Physical Security: Movie vs. reality

– Ocean's 11 –

Cristopher Dahlström
Email: crida498@student.liu.se
Supervisor: Juha Takkinen, juha.takkinen@liu.se
Project Report for Information Security Course
University of Linköping, Sweden

Abstract

This report contains descriptions and analyses of the security solutions found in "Ocean's eleven". Three scenes in which perpetrators try to attack a system are being described; the different attacks as well as the security solutions. A discussion of how the system can be learned is included in the analysis. From this two conclusions have been made. The first is that the security systems described in the movie are realistic, but impractical, while the attacks are unlikely due to made-up technology. The second conclusion is that a layered defence that requires different kinds of attacks in sequence is harder to penetrate than a system of low complexity, and also that small details are often enough to plug a lot of holes in a security system.

1. Introduction

What is a movie? At a first thought most might say "90 minutes of entertainment", but they would soon start to remember all things learned from movies, be it about war and weapons, sports and events, drugs and crime, or far away countries with their customs. We all know that the truths that are shown in movies are not always truths in the real world; yet the truth in the movies needs to have some grain of real truth in it, and more importantly, the "Hollywood Science" needs to be consistent. In more classical words one could say that movies are nothing but "if"-scenarios.

If we use "Star Trek" as an example; the series are built on one big if; "What if Zefram Cochrane managed to create a warp-drive in 2073?" This "if" would be interesting if one wanted to explore the possibilities space-travel might bring; the series might not hold that many truths in the world we know today, but "what if" it turned out that we could make a warp-drive, then the series might be used as inspiration to learn more of the possibilities that exists. In other words: "If 'if' is true, then what is based on the 'if' is likely to contain truth." Admittedly, Star Trek is based on a fairly big "if".

If we instead look at a movie that is closer to the reality, where the "what if" is much smaller, we would soon realize that we could learn a lot from it. In "Ocean's 11" the "if" contains a protected vault, and a group that wants to break into the vault.

This report uses the movie "Ocean's 11" as inspiration. The defences and the attacks in the movie have been analysed, and conclusions about whether they are possible or not in the real world have been made. The analyses have then been used to gain some insights in the nature of physical security in the real world. The goal is not to gain insights in the movie, but to gain insights in, and draw conclusions about, about physical security in the real world.

1.1 Defining the task

The given task is to "Select a movie or a TV series of your own choice, e.g. "24" or "Hackers", and analyse it with regard to physical security in theory and practice versus "the movies"".

1.1.1 Breaking down the task

The task can be broken down into three major questions:

- *Which movie/scenes should be chosen?* The selected scenes has to attempt to picture a real, or at least plausible, scenario, it has to be creative enough to not be too obvious and it needs to be detailed enough to provide a solid ground for analysis.

- *What security solutions and attacks are presented in the selected scenes?* In other words, how did the solution and the attack work, how was it constructed, and could the solution be improved so that the attack would have been prevented?
- *What can be learned from the analyses?* Would the solutions and the attacks work in the "real world", and what can be learned from looking at the solutions and attacks presented in the movie?

1.1.2 Expected results

The expected outcome of this report is a discussion about several security measures and an analyse of the layered defence shown in the movie, and whether any wisdoms can be learned from what was done, and what was not done in the movie.

1.1.3 Specify limitations

A maximum of three scenes or security-solutions will be analysed. This paper will only briefly approach the subjects of network and IT security. Subjects such as advanced technology will also be avoided; the emphasis should be on the attacks and the ways to counter them.

1.2 Method

In order to assess the physical security in a movie, a movie has to be chosen. The first step is therefore to assess a number of movies and try to evaluate which of them is the most appropriate when it comes to reality/plausibility, creativity and detail.

Once that is done literature-studies of the given course materials will be on the agenda, and the theory-section will be constructed from this. Once this is done the theoretical framework will be assessed, and if it is deemed to be lacking in any areas further studies will be required.

Parallel with the literature studies the scenes from the movie are to be studied and described carefully. The focus of this study will be to describe the protective systems and how they are being defeated, rather than have focus on the involved characters or the plot.

Once the theoretical framework and the descriptions of the security solutions are complete, the two will be combined into an analytical framework that, in the conclusion, answers the questions found in "Assessing the task".

1.2.1 Sources

A number of different sources have been used for this, a few of them of questionable value in a report. it is therefore important to carefully examine what information is used for what purpose. The movies are used mainly as sources for ideas, and since one of the goals is to compare the reality of the movies with the real realities, the inaccuracies or falsities will not have a negative impact on the outcome of the report. IMDB and AMC filmcritic.com are only used to a lesser extent to supply background information, and the reliability of those sources are therefore of lesser importance. The information fetched from the rest of the internet sources is of a nature that falsities would not affect the major outcome of the report. The applications for cameras in "Warning Strange behaviour" are commonly known, as is the outcome of the Milligram experiment. Wikipedia is used as a source, but only for information that vaguely helps to enforce the intuitive fact that the charges used appears to be too small for their purpose.

The remaining literature can be considered as reasonably reliable, partly because the information given appears to be intuitively correct; the same can be said for the information from the lecturer.

1.3 Structure

The rest of the report is structured as follows:

2. Background
3. Theory
4. Chosen scenes: Description and analyses
5. Discussion
6. Conclusions

2. Background

The chosen movie is "Ocean's eleven". This section will explain why the said movie have been chosen, and give some information on some of the alternatives.

2.1 Plot and description

Ocean's Eleven is Steven Söderberg's remake of "Ocean's 11" from 1960, starring Frank Sinatra, Dean Martin and Sammy Davis Jr. (International Movie Database, 2011)

Ocean (George Clooney) who has just been released from prison starts to plan the biggest heist in Las Vegas history together with Dusty Ryan (Brad Pitt). Together with 9 other criminals, all experts in their own fields, they intend to empty the vaults of Bellagio (Andy Garcia), the questionable owner of three casinos, of $150 million. (Ocean's 11, 2001)

The experts consists of one "techie", one "shadow", one munitions expert, one inside man, two mechanics, one seasoned veteran and one Chinese gymnast. (AMC Filmcritic.com, 2011)

2.2 Motivate the choice

The three main criteria used for choosing a movie are plausibility, creativity and detail. "Oceans 11" fulfils all three of them, namely, plausibility/reality, creativity and level of detail. Even if a more recent movie is preferred over an older one, most movies falls short when they fail to meet the set criteria. A summary of the assessed movies follows.

2.2.1 Die Hard 4

The storyline describes how a group, led by an expert hacker, mounts an attack on North America, taking out important functions for the infrastructure, such as electricity, cell phone and internet connectivity, banks and finance with the intent of extorting the government. While the scenario seems reasonably plausible, and it is certainly creative enough, the level of detail is very low. You get very few explanations of how or why they do certain things, and the audience is left in the dark to how the security solutions that are defeated are constructed. (Die Hard 4, 2007)

2.2.2 Mission Impossible 3

The movie begins with a rescue mission, in which force7 is used to free a person. The on-going theme in the movie is to either get people in, or out from buildings with varying levels of security. A lot of extreme technology is used, and to the characters in the movie it is trivial to imitate persons (voice change-technology and perfect rubber-masks). The technology being used might perhaps be plausible, but because of the excess of it, it has to be considered as pure sci-fi. Furthermore, the level of detail is greatly varying, but overall a very small insight in the different scenarios is being given. (Mission Impossible 3, 2006)

2.2.3 Ocean's eleven

All security-solutions in the movie appear, at a first glance, to be technically possible. Some implementations are poor at best, while other borders to insanity. As the value being protected is in the range of 150 million USD a certain amount of eccentricity can be accepted, and every system in the movie has been given some explanation (except for one the reason and purpose are obvious). (Ocean's 11, 2001)

Not only standard solutions are used in the movie; some are a bit eccentric, and others border to the ridiculous, but the layered the defence as a whole shows a certain amount of creativity that is not commonly seen in "normal" security solutions. (Ocean's 11, 2001)

Quite a lot of information is given about the different aspects of the layered defence, and even more can be learned from the ways the defences are circumvented or defeated. Information is lacking in some areas; for example how one of the attacks on their IT system is being launched, but overall the level of detail shows that the script of the movie is based upon at least some research. (Ocean's 11, 2001)

2.2.4 Ocean's 12 and Ocean's 13

While being more recent than Ocean's eleven, the level of detail is what sets these two movies apart from the first one in the series. The security systems are barely described at all, and they border on sci-fi with some of the technologies being used. Because of this, the first movie in the series is preferred, despite it being slightly older. (Ocean's 11, 2001)

3. Theory

In this section the theoretical framework for the analyse and the conclusions can be found.

3.1 Concepts of data security

There are three main concepts of data security, namely availability, integrity and confidentiality. Availability means that it has to be able to access the data when there is need for it, integrity means that the data has been unmodified, in essence, only those allowed to change the data should be allowed to, and the third concept is confidentiality, meaning that only those authorized can access to read the data. A simple example is an online mail service; availability means that you can log in from anywhere you want, integrity means that there is sufficient encryption to ensure that the data will not be modified, or simply use hash values to ensure that the data have not been manipulated. Finally, confidentiality implies that only you should be allowed to log into your account. (Matthews, 2004)

3.2 Layered defence

When planning a layered defence three principles are central; breadth, depth and deterrence. (Matthews, 2004)

Breadth can be considered as "plugging the holes in a wall", in other words, making sure that each layer in the defence is solid and "cannot" be penetrated. (Matthews, 2004)

Depth is to be viewed as having several walls. A realistic approach to physical security is that walls will

break down, and even if the principle of breadth has been taken under consideration, one cannot rely solely on one wall; one reason for this being if the base for the wall breaks down, e.g. a system that relies on electricity will fail if the electricity fails, one could argue that if breadth have been considered the system would have a backup electricity system, but that would only raise the question of, what if that fails as well, or if we attack the cords connecting the system to the power grid. Simply put, any given control can be defeated, and therefore a layered defence is required if one wants to secure something. (Matthews, 2004)

The third principle, deterrence, can be viewed as costs vs. benefits for those that defeat the system; one could argue that it should be viewed as "threat of costs vs. possible benefits". This principle deals with the psychological aspect of the defence, and it is very important to remember who the costs and benefits matters for. A company might value an asset in a certain way, but if stolen it would most likely be valued in a different way, and vice versa. Consider a $5000 server, which could be sold for $1000 on the street but contains information worth $50000 to the company. The psychology of the perpetrators needs to be taken into account; if the goal is to sell it, the threat of costs only has to be at least $1000 to deter him/her, but if the goal is to damage the company, the threat of costs would have to be $50000. Because of this it is important to consider who is likely to attack the system. (Matthews, 2004)

When designing a security system one must take each layers contribution to detection, deterrence or delay into account as well as the threats motivation and capabilities. This is commonly referred to as analytical risk management. (Matthews, 2004)

Five questions have to be answered before designing the layered defence.

- What is to be protected?
- What is the value to the owner?
- Who do we protect it from?
- What is the value to the attacker?
- What is the likelihood of an attack?

(Matthews, 2004)

3.3 Controls

When one constructs a layered defence, different controls can be put into place. All the controls aims to do one, or more, of the following: Deter, Detect, Delay and react. (Matthews, 2004)

The best is, of course, if the system never has to work, if possible perpetrators are reluctant to even attempt an attack, but since engaging in the mere discussion about physical security implies that physical security is needed to protect something, it is most likely needed to consider all controls.

3.3.1 Detect, Delay and React

Assume that the deterrence fails, someone, or some group have come to the conclusion that the possible benefit of defeating the system is greater than the threat of failure. Also include the notion that, given enough time and resources, any and all defences will fail. The first goal of the security system would therefore be to detect an attack and react before all layers of defence have been defeated. Assume a simple scenario, one locked office-door and one locked desk. An alarm chimes and notifies the local police, which arrives within 10 minutes. If the perpetrators are likely to open the locked desk and leave the perimeter within 10 minutes one could make the conclusion that another layer of defence would be required. The reaction has to be contemplated as well, if, for example, the possible perpetrators are school children, then it would be enough to have a janitor react when the alarm chimes, but if it is a high security vault containing millions of dollars, the janitor would not suffice.

One could, therefore, categorise different security components according to what they achieve in terms of deterrence, detection and delay. For example a locked door would delay, but if a tamper-alarm is added it might also detect, because of the connection between detection and deterrence one could argue it affects all variables. (Matthews, 2004)

3.3.2 Cameras for detection and assessment

It should be mentioned that cameras are not always a good tool for detection, this since they can be fooled in different ways, and the eyes watching the monitors might not always be observant, but when combined with an alarm they can be a great tool for assessing a situation. (Matthews, 2004)

The border between cameras as mere tools for assessment can however be questioned to some extent. The most common application is motion detection which can trigger an alarm should certain levels of movement be detected. Cameras also open the possibility of active surveillance systems, where certain patterns trigger reactions. The article "Warning! Strange behaviour." mentions that this system is already in use in some subways, and that it allows automatic detection of for example bags being left on the ground (possible

containers of bombs), or people prone to suicide. As certain movement patterns, identify groups of people or individuals can be identified with this system, it is implied cameras can, together with analytical software, be considered as tools for detection as well. And since this article describes a technical solution from 1999, one can make the conclusion that it have been improved quite a bit. (New Scientist, 1999)

3.3.3 Access control – User Authentication

First of all one has to examine the difference between authentication and identification. Boiled down to the extremes authentication says "I am <…>, this is how I prove it", while identification says "You are <…> because of…". The difference might seem insignificant at first, but the two systems needs to be implemented quite differently. A system for authentication requires the user to first claim an identity, and then prove that the claim is correct, in the normal case requiring the user to provide a login (claimed identity) and a password (verification). This normally requires one database search to see if your verification is correct or not. In the case of identification the user needs to be compared to the entire database to find out who he, she or it is. For authentication the identity can be claimed in many different ways; for example by stating a name, provide a login, or by owning a token. For example, if you perform a bank transaction at an ATM-machine you insert a card which is connected to an account, you then give verification to the cards-identity by entering a code. (Fåk, 2011)

A person can be identified/authenticated in three different ways:

- What the person knows – Passwords, pins
- What the person has – ID-cards, smart-cards, tokens
- What the person is/does – Biometrics

It is not uncommon to use multiple methods of identification/authentication, as mentioned above, using a smart-card and a code. One important question to ask is, what the system is for; for example, to have a card to open a door might seem like a good idea, but without the added security of a pin code (or some other authentication method), anyone who steals your card can open your door. (Fåk, 2011)

3.4 Vulnerability assessment process

John J. Fay suggests the following methodology for assessing a physical protection system (PPS) (Fay, 2007)

1. Locate all assets
2. Make a path analysis
3. Make a scenario analysis
4. If needed, make a neutralization analysis
5. Determine system effectiveness
6. Improve the system if the effectiveness is not acceptable

The scenario analysis includes the nature of the likely attacks. There are three possible tactics for defeating a PPS; stealth, force and deceit. These three can be used on their own or in a combination during a scenario. Stealth means circumventing a line of defense; deceit means tricking it in one way or another and force means simply overpowering it. (Fay, 2007)

The writer says that the primary functions of a PPS are detection, delay and response, however, it is important to remember that the response refers to a threat, and not to an actual situation, an example of this is "deterrence" that prevents a threat from becoming reality rather than being a direct response to someone trying to attack the PPS. (Fay, 2007)

- Deterrence – Discourage attackers
- Denial – Prevent access
- Containment – Prevent leaving with assets
- Recovery – Recover lost assets

Furthermore, it is written that quantitative methods are preferred for facilities protecting high value assets, and that qualitative methods are better when assets of lower value are included or when the data is lacking. In the qualitative assessment it is suggested that "low, medium, high" should be used instead of numbers. (Fay, 2007)

3.5 Social engineering

There are several ways to use social engineering to defeat or bypass security solutions. It is quite possible to get the needed information by using threats, bribes or even just engage in a normal conversation. In bigger organisations clothing and "know-how" becomes more and more important. As long as someone appears to have the right to be somewhere, or appears to know what only insiders should know, it is likely that he/she will be allowed access. The process is incremental; by asking a few "innocent" questions basic information can be gathered, enough to be able to proceed to the next step; and once a solid information-base is established it is easier to come across as an employee, or at least someone who has the right to be where he/she is. (Matthews, 2004)

The Milgram Experiment, 1961, shows an important aspect of social engineering. In the experiment the test subjects were either assigned to be teachers or students, but in reality all were chosen as teachers. The participants are told that the experiment is a study of memory and learning. The student was played by an actor. The teachers were to ask questions to the student, and depending on the answers the teacher were to give the student an electric shock (increasing voltage). The shock generator was a fake, and only generated the sounds of electric charges, the rest the actor stood for (acting as if in severe pain). The experiment showed that, even if the student screamed in pain, and complained about his aching heart and his heart problems, 100 % of the teachers gave shocks up to 300 V, and 65 % of all continued up to the maximum of 375 V. (Experiment-resources.com, 2008)

The experiment shows that women and men alike are equally willing to obey authority when given a command; regardless of whether they like doing it or not. In everyday life this means, people are likely to obey if someone acts is if they have the right to command, and if someone behaves as if they have the right to be somewhere, most would not question them; after all, 65% did not question giving lethal electric shocks to their student, the sole reason being them being told to do so. (Experiment-resources.com, 2008)

A very common practice is to "tailgate" or follow someone into a restricted facility; once again it should be pointed out that the more someone appears to be allowed somewhere, the more likely they are to be let in, or even have the doors being held open for them. Ways to enhance this is, by for example feigning impatience. A technique, similar in nature, is "shoulder surfing", to simple look over the shoulder when someone types a code, password or similar. (Matthews, 2004)

Since social engineering targets people and their trust in others, the countermeasures have to be aimed towards people as well. The most common countermeasures to social engineering includes outright paranoia (trust no one), penetration tests (test what flaws and weaknesses exists and make people aware of the risks), reminding messages (making people aware of the risks) and policies/procedures. (Matthews, 2004)

4. Security solutions and analysis

In this section three scenarios are being described and analysed, and then a combined analysis of all three scenarios have been made.

4.1 Scene 1: Establishing Surveillance

In the movie it is revealed that close to all areas of the casino are being monitored by cameras from a central security room (around 8 persons monitor the screens in there). A smartcard is required to get past the outer doors. Once inside the inner parts of the casino, an elevator, whose door is protected by a six digit code that is changed every day, leads down into the vault (left side of the image). The elevator uses a fingerprint authentication system, as well as a voice confirmation from the central security room in order to work. The elevator shaft is protected by green lasers. Between the elevator and the vault two guards have been positioned. The vault door itself is thick steel and is said to be very advanced. (Oceans 11, 2001)

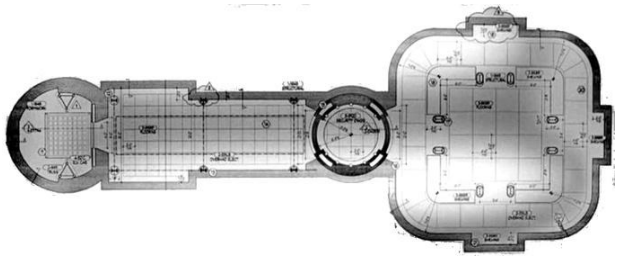


Figure 1. Map of the vault (Oceans 11, 2001)

4.1.1 Describe the scene

Before the scene even starts, it is been established that the perpetrators managed to acquire blueprints of the building, including the vault. How they did this is not explained, but it is indicated that the leader of the group knows a guard that aids him with acquiring them.

One of the tasks in the movie is to get in to the inner part of the building and connect the own surveillance system to the surveillance system of the casino and vault. Social engineering, talking and listening, reveals that two technicians work at the casino, and that one of the technicians is a single and has a crush on a dancer in a club. The perpetrators hire her to give him a lap-dance and, at the same time, acquire his smartcard (which is attached to his shirt with a clip). The entire casino, including the door to the inner parts, are being monitored by cameras, so the perpetrators arranges so that helium balloons are released and covers the camera for a short amount of time, enough for their own technician to sneak in through the door (even if a guard immediately is dispatched to the scene of the balloons to sort things out), which only requires him to insert the smartcard into a slot. (Oceans 11, 2001)

Figure 2. Smartcard-reader (Oceans 11, 2001)

Once inside, the technician heads straight to the server-room, using a map drawn on the palm of one of his hands. The inner corridors are being surveyed as well, but the personnel in the security central are talking to each other's, and fail to see him. The door to the server-room is protected with the same smartcard system as is used for the outer door. Once inside the room servers and cables are arranged in racks, but there are no locks doors or alarms. He attaches devices, 1x1 cm in size with a 5-10 cm antenna to several of the cables. The devices are clipped on, using no power whatsoever, indicating that it uses some kind of probing on the cable. (Oceans 11)

Figure 3. Small probe (Oceans 11, 2001)

Immediately after attaching the devices perfect high-resolution transmission is achieved in a neighbouring building of all cameras inside the casino. (Oceans 11, 2001)

In the way out he forgets his mini-TV (that he used to see if the connections worked), a guard finds it and hurries after him in order to give it to him, catching him just before the door and hands it to him. (Oceans 11, 2001)

4.1.2 Motivate why this scene is chosen

The scene is chosen because it portrays a likely scenario. Social engineering to achieve information so that even more social engineering can be used to retrieve a token, blocking cameras with balloons, entering using a stolen token, opening the server-room door using a token, accessing all cables and attaching spying devices, being detected by a guard, but dismissed as yet another technician.

4.1.3 Movie vs. reality

Two security solutions are found in this scene: Surveillance cameras, smart-card protected doors.

4.1.3.1 Surveillance cameras

Surveillance cameras count as one of the most basic tools of assessment in all security assessments. But, since cameras are used almost solely for assessment one has to consider the reactions from the surveillance-personnel. A few seconds after the balloons blocks the cameras a guard is dispatched. The response is fast and reasonably efficient. The use of cameras, to have a surveillance centre that can dispatch a guard at a few seconds notice, is a plausible scenario for a casino, and systems like this does exist in the real world.

4.1.3.2 Smart card locking system

Locking doors with smart-cards is to be considered common practice. That a technician has a token that gives access, first through the outer doors and then into the server room is no unlikely scenario.

4.1.4 The attack and how to counter it

The attacks used are social engineering to obtain a token, a simple distraction in the form of blocking a camera, and the use of a "mystical" device to intercept the video-transmissions.

As mentioned before, cameras are not a tool for detection, but merely for assessment, at least as long as they are not being constantly monitored. A few simple measures could have made the cameras more useful in

the scene. Assume, for example, that the surveillance-crew were alerted every time the smart-card protected door were opened, they would then have been able to identify the technician using another camera after walking through the door. Another measure would be to simply lock down entry access for as long as the cameras are being unable to provide accurate information due to being blocked, but this might complicate the normal routines at the casino. Perhaps the simplest measure would be to have a routine that says, if a camera is blocked, send two guards, one to locate, identify and deal with the reason for it being blocked, and another for securing what the camera was meant to cover.

A door that requires a token is a poor line of defence, if the token can easily be obtained. The obvious attack was that the dancing girl took his key-card, but one must not forget what lead to this attack being possible. The attack started using an insider that obtained information about a guard. If planned long enough ahead this initial obtaining of information is close to impossible to counter; even if routines for hiring include checking old police records and similar, it is not practically possible to even fight this form of information gathering. Once again the counter to the attack can be adding routines to the work-place of the technician, or to improve the technology used in the security solutions. Ponder a scenario where you hand in your pass-card when you are not working, or where the pass-card is disabled during the time you do not work; a measure like this would have prevented this attack completely. Another solution would be to add another method of authentication, for example adding a code to the door, or at least to the server-room. After all, having one pass-card bypass all the layers of defence, defeats the purpose of a layered defence.

One also needs to consider the target of the attack; the internal surveillance system. The false technician penetrates all defences and reaches the server-room, in there he attaches a device to a cable. With a surveillance-system as advanced as the one for the casino, it does not seem plausible that 15-20 different cameras all are connected using coaxial cables, but if that would be the case it might appear possible to attack them using a small device. If they, instead, are network cables, Ethernet cables, this attack suddenly becomes less plausible, because simply clipping the device to the cord would not be enough. The cable would have to be opened, and the different cables inside the cord would have to be identified. As this is not a study of the technical aspects of different probes, no more will be said apart from that it is unlikely this attack would work in the real world. While possible to create small transmitters, it is unlikely that a transmitter that small would be able to submit high-resolution transmissions, through several walls, through electric interference, even to a nearby building. If we ignore the fact that the attack is unlikely to work, the counters would have to be of a more technical nature. If it indeed is a network that is being probed, then adding encryption to the different streams might be possible. Apart from that, adding locked doors to the server-racks would also make it harder. One possible solution might be to make the cords tamper-resistant, if the connection is shut down or is weakened the security centre is being alerted, but since the "mystical device" is clipped on, this is unlikely. All this points towards that, since an attack on this system would have to be technically advanced, the countermeasures would have to be advanced as well, and it would therefore be easier to just add another layer in the defence and restrict access to the server-room.

One possibility that is not being mentioned above, that is slightly connected to tokens ("What I have"), is clothes. Assume that all technicians wear some special kind of uniform that are made solely for the casino-technicians, and that the technicians change into work-clothes at work; then it would be much harder for any perpetrators to pose as casino-technicians; they would have to have the clothes specially tailored for the occasion which would, by no means be impossible, but it would definitely complicate matters for a possible attacker.

4.2 Scene 2: Reaching the vault

4.2.1 Describe the scene

Through social engineering and outright spying it is found out that the casino changes the codes to the elevator leading to the vault every day. And when the codes have been changed, the new codes are given to the owner in a small envelope, every day at the same time. One of the perpetrators uses this by disguising himself as an official of the Nevada Gaming Commission. He walks up to the owner of the casino after the codes have been transferred and tells him that the insider previously mentioned has a past of being a criminal. The insider starts making a scene, and during the ruckus the disguised perpetrator picks the owners pockets and steals the codes to the elevator doors. He then walks to the elevator and enters it. The "mysterious probe" previously mentioned, is now used to replay recorded video to the internal surveillance-system, thus preventing detection as the man inside the elevator opens up a small hatch in the ceiling, and climbs up into the elevator shaft. The reason for not taking the elevator down is that it is protected by a finger-print sensor that is said to be impossible to trick, and voice verification from the security room. The attackers' next step is to climb down into an elevator

shaft that is protected by several lasers that, supposedly, chimes an alarm if the light is broken (Oceans 11)

At this time another attacker uses a "pinch" out on a nearby street to create an electromagnetic charge that disrupts all electrical systems in the city block for 30 seconds, during which time the perpetrators lowers themselves into the shaft. The guards standing in front of the vault door are rendered unconscious using an undefined gas. (Oceans 11, 2001)

4.2.2 Motivate why this scene is chosen

The scene is chosen because the essence of it is plausible. If we look past the fact that lasers might not be the optimal choice for motion detection, and that a "pinch" does not exist in the form that it is used, it shows two important principles. The first one being that exaggerated security might, in itself be a hole in the security (such as changing codes to often), and the second one being that even the best layered defence fails, if the assumptions it is constructed on fails (in this case the assumption that the electricity will not be interrupted).

4.2.3 Movie vs. reality

The following defensive systems are being shown in the scene:

4.2.3.1 6 digit door code

Implementing a system that requires people to enter a code in order to open a door is close to trivial, and is a set standard in many buildings and houses.

4.2.3.2 Surveillance cameras

Discussed earlier in the report.

4.2.3.3 Fingerprint detection and verbal confirmation

A fingerprint system that cannot be fooled is close to impossible to construct, especially if the attacker has enough resources. It can, however, be interpreted as "a fingerprint system that is impossible to fool within a given time", and in that case it is very much a possibility. If the verbal confirmation is added to the authentication system, the system can be said to be fairly safe, and even more important, fingerprint detection exists today, and different communication systems such as telephones also exists.

4.2.3.4 Lasers

A system that is reasonably simple to implement, and even if placing said system in an elevator shaft, there are no reasons for why it could not exist in the real world. it is not uncommon to see systems where the breaking of a beam of light triggers a bell for a door, and thus it must be considered as possible.

4.2.3.5 Guards

The usefulness of having two guards standing in a corridor talking to each other's might be discussed, but that it would be possible in a real scenario is beyond doubt.

4.2.4 The attack and how to counter it

The principle behind the attack on the 6 digit code is reasonably simple. A situation is created (by exposing the insider) and the victim is distracted (by the insider) so that his pockets can be picked.

The one reason for the attack to even be possible is that an attempt is made to achieve security by changing the codes often rather than have solid routines for how the codes should be handled. A risk analysis could easily have shown that passing the code from person to person every day is a big risk, and that the risk would have been reduced should the code either been passed less frequently, or in a way that would prevent it from being intercepted.

The next line of defence, whose efficiency is not tested due to the attackers circumventing it, is the fingerprint authentication and the verbal confirmation. These two defences, when combined with the surveillance cameras as a tool of assessment, provides a strong line of defence that is difficult to defeat. If one examines the system one sees that it is based on the principles "What I know" (knowing the code) and "What I do/am" (having the right voice/fingerprint). The only way to increase this layer of defence would be to, first of all remove the design flaw that allows an attacker to circumvent it (going up on top of the elevator through a hatch) by either sealing the hatch or move the authentication systems to the door leading into the elevator.

Lasers as a defence is questionable at best, since lasers can be redirected or simply avoided. (more of lasers in the last scene). The attack does not target the detectors as such, but rather the system beneath it, the power grid. The "Pinch" that is used to release an electromagnetic pulse could very well exist. It most definitely exists in a smaller scale, but whether a device, big enough to fit in a trunk and being powered by 12 car batteries can disrupt the electricity in an entire city block for 30 seconds is uncertain. (Non-nuclear Electromagnetic Pulse Generation). Regardless of whether the "Pinch" is to be considered a possibility or not, it most definitely is a

possibility that an attacker might target the power grid. It is important to remember the "fail-safe" aspect of defence, in other words, what happens if the electricity goes down? Will it be possible to open doors or will everything be locked down? The conclusion here is that, if the pinch is to be considered a reality, the only counter is non-electronic defences.

The last step, to position two guards in an empty environment to guard a door that no one is supposed to pass through is a questionable solution. The reality that the guards will not be able to remain alert for long must be taken into account, and should an attacker take the most likely route, the elevator, it is likely that they could be incapacitated before they would be able to react. Had instead an extra layer of defence been added, a layer where the guards had to grant access in order to proceed it would have added to the defence, but in the current form it adds close to nothing.

The probe used on the internal surveillance system was discussed a bit previously, and in this scene it is assumed that the probe can also continue to send it is transmissions to the neighbouring building, while at the same time receiving transmissions and use it to replace the original data flow. The step from simply probing a cable to with a clip on device, to actually replacing the transmission, while both sending and receiving high definition video is, in its current form, nothing but science fiction. Had a more advanced computing unit been placed in the server-room it might have been possible, but that would also add the possibility of other counters.

4.3 Scene 3: Breaking into, and escaping the vault

4.3.1 Describe the scene

Breaking into the vault consists of several parts. First they smuggle a man into the vault, but placing him inside a cart that is used for collecting the winnings in the casino and leave him to be deposited. The two that delivers him lacks proper identification, but they are not questioned, nor is the cart checked, but instead immediately brought to the vault. Inside the vault green lasers covering the floor is the only defence, and it is outmanoeuvred by jumping from obstacle to obstacle. The goal of placing a man inside the vault is that he is supposed to apply shaped charges to blast the rods holding the door in place. (Oceans 11, 2001)

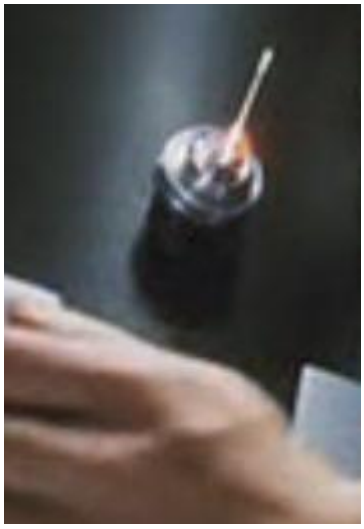


Figure 4. Shaped charge (Oceans 11, 2001)

When the door is blasted open, without chiming any alarms, the perpetrators calls the casino owner and informs him that the casino is currently being robbed, with the effect that the owner immediately calls the city police from a cell phone. The phone call is intercepted, and the attackers answer it, dispatching a fake SWOT unit. The fake SWOT enters the vault, and carries the money out. (Oceans 11, 2001)

4.3.2 Motivate why this scene is chosen

The scene is chosen because of the delicate balance between simplicity and complexity. A small mistake (not checking the identity of those delivering the cart) makes the entire operation possible, and the trick of pretending to be the police and use that ploy to escape with the money shows how important trusted sources are. A user normally does not expect a phone call to be directed to the wrong place, or a DNS server to give false information, yet when it happens, all measures based on that security immediately falls.

4.3.3 Movie vs. reality

Two layers of defence are being presented in the last scene:

4.3.3.1 Lasers

Discussed earlier in the report.

4.3.3.2 Vault door

There is no discussion about whether a vault door made of steel can exist.

4.3.4 The attack and how to counter it

The first part of the attack consists of sneaking a person into the vault. The easiest way to counter this attack would be to question those that handed over the cart without being able to show proper identification. Routines have to cover all eventualities, common as well as uncommon. If there is doubt the security has to be prioritised. A routine saying that the carts has to be examined would also have countered the attack, as would adding a tag system to the carts themselves, so "false carts" could not be used.

To avoid interrupting laser beams by simply climbing on obstacles is a trivial attack, and the attack shows the weakness of lasers as a line of defence. Had ordinary motion detectors been used instead, the vault would have had a better protection, as a much lower cost.

It is possible to blast a steel door open, but the attack as portrayed in the movie is not. In military applications a shaped charge can penetrate about 7-10 times the diameter of the explosive charges cone diameter. (See schematic figure of a shaped charge in Appendix) A rough estimate tells us that the charges seen in the movie would have a diameter of about 0.5 inches, thus meaning 3.5-5 inches of steel could be penetrated. (Wikipedia, 2011) Even if the charges would have enough effect to actually cause any damage on the door, it seems unlikely that a vault door would not have an entry alarm, and the best counter for this effect would be to add a vibration alarm to the doors.

It is questionable whether the last step is to be considered an attack on the system or not, but it could be seen as social engineering, posing as someone that is allowed access to and from the vault (the SWOT team). The only way to counter this specific attack would be to question the trust relations, as in questioning the police being called to help. It would, however, be reasonably easy to demand that the team identifies themselves before entering the vault, but as the Milligram experiment shows, people in general are unwilling to question authorities.

4.4 Combined analysis

Accordning to John J. Fays methodology concerning how a system can be assessed it's stated that a quantitative approach is preferred but if the data is lacking a qualitative approach is acceptable.

The asset to be protected is the money; other possibilities such as the integrity of the game-machines, information about the casino workers etc. could also be of interest, but since this report is limited to the three scenarios, and the driver in the scenarios is money, that will be the only asset mentioned in the assessment. A brief analysis of the path shows the different layers and lines of defense that has to be defeated in order to obtain the assets. The path is listed in the table, as are the methods of attacks and a short description of the defense used in each layer.

Asset	Money
Path	Outer casino, inner casino, elevator, vault corridor, vault door, vault

Layer	Protection	Protection principle	Attack	Attack Description
General	Cameras	Detection	Deceit	Manipulating transmissions
General	Police	Reaction	Stealth	Avoiding contact
Outer casino	Guards	Reaction	Stealth	Avoiding contact
Inner casino	Smart card lock	Denial	Deceit	Social engineering
Elevator	Door code	Denial	Deceit	Social engineering
	Fingerprint authentication	Denial	Stealth	Circumvent
	Verbal confirmation	Denial	Stealth	Circumvent
Elevator shaft	Laser detection system	Detection	Stealth	Disable by attacking power supply
Vault tunnel	Armed guards	Reaction	Force	Knocking the guards out
Vault door	Bolt-locks	Denial	Force	Shaped explosions
Vault	Laser detection system	Detection	Stealth	Circumvent (acrobatics)

Table 1. The layered defense

One of the conclusions that can be made from this table is that there appears to be three phases of the attack, an initial phase where social engineering is the main element, one phase where circumvention is the main element and a final phase where brute force is used. One can also make the conclusion that, the three detection-systems were being used, one of which could be manipulated, and two that could be circumvented. As stated before, any security system will fail if the attacker has enough time, and since the first targets of attack were the detection-systems the rest of the systems eventually failed as well. This points towards that, even if all lines of defense were defeated (circumvented, deceived or overridden), what needs to be improved the most are the means of detection. The entire operation was based on the cameras being disabled; one natural solution to this problem would be to have several independent systems for detection; and perhaps routines for controlling the integrity of the detection systems as well.

The idea of the attack being divided into three different phases is an interesting one, because of the simple fact that the initial phase is close to impossible to prevent, and the second phase is based on avoiding or disabling defenses. It is only the third line of defense that is likely to trigger alarms in the current setup, which means that the reaction time is reduced. Even if an alarm had chimed when the perpetrators blew the vault door open they would have gotten away. Because of this one could simply view the current system as a much smaller system.

Layer	Protection	Protection principle	Attack
General	Cameras and alarms	Detection	Deceit/Stealth
Entrance	Codes and authentication	Denial	Deceit/Stealth
Vault-area	Guards, doors	Denial	Force

Table 2. Simplified system

One quickly realizes that this would not be possible should the PPS be arranged differently. If the defense-system forces the attackers to do a sequence of attacks, it would not be possible to divide the PPS into subsystems, for example: Stealth → Force → Deceit → Force → Stealth. Thus the goal should, logically, be to force the attackers to have to reveal themselves, so that the principles of detect, delay, react can be used.

Another lesson that can be learned from the above scenarios is how easy it is to attack a system with only one kind of protection. For example, in the movie a smartcard was obtained, a smartcard that allowed access to the inner parts of the casino and even to the server-room. All that was required in order to succeed was to distract a technician so that his card could be stolen; a fairly simple task that could easily have been achieved using blunt force, deceit (social engineering and similar) or simply picking his pockets (stealth). If the system had required multiple methods of authentication (for example adding a door code) the complexity would have increased drastically.

5. Discussion

Two kinds of conclusions have been made in this section, one concerning the nature of the movie vs. reality, and the other concerning the nature of physical security.

5.1 The movie vs. reality

There are several layers of defence presented in the movie, and the conclusion is that all lines of defence are possible. Some parts are clearly impractical, some could, and should, be enhanced and other parts are quite clearly missing. To give examples of each category; lasers are quite clearly impractical, seeing that a standard motion detection system would yield better results at less cost; smart-card authentication might be simple but it should be enhanced, but for a server-room using both a smart-card and a code would be preferred; it might also be good to add software to the surveillance system that triggers an alarm should motion be detected in restricted areas; one part that is quite clearly missing is a sensor that triggers an alarm if the emergency hatch on the elevator is opened, or that triggers when the vault is blown open in an explosion. That it is possible to change elevator-codes every day is beyond doubt, but this is something that reduces security rather than increases it.

As for the attacks, a majority of the attacks would quite clearly work in real life. Social engineering and the study of guards would, in many cases, be quite efficient, and obtaining smart-cards and codes by picking pockets is not at all impossible. However, the technology fails. The probe used for streaming and manipulating the video-streams is improbable at best, and most likely impossible. The concept of shutting down the power in order to bypass a line of security is not unknown, however, the "pinch", even if it uses known principles from the physics, is unlikely to work in the magnitude show in the video. The final and last piece of advanced technology, the shaped charges used to blow the vault door, are unlikely to be possible. Shaped charges that could do it, with no doubt exists, but they are likely much larger.

The conclusion is therefore that the defenses are possible, but impractical, and that the attacks were impossible due to made up technology that does not exist in the real world.

5.2 Physical security

Two conclusions have been made about the nature of the physical security.

The first conclusion being that, unless the principles of "detect, delay, react" are being observed the PPS will fail. The defence needs to be layered if it is to successfully neutralize a threat, and it is not enough to just add more and more components, if the security components are not organized in a manner so that they cannot be grouped together the system is more likely to fail. This means that a system, in order to be safe, not only needs to be layered, but the layers needs to add complexity to the attacks used to beat it. If we consider the required attack patterns:

Weak defense:

Stealth→Stealth→Stealth→
Deceit→Deceit→
Force→ Force

Weak defense (simplified pattern):

Stealth→Deceit→ Force

Strong defense:

Stealth→Deceit→Force→
Stealth→Deceit→
Force→Stealth

The "weak defence" is fairly easy to attack, especially if one considers the simplified pattern. A possible attacker will not have to change tactics much at all, and the defence, even if it consists of 7 different parts, is, in essence, nothing but a 3 part system. The "strong defence" on the other hand, forces the attacker to change

strategy several times. It is important to remember that, while both defence systems are slightly different in outlook, they have the same components.

The first line of attacks is quite easy to achieve, while the other line requires changing strategies, and thus is much more complex both in construction and

The second conclusion is that very small measures are required to plug the holes in a defence (breadth). Combining pass-codes with smartcards, or just changing basic routines (like storing the clothes in a locker at the workplace or requiring all that identify themselves if they are not known) might be enough to prevent most attacks, including social engineering.

5.3 The method

The methodology used in this report uses a standard approach

- Select the object of study (the movie/scenes)
- Describe the important aspects of the object
- Establish a theoretical framework
- Analyse the object in accordance with the framework
- Make conclusions

While the methodology does provide a solid framework for a report, it is important to understand the limits of it. Since the object should be viewed in the light of the theoretical framework, rather than the other way around, starting by selecting an object of study is a questionable, but understandable, approach. The reason for this might be that the task was not specified enough from the start. Had the task for example been to "evaluate the shaped charge that is described in the movie" the structure would be radically changed, but it would have enabled a different approach. The example of the shaped charge also illuminates a second limitation of the report, namely the depth of it. Within the scope of this paper it is not possible to go into the required level of detail to fully evaluate the technical aspects of the shaped charge or the probes described in "scene 1". This in turn implies two possible paths of further studies of the object; the first path being a deeper evaluation of the technical aspects of the security solutions and of the attacks, the second path being on a more strategic level, where the system as a whole is being examined more thoroughly, having the focus on breadth, depth and deterrence rather than on the individual parts. Aspects of cost and benefit could also be included in that path.

6. Conclusions

This report contains descriptions, analyses and discussions about the security solutions found in "Ocean's eleven". The movie has been chosen because it presents a reasonably real/plausible scenario with enough detail to allow a deeper analysis.

Three scenarios from the movie have been analysed, and discussed. The conclusions made are twofold, the first part covers whether the movie can be considered as "real" or not, and the second part covers what conclusions can be made from it.

For the first part, the conclusion is that the defences described in the movie are possible, each and every security measure could be used in a real scenario, even if some parts of the defence are lacking (no explosion-alarm on the vault door, common access to server-rooms etc.) or outright impractical (changing codes every day, laser-beams for motion detection etc.) However, the attacks on the system are not possible; several of the attacks rely on non-existing technology (made up probes, small shaped charges).

As for the second part, what can be learned is that the nature of the plausible attacks on a layered defence needs to be carefully considered. The PPS (Physical Protection System) needs to force the attackers to change tactics. For example, a PPS with 5 layers that all can be defeated using stealth, can, and should, be considered as one single layer, since only one tactic of defeating the system is required. The other conclusion is that it often takes very little to improve the security; a change of routines, or simply adding a key-code to a smart-card protected door would be sufficient to stop most attacks

6.1 Further studies

The paper opens up for two possibilities for further studies of "Physical security in Ocean's 11".

The first being of the technical aspects; how are the solutions and the attacks constructed, could a probe or shaped such as described exist.

The second being of the system as a whole; how well do the system adhere to the principles of breadth, depth and deterrence. What are the costs and the benefits of certain layouts when compared to others? This path would be possible both from the perspective of the construction of the security system, as well as the attackers' perspective.

References

Internet

International Movie Database, *"Ocean's eleven" [online]*. Available at: http://www.imdb.com/title/tt0054135/ [Accessed 2011 Mar 15]

AMC Filmcritic.com, Ocean's eleven [online]. Available at http://www.filmcritic.com/reviews/2001/oceans-eleven/ [Accessed 2011 Mar 15]

New Scientist, 11 December 1999, "Warning! Strange behaviour!" [online].Available at: http://architecture.mit.edu/house_n/web/resources/articles/lifeinthefuture/New%20Scientist%20Feature%20Warning!%20Strange%20behaviour.htm [Accessed 2011 Mar 16]

Experiment-resources.com, 2008, *"Stanley Milgram Experiment (1961)"* [online]. Available at: http://www.experiment-resources.com/stanley-milgram-experiment.html [Accessed 2011 Mar 16]

Jerry Emanuelson, 2010, *"Non-nuclear Electromagnetic Pulse Generation"* [online]. [Accessed 2011 Apr 7]; Available at: http://www.futurescience.com/emp/emp-gen.html

Wikipedia, *"Shaped charge"* [online]. Available at: http://en.wikipedia.org/wiki/Shaped_charge [Accessed 2011 Apr 7];

Movies

"Die Hard 4", 2007. [DVD] Len Wiseman, USA. 20th Century Fox.

"Mission Impossible 3", 2006. [DVD] J.J. Abrams, USA. Paramount Pictures.

"Ocean's eleven", 2001. [DVD] Steven Soderbergh, USA. Warner Bros. Pictures.

"Ocean's 12", 2004. [DVD] Steven Soderbergh, USA. Warner Bros. Pictures.

*"Ocean's 13",*2007. [DVD] Steven Soderbergh, USA. Warner Bros. Pictures.

Lectures

Viiveke Fåk, 2004-01-21, *"Advanced User Authentication"*, The Department of Computer and Information Science. Linköping's University, Unpublished

Literature

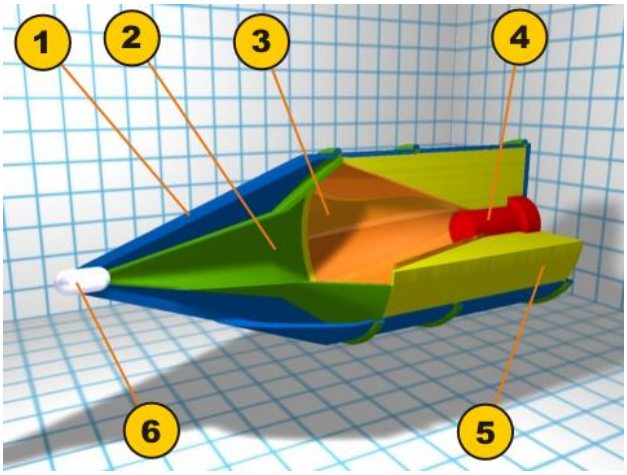
Matthews, Bruce R., 2004, *"Physical security: controlled access and layered defense"*. in Tipton & Krause (Eds.) *"Information Security Management Handbook"*. 5th ed.. Auerbach.

John J. Fay, 2007, *"Encyclopedia of security management"*. 2nd ed. Elsevier.

Appendices

Shaped charge

Below is a schematic picture of a shaped charge. The angle of the conical liner is usually 40-90 degrees, even if conical liners do exist. For this paper it's important to observe the length of the device in relation to its width, and to also keep in mind what the dimensions, and possible volumes of explosive would be if the device had a length of 0.5 inches. (Wikipedia, 2011)



Figur 5. Shaped charge (Wikipedia, 2011)

1. Aerodynamic cover
2. Empty room
3. Conical liner
4. Detonator
5. Explosive
6. Piezo-electric trigger