2019-2020

Formal Methods for Secure Systems Project

Barsanti Nicola, Tumminelli Gianluca

Bank Robbery

**Contents**

**Introduction**

The following paper will document the development of an *ADVICE*(ADversary VIew Security Evalution) model realized to analyse the behaviour of a bank subject to security attacks.

Through *Mobiüs* we simulated two different types of attacks that can be carried out to steal money from the bank or from its customers, in particular we analyzed:

* **A physical attack**:the opponents try to rob the bank following a planned attack and gaining the control of its safety devices
* **A cyber attack**: the opponents try to infiltrate into the bank network or to steal credentials from its customers to transfer money into their accounts

We have considered that the opponents are professionals, they know how to attack and what they have to do to reach the goal. We have identified two main types of attacker:

* **Professional Robbers**: they prefer rapid attacks in which they have not to spend a lot of resources. They are accustomed to the risk of being identified and they don’t care about it.
* **Hackers**: They don’t care about the time, the resources needed or if the attack will not gain so much money. Their main interest is to remain anonymous and not risk to be identified.

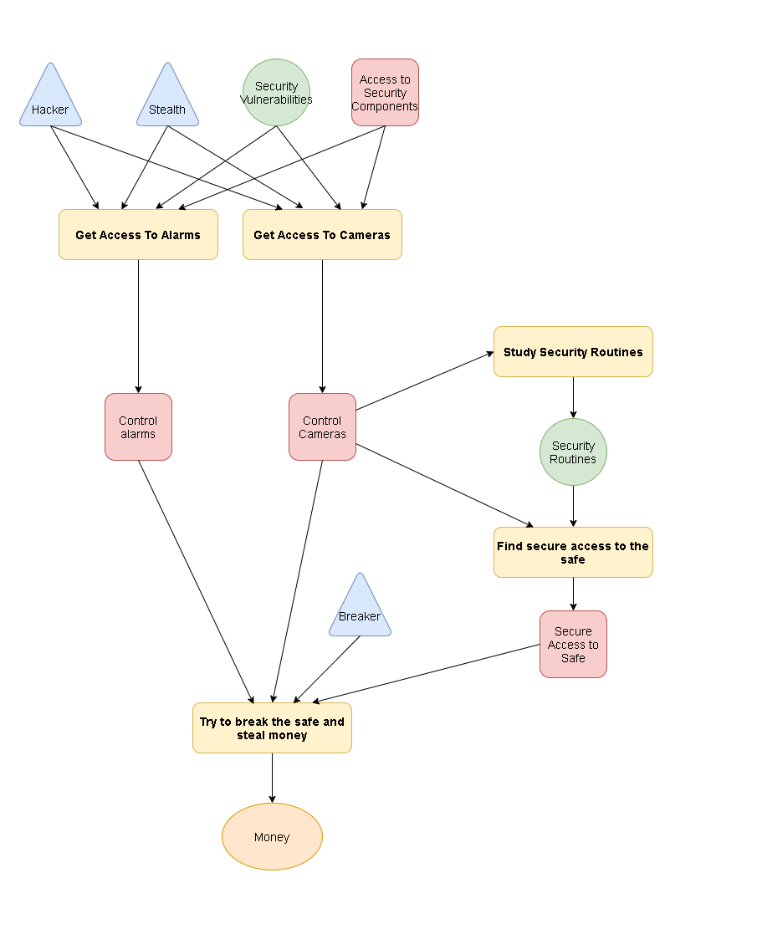
Finally we have considered the bank pretty secure. It uses an highly secure building protected by cameras, alarms and secure guards. The informatic system is secure too and made by professionals careful to not allow vulnerabilities to eventual attackers. To verify that all the bank systems are not compromised periodically technicians will verify the integrity of all the secure and informatic systems to detect eventual impairments.



Figure 1: Example of a Bank Structure

**Attacks**

Now we will describe in detail the assumptions and the steps of each attack designed into the simulation

**Physical Attack**

**Main Characteristics:** An attack which not require a lot of time to be performed, it’s risky but the attackers can obtains all the money contained in the vault

**Most difficult parts to handle:** The planning of the attack which requires the control of all the security devices and to find a way in

**Skills needed:** Hacker, Stealth, Breaker

**Starting point:** The attackers have to know a vulnerability of the security devices and a way to use it

**Adversary Preferences**:

**Cost**: 0.4

**Detection**: 0

**Payoff**: 0.6

**Steps:**

* **Get Access To Alarms**
  + **Preconditions**: The attackers needs to know the vulnerabilities of the system and a way to approach and violate it without being seen.
  + **Description**: Violate the alarms secure system to disable it.
  + **Cost**: 30
  + **Time**: 5-30m, the requested time depends on the hacker abilities of the attacker
  + **Possible outcomes**: The attack can be conclude with a success(1%) or with a failure(99%). The probability of being detected is high with 35% in case of failure and 5% in case of success.
* **Get Access To Cameras**
  + **Preconditions**: The attackers need to know the vulnerabilities of the system and a way to approach and violate it without being seen.
  + **Description**: Violate the cameras secure system to be able to view their video streams or disable them.
  + **Cost**: 30
  + **Time**: 5-30m, the requested time depends on the hacker abilities of the attacker
  + **Possible outcomes**: The attack can be conclude with a success(1%) or a failure(99%). The probability of being detected is high with 35% in case of failure and 15% in case of a success.
* **Study Security Routines**
  + **Preconditions**: The attackers need to control the bank cameras and see their content.
  + **Description**: Observe the security guard routines, the patrolled routes and the time and timing of the guard checks using the cameras of the bank.
  + **Cost**: 5
  + **Time**: 1000
  + **Possible outcomes**: The attack can be concluded with a success(75%) a failure(15%) or because the camera violation has been detected(10%). In the last case the bank will remove the violation and the attackers will loose their access to cameras. The probability of being identified is 0 for all the outcomes except for the detection of the violation into the cameras(10%).
* **Find Secure Access To The Safe**
  + **Preconditions**: The attackers need to control the bank cameras and see their content ant to know the security routines.
  + **Description**: Observe all the bank internal structure and using the knowledge of the security routines find a valid route to reach the safe without been uncovered.
  + **Cost**: 5
  + **Time**: 2000
  + **Possible outcomes**: The attack can be concluded with a success(10%), a failure(70%) or because the camera violation has been detected(20%). In the last case the bank will remove the violation and change the security routines to prevent a possible violation of the security. So the attackers will loose their access to cameras and their study of the security routines became useless.
* **Safe Break**:
  + Preconditions: The attackers need to control the cameras and the alarms of the bank. They also need a secure path to reach uncovered the vault.
  + Description: A breaker will force the safe and the robbers will get the moneys. This attack is also extended in combination with the cyber Attack which permits to the robbers to obtain the safe combination by violating the bank informatic systems.
  + Cost: 40(Using safe combination),70(Using a breaker)
  + Time: 20(Using safe combination),60(Using a breaker)
  + Possible outcomes: The attack can be concluded with a success(75%) or with a failure(25). In case of success the probability of being identified is low(15%) buti f the attack fails the robbers will almost certainly identified(95%).

Figura 2 ADVISE attacco fisico

**Immagine che contiene testo, mappa

Descrizione generata automaticamente**

**Cyber Attack**

**Main Characteristics:** An attack which require time and resources to be performed. The money obtained are limited by the limitation of online transactions but the attacks have very low probabilities that the attacker will be identified.

**Most difficult parts to handle:** The access to the secure systems for generate a backdoor.

**Skills needed:** Hacker, Social Engineer

**Starting point:** The attackers have to know a vulnerability of the bank informatic systems otherwise they can also do phishing to the customers

**Adversary Preferences**:

**Cost**: 0

**Detection**: 0.4

**Payoff**: 0.6

**Steps:**

* **Phishing**
  + **Preconditions**: The attacker needs social engineering skills to cheat his victims
  + **Description**: The attackers will send tons of mail or every possible phishing channel with the hope that someone will be cheated and gives his credentials
  + **Cost**: 50
  + **Time**: 3000-5000m(depending on the social engineering skill of the attacker)
  + **Possible** **outcomes**: The attack can be concluded with a success(1%) or with a failure(99%), in each case the probability of being detected is null.
* **Transfer Customer Money**
  + **Preconditions**: The attacker needs the customer credentials
  + **Description**: The attacker using the customer credentials access to the victim account and transfer money into an anonymous account of his property
  + **Cost**: 5
  + **Time**: 5
  + **Possible** **outcomes**: The attack can be concluded with a success(80%) or a failure(20%). In case of failure the probability of being detected is 10%
* **Cyber Attack**
  + **Preconditions**: The attackers need to know the vulnerabilities of the system and to have hacking skills to exploit the system
  + **Description**: The attacker using a vulnerability will exploit the system and generate a backdoor to perform a deeper attack into the system
  + **Cost**: 70
  + **Time**: 30-60m(dependent on the hacking skill of the attacker)
  + **Possible** **outcomes**: The attack can be concluded with a success(1%) or a failure(99%). The probability of being detected is of the 5% in case of success or 1% in the case of failure.
* **Infect the system**
  + **Preconditions**: The attackers need a backdoor into the bank system
  + **Description**: The attacker try to infect the bank net to gain control of all the informatic systems
  + **Cost**: 65
  + **Time**: 10-30m
  + **Possibile** **outcomes**: The attack can be concluded with a success(5%) a failure(65%) or because the technician has found the backdoor and close it(30%). In the last case the attackers will loose their access. The probability of being detected is very low for each attack and estimated around the 5%.
* **Get Director Credentials**
  + **Preconditions**: The attackers need a backdoor into the bank system
  + **Description**: The attackers try to steal the director credential from the bank system
  + **Cost**:
  + **Time**:
  + **Possibile** **outcomes**:
* **Get Safe Combination**
  + **Preconditions**: The attackers need a backdoor into the bank system
  + **Description**: The attackers try to steal the safe combination from the bank system. This attack is very particular because it is usefull in conjunction with the Phisical Attack to make more easy access the safe
  + **Cost**:
  + **Time**:
  + **Possibile** **outcomes**:
* **Transfer Bank Money**
  + **Preconditions**: The attackers need the control of the bank informatic system of the director credentials
  + **Description**: The attackers controlling all the bank informatic systems or by having the director credentials transfer money directly into a private account of their own
  + **Cost**:
  + **Time**:
  + **Possibile** **outcomes**: