, but Penn still strongly disliked the act. The final piece of this trick that Teller added stemmed from his belief that one you should “put yourself in the position of the audience at every moment...[and] try to manipulate” what the audience would be thinking. Interestingly, two magicians viewing the trick were incredibly impressed because they knew that there was a piece of thread, but still had no idea how the trick was being executed. Teller realized that these magicians were reacting better than “an audience that could imagine that this was being done with a little gyroscope inside the ball” (Glass, 2018). In the final version of the trick Penn reveals that the trick is done with a single piece of thread so that the “audience [can’t] see the thread, but they know it's there somewhere” (Glass, 2018).

2. Human Exploit Hacks

Herb Lin

During my interview with him, Professor Lin provided insight into a hacking methodology directly connected to the “perfectly natural assumptions” discussed in the previous section of this chapter. The methodology that Professor Lin discussed was on the nature of email fishing. He asked me to imagine that he received and email from SamSagan@gmail.com or a similar fictitious email: “how do I know it’s really you” (Lin, 2018). Emails like this are a perfect way of exploiting the “perfectly natural assumptions” that an email being received is
really from who it says. Professor Lin says since “I work in this business, I would NOT make that assumption” (Lin, 2018)

However, Professor Lin told me about a service called PhishMe, in which a company emails you, attempting to get you to fall for fictitious scams, with the goal of training its users to spot real scams. (PhishMe, 2018) Professor Lin told me that through using this service “I have learned from them, I know now” how to spot the signals. Initially, however, Professor Lin opened a “cybernews or something similar that essentially looked like something that I would subscribe to” (Lin, 2018). Even such an innocent “spooooky Halloween” email, displayed above could be a fishing scam. Both Professor Lin’s magic trick and his discussion of PhishMe, demonstrate the intrinsic values of “false assumptions” to both magic and cybersecurity exploit designers.

**Datajunkie**

The passage below was written for me by Aiden Riley “Caezar” Eller, former CTO of Unium, a Wi-Fi Router technology startup (recently acquired by Nokia) when prompted with the question “What is your favorite trick/hack or the one you admire most and why?” For context CTF is a computerized hacking competition at Def Con, modeled after the children’s game Capture the Flag and GH is the team that Caezar competes with, the Ghetto Hackers.

Datajunkie wore a short skirt and played exceptionally stupid during one year's contest, going from table to table asking young male players whether she could use their laptop for a second to check a file on her thumb drive, a drive that was loaded with malware designed to create CTF files, malware that scored more points total than all of the other hacks that GH ever accomplished; her move was so simple and so powerful that we scored on something like 40% of all of the *players* that year. Defenders were almost
relegated to a hilarious note in history by comparison to the widespread harm done by the chauvinist attitudes of young hackers at the turn of the millennium. (Eller, 2018)

This exceedingly creative tactic stemmed from a human vulnerability, specifically the “chauvinist attitudes of young hackers at the turn of the millennium.” The hacker known as datajunkie observed that she could easily exploit these young (presumably male) CTF players because of their attitudes toward her as a female hacker. The short skirt served as a piece of misdirection, however pretending to be “exceptionally stupid” during the competition served a much more subversive purpose. By playing “exceptionally stupid,” datajunkie was able to reinforce the negative stereotypes of female hackers projected onto her by the victims. After reinforcing these stereotypes and getting her victims to trust her, she was able to execute a hack that allowed her to score “40% of all of the *players* that year” (Eller, 2018)

This was not the only hack that Caezar told me about. Another hack, executed by the Ghetto Hackers during their CTF games at Def Con over the years, was a literal example of a “Trojan horse,” and is discussed in the next section.

3. Technological Exploit Tricks

**Alex Stone**

As a secondary source for this project, I have selected Alex Stone’s book *Fooling Houdini*. The book follows the story of Alex Stone designing a new trick for a competition known as “The Magic Olympics.” Stone’s design process is well-documented in this book and provides an intriguing insight into the mind of a magicians. It is also important to note that Stone attended Harvard and has a Master’s Degree in Physics from Columbia. Throughout the book, he mentions his physics degree and how it helps him think differently than other magicians.
Initial Conception

Stone journey in designing this trick takes him to research the work of Perci Diaconis, professor of Statistics and Mathematics at Stanford University, and famed Math Magician. Stone tells us about a card trick that could be accomplished remotely via telephone and mail, allowing the spectator to shuffle the pack. This “trick caught [Perci Diaconis’s] eye because it suggested something counterintuitive about shuffling, namely that shuffling doesn’t work as well as people think it does” (Stone, 252). This is not discussing Stone’s original trick, but instead is discussing the initial conception of Perci Diaconis’s research project attempting to discover how many times a pack must be shuffled to be truly mixed. I would like to note how well Diaconis’s “initial conception” fits the framework of analysis, specifically as a Human Vulnerability Magician. Diaconis’s study concluded that a shuffling a deck 7 times resulted in a pack in which “every arrangement of the 52 cards is equally likely or that any card is as likely to be in one place as in another” (Kolata, 1990). Stone’s analysis of what initially caught Diaconis’s eye is incredibly interesting because Diaconis’s initial observation is a human one. Diaconis’s initial observation was not that a supposedly shuffled deck is not truly random, but instead that a human’s perception of how many shuffles it takes to have a truly random deck is flawed.

Stone’s new trick ends up being based off a trick designed by Perci Diaconis. “The secret [behind Diaconis’s trick], it turned out, was rooted in an obscure mathematical principle known as the De Brujin sequence” (Stone, 270). Here, Stone observed an obscure technological tool that he could utilize in his own trick. This is a case where the technological tool is physical piece of technology, but instead a mathematical principle. Treating this mathematical principle as a piece of technology to exploit for a magic trick is one factor that made Stone’s and Diaconis’s trick so effective. Stone’s objective in designing this trick was to fool not only audience members, but a
panel of world renowned magicians. Magicians generally have extensive knowledge about the technology that can be used to “gimmick” or set up a deck and would not be fooled by a trick that used a gimmicked pack of cards. Since the technological tool is an obscure mathematical principle used to organize the deck, magicians, who don’t necessarily have a strong background in mathematics, would be much less likely to be able to discover the secret behind this trick. Bell and Whaley claim that “few, if any magicians, however, deceive themselves that these new innovations do anything more that refresh a tired repertoire of effects” (Bell and Whaley, 1991, 142). However, this trick is a clear counter example to this claim, in that Stone and Diaconis were able to take an unknown mathematical principle and incorporate it in to an entirely new trick.

**Practice**

Throughout this book, Stone reflects on the multiple ways that he practices his tricks. Stone tells the reader, “To further my sense of touch, I blindfolded myself during practice sessions. Studies have found that visual deprivation causes almost immediate changes in the brain” (Stone, 94). This particular practice method caught my eye because it deals with perception in an interesting way. By depriving his own perception, Stone can better understand how to deceive an audience without having to deal with his own perception.

Penn and Teller liken the process of becoming stage ready to getting a pilot’s license. Before pilots get their wings, they have to log a certain amount of supervised flight time. There is no way around this. You simply have to log the hours. I logged hours every chance I got. I invited people to a party and made them watch my act. I high jacked other people’s parties and turned their guests into my Guinea pigs. (Stone, 284)

Here, Stone reflects on the importance of **practice**, especially when dealing with an original “act” like the one he was designing in this book. Penn and Teller’s analogy serves to remind the
reader that **practice** is a fully necessary element in the creative design of a magic trick. This quote also highlights the importance of **dry runs**.

### 4. Technological Exploit Hacks

**Aiden Riley “Caezar” Eller**

In his email to me, Eller discussed the rules and regulation behind the game of Capture the Flag played at def con every year, before he and his team “took over the contest and designed something a bit less vulnerable to hackers” (Eller, 2018). This particular hack took place during the Ghetto Hacker’s “third year playing and was to become our second year winning” (Eller, 2018). Eller claims that his team wanted “very much to avoid the work required to win the contest” (Eller, 2018).

#### Initial Conception

The vulnerability that Eller and the Ghetto Hackers decided to exploit was in “security area called a network operations center (NOC); a network for attaching the players to the defenders and permitting some amount of digital communication” (Eller, 2018). They saw a technological vulnerability in the system of rules created by the organizers. Specifically, that since adding another server to the NOC “literally [scored] zero points... the designers did not consider the security ramifications” (Eller, 2018). The primary exploit here is in the fundamental design of the technical specifications of this competition.

#### Ideation

Here the Ghetto Hackers used what Eller describes as “oldest trick in the book: the Trojan Horse” (Eller, 2018). By exploiting the fact that the NOC allowed new servers to be added, the Ghetto Hackers were able to use a “physically very large server chassis” (Eller, 2018) to sneak one of their team members into the NOC.
Misdirection and Disguising

The team member selected to be inside their fake chassis was Brazen Angel, who was able to fit in the chassis with “a laptop perched on her knees” (Eller, 2018). The team was also concerned that NOC security would try to verify the functionality of their fake chassis. To trick the NOC security, they “loaded [Brazen Angel’s] laptop with a believable software image, and wired the ports to those of the chassis, so that the machine might appear to be quite functional should anyone check” (Eller, 2018).

Execution

During any hack or magic trick there is always the possibility of unintended or unexpected obstacles during the execution. In this case, the Ghetto Hackers “did not account for a security guard posted outside the NOC” (Eller, 2018). Their initial plan was to “was to roll the server toward that space just a few minutes before the expected NOC closing time, around 6pm” (Eller, 2018), allowing Brazen Angel to leave through the front door after the NOC staff had left. However, the security guard was stationed outside the door past 6pm. After Brazen Angel had gotten out of the server chassis, she implanted Ghetto Hacker “flags on all the machines” in the NOC. Here the Ghetto Hackers had to improvise and coordinate via text to execute “what ended up being a critical moment” in which two members of the Ghetto hackers “stood and distracted the guard while [Brazen Angel] delicately opened the NOC door from within, let it close, and walked quickly away” (Eller, 2018). While this exploit was primarily a technological one, this particular moment is an expertly exploited human vulnerability by the Ghetto hackers.

James Harvey

In his 2016 article, How a Group of MIT Students Gamed the Massachusetts State Lottery, Adam Kucharski tells the story of James Harvey, an MIT student who discovered a
method to beat the Massachusetts state lottery. The technical vulnerability exploited by Harvey was within the rules of a particular lottery game called Cash Winfall.

**Initial Conception**

The unique reason that Cash Winfall could be exploited was that unlike most lottery games, the prize did not “roll over” to the next game if no participant got every single number correct. The issue with “roll over” lotteries is that there are not constant winners and “if no smiling faces and giant checks appear in the newspapers for a while, people might stop playing” (Kucharski, 2016). In an attempt to alleviate this issue, Cash Winfall “[limited] the jackpot: If the prize money rose to $2 million without a winner, the jackpot would “roll-down” and instead be split among the players who had matched three, four, or five numbers” (Kucharski, 2016). Due to this “roll-down” system, Harvey realized that when the “roll-down happened, there was at least $2.30 waiting in prize money for every $2.00 ticket sold” (Kucharski, 2016).

**Ideation**

In 2005, to discover exactly how to game this Cash Winfall, Harvey went to “the town of Braintree, where the lottery offices were based... to get hold of a copy of the guidelines for the game, which would outline precisely how the prize money was distributed” (Kucharski, 2016). However, it wasn't until 2008 that “the lottery finally sent him the guidelines” (Kucharski, 2016). Harvey and his “group found that if the jackpot failed to top $1.6 million, the estimate for the next prize was almost always below the crucial value of $2 million” (Kucharski, 2016). This meant that if they could push the jackpot to $2 million themselves, they would be incredibly likely to win money.

**Misdirection and Disguising:**
This case is particularly interesting because the victims actually knew about the vulnerability. According to Kucharski, the lottery designers knew that a single person or group could buy tickets in bulk to tip the balance of the game by prematurely reaching the “crucial value of $2 million” (Kucharski, 2016).

They calculated that a player who used stores’ automated lottery machines, which churned out tickets with arbitrary numbers, would be able to place 100 bets per minute. If the jackpot stood at less than $1.7 million, the player would need to buy over 500,000 tickets to push it above the $2 million limit. Because this would take well over 80 hours, the lottery didn’t think anyone would be able to tip the total over $2 million unless the jackpot was already above $1.7 million. (Kucharski, 2016).

The Cash Winfall designers did not believe that anyone would invest the “80 hours” to exploit this vulnerability.

**Practice**

According to Kucharski, Harvey claims that this particular exploit “took us about a year to ramp up to it” (Kucharski, 2016). While the article does not say what this year of preparation entailed, one could assume that the MIT students spent the time meticulously planning and running mathematical models to maximize their chances of profit when the time came.

**Execution:**

To execute this exploit, Harvey and his compatriots “had to fill out around 700,000 betting slips, all by hand” (Kucharski, 2016). By submitting these hand-filled slips, Harvey and his compatriots had triggered “a huge increase in ticket sales, enough to drive the total prize money past $2 million. This flood of sales triggered a premature roll-down” (Kucharski, 2016). According to Kucharski, this exploit was fully successful and the team made over $700,000 playing this game. Since playing the lottery in this way “betting syndicates [like Harvey’s] have
managed to repeatedly—and legally—turn a profit” (Kucharski, 2016). Much like counting cards, this practice is not distinctly illegal and therefore difficult to thwart.

**Gustavus Simmons**

For the purposes of this project, Gustavus Simmons, retired cryptographer and senior fellow at Sandia National Laboratory, provided me with a story regarding his work “developing technical means to verify compliance with various arms control and arms reduction treaties” during his time at Sandia National Laboratories. For this compliance project, Simmons falls into the category of a Technological Vulnerability Hacker. The interview received by Simmons did not contain enough information to fully fill out the Framework of Analysis. However, I have sorted excerpts from his interview into Initial Conception, Ideation and Execution about which he provided in-depth discussion.

**Initial Conception**

“That technology would have to protect the integrity of the devices the United States planned to deploy in Russia to gather, store and transmit the information on which treaty verification depended…We knew how good the physical sensing and penalty invoking technology was” (Simmons, 2018).

As we can see from the quote above, Gus Simmons believed that the inception of this project was a technological one. Simmons believes that the current understanding of power behind existing “physical sensing and penalty invoking technology,” (Simmons, 2018) was what motivated him and his compatriots to pursue this project.

**Ideation**

We had hired the Stanford Research Institute (SRI), the Illinois Institute of Technology Research Institute (IITRI) and Braddock, Dunn and MacDonald (BDM) in no holds barred contracts and essentially open funding so long as progress was being made to try and defeat the protective technology. (Simmons, 2018)
Interestingly, Simmons and his team at Sandia National Laboratories acknowledged that they could successfully execute this project themselves. In order to accomplish this daunting task, they decided to give “essentially open funding” to multiple research institutions to try to make progress on a specific issue with their verification technology. This sort of collaboration is particularly intriguing because Sandia found it necessary to partner with and provide funding for three different research institutions.

**Execution**

Even though Simmons and his team were executing this project out of from a technological initial conception, they decided that they could not adequately protect against a “human opponent whose objective is to deceive you” since “there are no limits on how he can try to do this” (Simmons, 2018). The particular problem that the team was worried about was humans attempting to alter or mimic secure data packages. According to Simmons, this form of packet deceit had “been successful attack modes against the nuclear weapons protective packages in the early rounds of testing and redesign” (Simmons, 2018). Simmons claims that “[Russians] might not have attempted such a deceit, but it was critical to be prepared,” (Simmons, 2018) for this type of attack. To address this problem, the team at Sandia National Laboratory brought in famed magician James Randi. To alleviate this concern regarding packet switching Randi was tasked with “[coaching] the US observers to be aware of distractions that might allow the Russians to swap packages etc.” (Simmons, 2018).

**5. Analysis**

Each of these narratives provided through first-hand interviews and primary sources, shows how both hackers and magicians utilize similar mythologies and ideas when designing
their exploits. While the Framework of Analysis provided an interesting insight into these narratives, generally the narratives would not fall into the framework well. Of course, every trick and exploit design process had Ideation and Practice, but they didn’t always require a Dry-Run or a Follow-Through. The design process in general is very fluid and can be conducted in many different manners.

However, the distinction between Human Vulnerabilities and Technological Vulnerabilities in the Initial Conception seemed to be the strongest corollary between the methodologies of magicians and hackers. Through the examples of Teller and datajunkie, we can see magicians and hackers have observed similar vulnerabilities in human perception. While the execution of Teller’s trick and datajunkie’s hack were drastically different in both practice and intent, their initial conceptions each preyed on specific vulnerabilities they noticed in their target population. The target population in Teller’s trick was his partner, Penn Gillete, and the general magic-going audience, while datajunkie’s target population was the hoards misogynistic young coders at Def Con. Even though these two exploits had vastly different intents and target populations, the correlation between their initial conceptions still stands.

There is also this same correlation between technological initial conceptions of magicians and hackers. The example of Alex Stone’s trick provides proof that, while the initial conception of a magic trick is generally believed to be exploited a human vulnerability, it is possible for a magic trick to technological exploit. Furthermore, the Eller and Cash Winfall cases are two examples of how hackers recognized a technical vulnerability in the rules governing the scoring system of a competition and the rule set of a lottery.
Chapter 4
Conclusion

The most successful part of the Framework of Analysis and a primary takeaway of this thesis was the distinction between Human Vulnerabilities and Technological Vulnerabilities in the Initial Conception. As discussed in the introduction, Whaley’s discussion of “David Devant’s motto—Give me a good "effect" and I'll find a way to do it” (Whaley, 1982, 190)—is particularly pertinent to my discussion of the Initial Conception. Here, the “effect” could be defined as the vulnerability to exploit and what the subsequent impact of that exploitation on the audience member or victim of a hack. When Devant says “I’ll find a way to do it,” he is referring to the lengthy ideation and practice periods necessary to effectively exploit a vulnerability. Ghustav Kuhn and his co-authors detail the tools with which magicians can exploit vulnerabilities: “the ability to control attention, to distort perception, and to influence choice” (Kuhn et al., 2008). However, these tools effectively fall into the later categories of my Framework of Analysis, such as ideation or even execution. The Initial Conception supersedes these tools. The tools described by Kuhn et al. are “a way to do it,” while the initial conception exists as the “effect” and stems from an observation of a vulnerability.

Through my research, I discovered that there are two types of vulnerabilities that magician and hackers typically base their exploits off of. This is not to say that some tricks and hacks could not exploit multiple vulnerabilities concurrently. However, the Initial Conception, the spark that makes someone want to pursue a magic trick or a cybersecurity hack, typically stems from either an observed Human Vulnerability or an observed Technological Vulnerability.

As I have already noted, Bell and Whaley claim that “few, if any magicians, however, deceive themselves that these new innovations do anything more that refresh a tired repertoire of
effects” (Bell and Whaley, 1991, 142). Innovation and new technology “add nothing to the ancient psychological principles of deception and cheating” (Bell and Whaley, 1991, 142). According to John McLaughlin, the ex-CIA Director and amateur magician, magic is “about psychology,” because “the hand is not quicker than the eye” (Rienzi, 2014). The “psychology” that McLaughlin is referring to is directly comparable to Bell and Whaley’s “ancient psychological principles of deception and cheating” (Bell and Whaley, 1991, 142).

However, Bell, Whaley, and McLaughlin underplay the impact that technology can have on innovation and new ideas. In his 1980 article, “Do Artifacts Have Politics,” Langdon Winner argues that since “technological systems of various kinds are deeply interwoven into the conditions of modern politics,” technology has “fundamentally changed exercise of power and the experience of citizenship” (Winner, 1980, 122). Since technology is so engrained into the modern “experience of citizenship,” I would argue that new technology can absolutely create or reveal new vulnerabilities that influence the “ancient psychological principles of deception and cheating” (Bell and Whaley, 1991, 142). Winner criticizes observers who discover “evil in aggregates of steel, plastic, transistors, integrated circuits and chemicals” and believes that it is foolish to “blame the hardware” (Winner, 1980, 122) for social failures in modern society.

This thesis similarly shows that it may be foolish to blame the software or hardware, when hackers exploit less obvious human or technological vulnerabilities. Cybersecurity specialists can see the vulnerabilities in both technological systems and human perception. These specialists are not individuals with extrasensory abilities. Rather they are, like the performing magicians also studied in this thesis, individuals who have keen insights into human and technological system vulnerabilities.
This thesis demonstrates that magicians and cyber-hackers are acutely aware that technological vulnerabilities exist and are different from the human vulnerabilities that traditional magicians focus upon. As evident by the participants and primary sources in the second column of Table 1: Matrix for Characterizing the Primary Exploit on page 30, magicians and hackers are often acutely in tune with contemporary technological advancements, and are very adept at incorporating new technological vulnerabilities into their exploits. During my interview with Herb Lin for this thesis, as well as my previous project with him, it became clear that Professor Lin as a cybersecurity expert is well versed in magician methodologies and is not at all hesitant to bring that knowledge into the world of cybersecurity. In the Eller case and the Cash Winfall case, the technological vulnerability was in a set of rules, which is not immediately apparent as a potential exploit. Furthermore, Alex Stone’s observed technological vulnerability was not anything obvious or tangible, but was in fact an obscure mathematical principle. Thus, Eller and the Cash Winfall hackers (in cybersecurity) and Stone (in magic) observed a technical vulnerability to be exploited. Essentially, they understood the technological design of the system and thus were able to design an exploit that utilized that vulnerability.

A major limitation of this thesis is that I have only studied the design behind a limited number of hackers and therefore cannot tell how often the kinds of similarities I discovered between magicians and hackers exist. While I leave that research to others to do in the future, I do believe it would be valuable not only to continue to explore these similarities, but to expand the scope of such research into other domains.

Whaley discusses that his ideas could be applied to “diplomats, counter-espionage officers, politicians, businessmen, con artists, charlatans, hoaxers, practical jokers, poker players, gambling cheats, football quarterbacks, fencers, actors, artists, mystery story writers, or you or I...
in our everyday lives” (Whaley, 1982). Similarly, my theories on Initial Conception and further ideation developed in this thesis could be applied to not only to demonstrate the similarities in design processes between not only magicians and hackers, but more broadly in any field that involves deception at some level. Whaley ended his seminal 1982 essay with a call for magicians to be more involved in national security and the intelligence community: “Here too a study of magic can be helpful because magicians – master deceivers themselves—have proven themselves the best detectives of the deceptions of three of the main types of deceivers: psychic frauds, gambling cheats, and other magicians” (Whaley, 1982, 190). This thesis has shown not only that hackers often have a background in magic, but that studying magic design can help identify the design tricks of cyberhackers.

This thesis serves as a preliminary work (with few representatives in each instance) in a potential new field, studying the methods of magicians as applied to cybersecurity and other security fields. This leads to a call for further research studies that bring the methodologies of magicians into the current discourse surrounding fields of security. As this thesis addresses how those working in cybersecurity might learn from the methodologies of magicians, other scholars could bring these ideas into multiple security and defense contexts. Bell and Whaley suggest that technology and innovation only has the capacity to “refresh a tired repertoire of effects” (Bell and Whaley, 1991, 142). This thesis intended to demonstrate that new technologies do not “add nothing to the ancient psychological principles of deception and cheating” (Bell and Whaley, 1991, 142). In fact, new technologies across all fields are integral to the initial conception and ultimate execution of drastically innovative exploits in the both cybersecurity and magic.

Ultimately, thesis aims to contribute to the demystification of the fields of cybersecurity and magic. Magicians and hackers are not wizards with super-human abilities. They are
intelligent and persistent individuals, who have an uncanny ability to recognize both human and technological vulnerabilities and then turn that recognition into dramatic and powerful exploits.
Works Cited


Eller, Riley Aiden. Email Interview, 18, Mar. 2018.


Simmons, Gustavus. Email Interview, 1, Feb. 2018.


Appendix A
Email Used to Contact Participants

Dear [NAME],

As a senior in Stanford’s Science, Technology and Society Honors Program, I am conducting a research project I’ve entitled “Cybersecurity Magic: Demystifying Hacking by Identifying Vulnerabilities to Deception and Misdirection.”

In this project, I am interviewing a number of hackers, cybersecurity professionals and magicians with the goal of discovering how both cybersecurity professionals and magicians identify and utilize human vulnerabilities and technological opportunities. Due to your work in [PERSONALIZE], I think your participation in this study would greatly assist me in contributing, in however a modest way, to our understanding of cybersecurity and its challenges by drawing on the parallels between hacking and magic.

There are three options for participating in this study, one of which I hope will suit you:

1. In-person/phone/video interview of 15-20 minutes.
2. Provide a written account of a hack or magic trick in as much detail as you wish.
3. Fill out the six-question survey attached to this email.

Please let me know whether or not you are willing to participate through one of these options, and if so, please read and sign the informed consent letter attached to this email.

Thank you for considering this request.

Sincerely,
Samuel Sagan

Cybersecurity Magic Survey

1. For either a hack or a trick that you designed or that you have come to know intimately, please provide a brief description (including a name for it if there is one).

2. What initially led you to pursue this hack or trick?

3. Did it involve exploiting a vulnerability or a technology, and if so, how does the hack or trick take advantage of it?

4. How has the execution of the hack/trick in the real world differed from practice and/or dry runs of the hack/trick?

5. What steps are taken after the execution of the hack/trick to “cover your tracks”?

Samuel K. Sagan
6. Are there other aspects about the origins or execution of the hack/trick that you would like to comment on, perhaps in comparison to other hack/trick?