2019-2020

Bank Robbery

Formal Methods for Secure Systems Project

Barsanti Nicola, Tumminelli Gianluca

Contents

1 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.

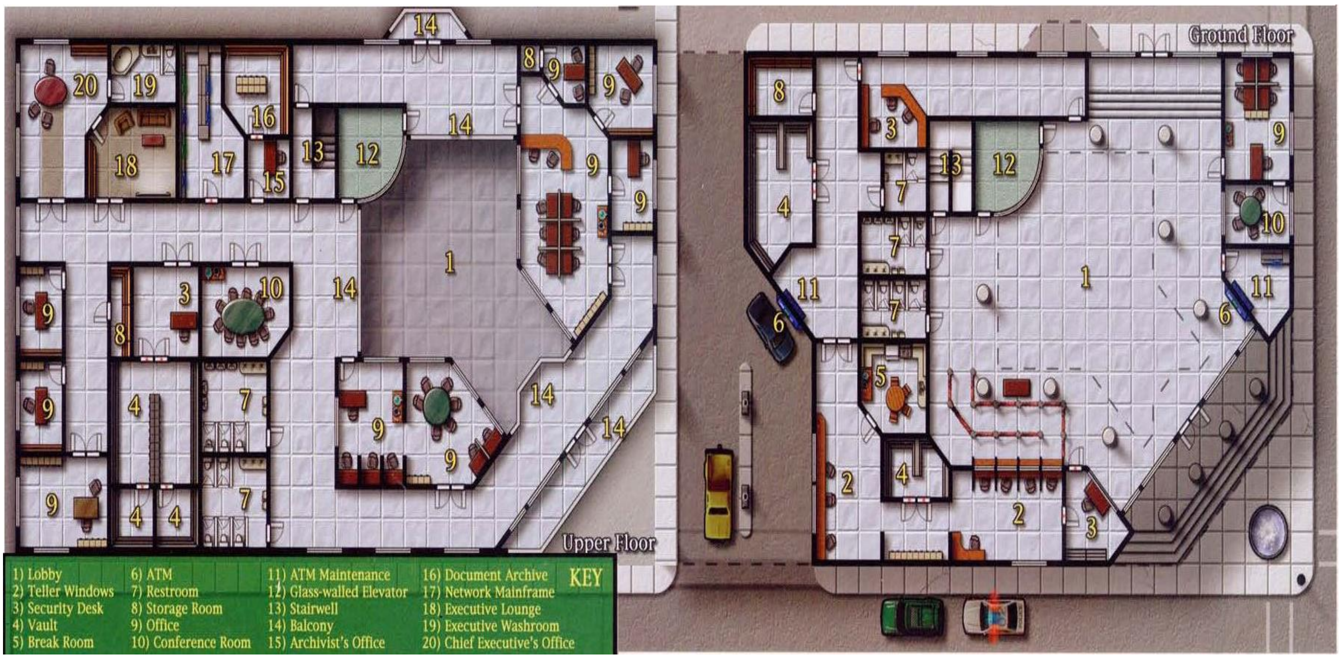
Through *Mobiüs* we simulated two different types of attacks that can be carried out to steal money from the bank or from its customers, in particular we analyzed:

- **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 attackers:

- **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.

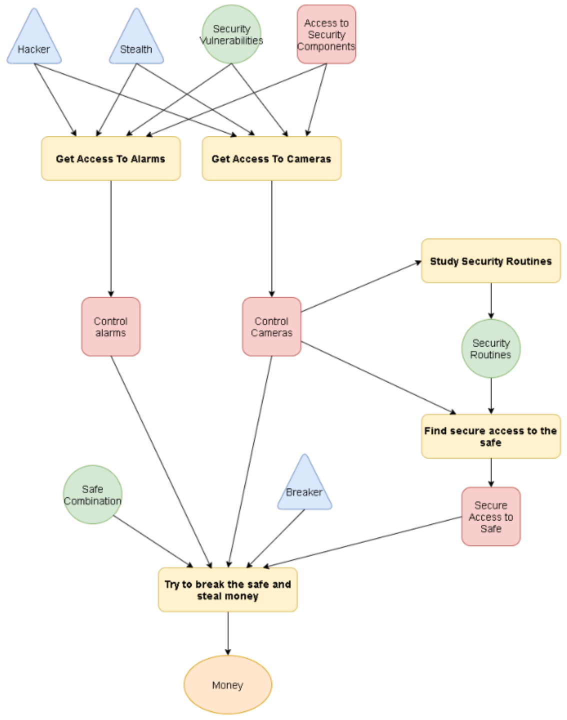
Finally we have considered the bank pretty secure. It uses an highly secure building protected by cameras, alarms and secure guards. The informatic system is secure too and made by professionals careful to not allow vulnerabilities to eventual attackers. To verify that all the bank systems are not compromised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



2 Attacks

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

2.1 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
  - **Outcomes**:
    - **[Success] probability:** 1% , **detection:** 5%, **results:** Obtain alarms control
    - **[Failure] probability:** 99% , **detection:** 35%, **results:**

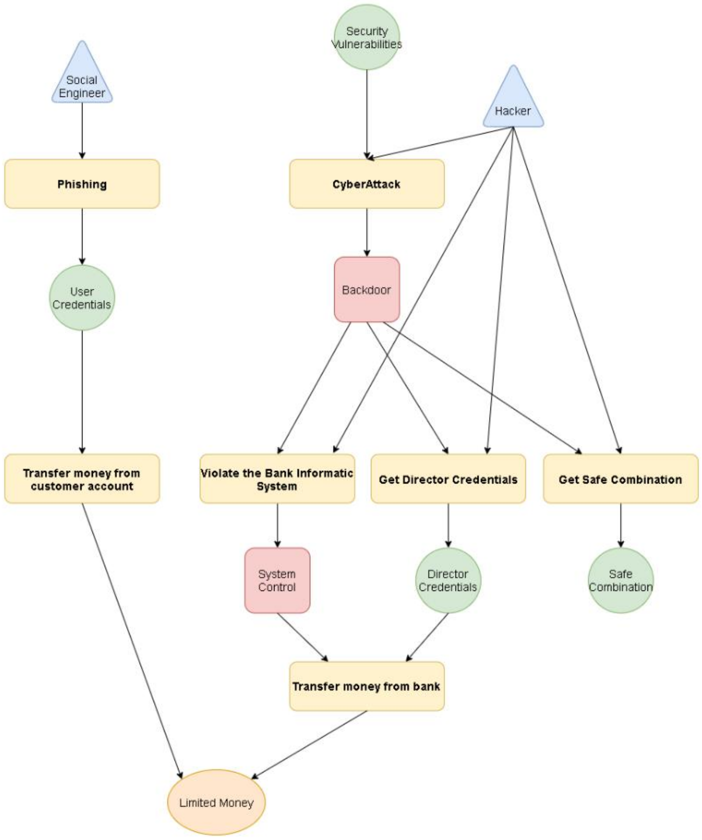
- **Get Access To Cameras**
  - **Preconditions**: The attackers need to know the vulnerabilities of the system and a way to approach and violate it without being seen.
  - **Description**: Violate the cameras secure system to be able to view their video streams or disable them.
  - **Cost**: 30
  - **Time**: 5-30m, the requested time depends on the hacker abilities of the attacker
  - **Outcomes**:
    - **[Success] probability:** 1% , **detection:** 15%, **results:** Obtain cameras control
    - **[Failure] probability:** 99% , **detection:** 35%, **results:**

- **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
    - **Outcomes**:
        - **[Success] probability:** 75% , **detection:** 0%, **results:** Obtain security routines knowledge
        - **[Failure] probability:** 15% , **detection:** 0%, **results:**
        - **[Camera Violation Detection] probability:** 10%, **detection:** 10%, **results:** Lose cameras control

- **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
    - **Outcomes**:
        - **[Success] probability:** 10% , **detection:** 0%, **results:** Obtain a secure path to the safe
        - **[Failure] probability:** 70% , **detection:** 0%, **results:**
        - **[Camera Violation Detection] probability:** 10%, **detection:** 10%, **results:** Lose cameras control, lose security routines knowledge

- **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)
    - **Outcomes**:
        - **[Success] probability:** 75% , **detection:** 15%, **results:** Obtain money goal
        - **[Failure] probability:** 25% , **detection:** 95%, **results:**

2.2 Cyber Attack



Main Characteristics: An attack which require time and resources to be performed. The money obtained are reduced 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)
  - **Outcomes**:
    - **[Success] probability:** 10% , **detection:** 0%, **results:** Obtain user credentials knowledge
    - **[Failure] probability:** 90% , **detection:** 0%, **results:**

- **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
  - **Outcomes**:
    - **[Success] probability:** 80% , **detection:** 0%, **results:** Obtain money goal
    - **[Failure] probability:** 20% , **detection:** 10%, **results:**

- **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)
  - **Outcomes**:
    - **[Success] probability:** 99% , **detection:** 5%, **results:** Obtain a backdoor for the bank system
    - **[Failure] probability:** 1% , **detection:** 1%, **results:**

- **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
  - **Outcomes**:
    - **[Success] probability:** 5% , **detection:** 5%, **results:** Obtain system control
    - **[Failure] probability:** 65% , **detection:** 5%, **results:**
    - **[Backdoor Detection] probability:** 30%, **detection:** 5%, **results:** Lose system backdoor

- **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**: 55
  - **Time**: 5-25m
  - **Outcomes**:
    - **[Success] probability:** 5% , **detection:** 5%, **results:** Obtain director credentials
    - **[Failure] probability:** 65% , **detection:** 5%, **results:**
    - **[Backdoor Detection] probability:** 30%, **detection:** 5%, **results:** Lose system backdoor

- **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**: 60
  - **Time**: 5-25m
  - **Outcomes**:
    - **[Success] probability:** 5% , **detection:** 5%, **results:** Obtain safe combination
    - **[Failure] probability:** 65% , **detection:** 15%, **results:**
    - **[Backdoor Detection] probability:** 30%, **detection:** 5%, **results:** Lose system backdoor

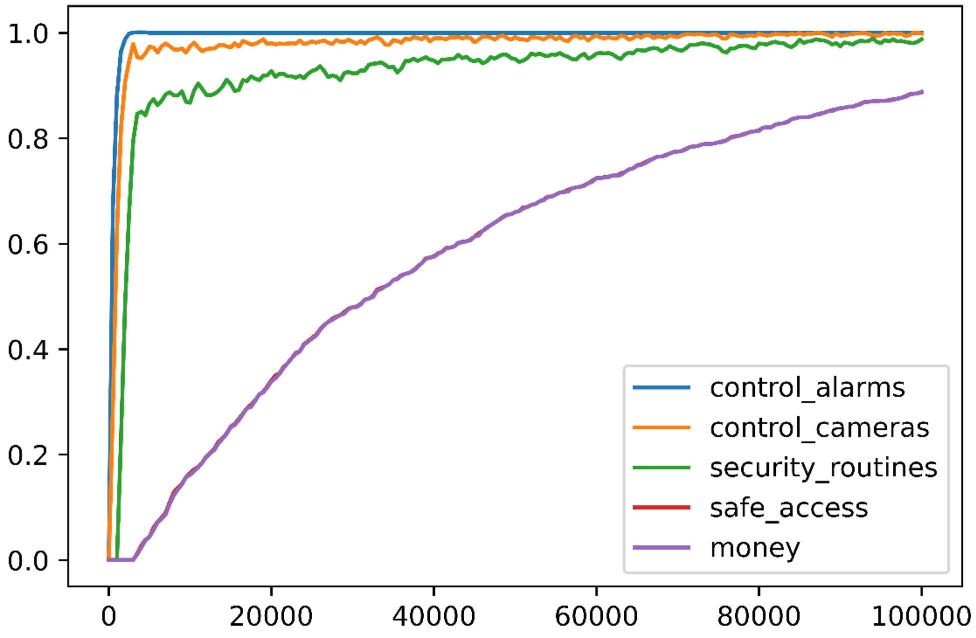
- **Transfer Bank Money**
  - **Preconditions**: The attackers need the control of the bank informatic system of the director credentials
  - **Description**: The attackers controlling all the bank informatic systems or by having the director credentials transfer money directly into a private account of their own
  - **Cost**: 5
  - **Time**: 5
  - **Outcomes**:
    - **[Success] probability:** 80% , **detection:** 5%, **results:** Obtain the money goal
    - **[Failure] probability:** 20% , **detection:** 10%, **results:**

3 Analysis

In this section we will analyse the results of the attacks simulation. In particular we will first analyse the behaviour of each single attack and at the end we will see how the attacks will affect on the bank security in a general scenario. Each graph is obtained by plotting the upper bound of the confidence interval of the correspondent variable. To calculate each variable we have config a confidence of 95% using 1000 batch processes.

3.1 Physical Attack

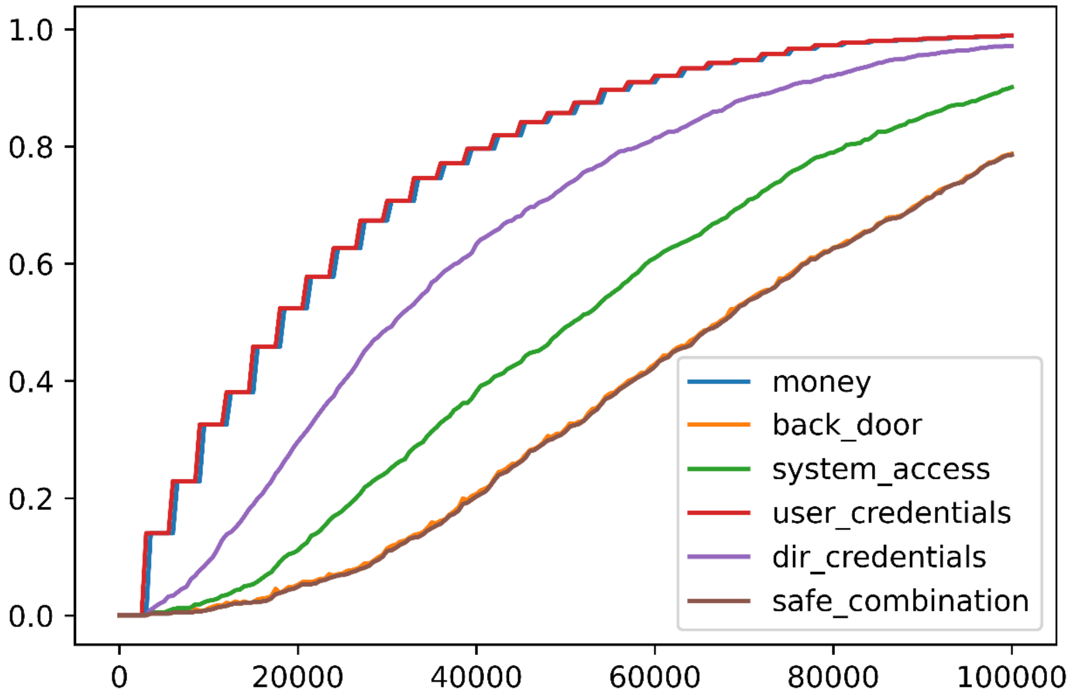
- **Reward of Interest**
  - **control_alarms**: the bank alarms has been disabled
  - **control_cameras**: the bank cameras has been violated
  - **security_routines**: the bank guards routines has been tampered
  - **safe_access**: a path to reach the bank vault has been found
  - **money**: the bank has been robbed



How we can see from the graph the security into the bank is strictly related to the difficulty of obtaining the cameras and alarms access. For this reason we see an interval [0,3500] of certain security in which the value money stay always on 0. Theoretically if we periodically verify the bank cameras and alarms from impairments with a period low than 3500m then the security of the bank to a physical attack is guaranteed with a confidence of 95%.

3.2 Cyber Attack

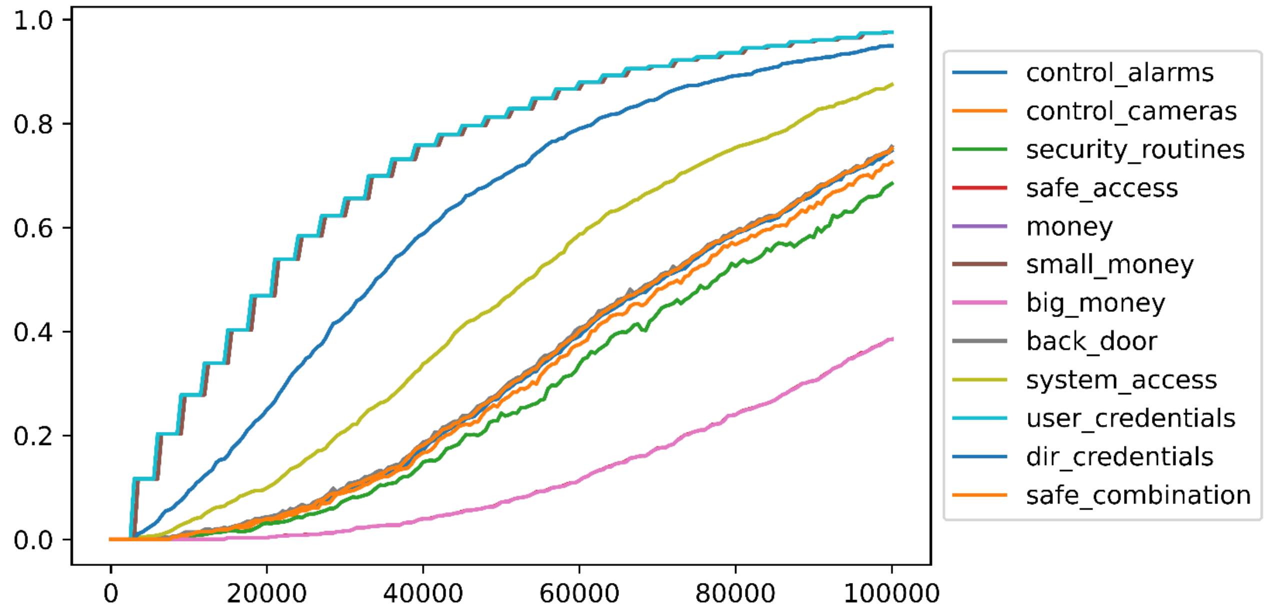
- **Reward of Interest**
  - **money:** an illegitimate transfer of money has been performed
  - **back_door:** the bank system has a backdoor installed on it
  - **system_access:** the bank system is under control of an attacker
  - **user_credentials:** a user bank credential has been stolen
  - **dir_credentials:** the bank director credentials has been stolen
  - **safe_combination:** the safe combination has been stolen



How we can see from the graph into the informatic area is easier to steal money. In particular is the phishing attack which guides the stealing of money. This has perfectly sense because is a simple attack based on an element(the men) that can't be controlled or "configured". Even if the probability of success is low the benefits of not been identified and the low cost of the attack makes the phishing a serious problem for a bank.

3.3 General Attack

- **Reward of Interest**
    - **control_alarms:** the bank' alarm has been disabled
    - **control_cameras:** the bank' camera has been controlled
    - **security_routines:** the bank' guards routines has been tampered
    - **safe_access:** a path to reach the bank vault has been found
    - **money:** money has been stolen
    - **small_money:** money has been stolen by a digital transaction
    - **big_money:** money has been stolen from the vault
    - **back_door:** the bank system has a backdoor installed on it
    - **system_access:** the bank system is under control of an attacker
    - **user_credentials:** a user bank credential has been stolen
    - **dir_credentials:** the bank director credentials has been stolen
    - **safe_combination:** the safe combination has been stolen



The attacks previously seen are not independent. They present a correlation on the safe_combination branch, in particular the breaking of the safe is easier if happens by using the safe combination which can be stolen during the exploit of the bank informatic system. So we expect a little improvement of the physical attack respect to the same scenario without the possibility to have the safe combination. The result show that in the general context the main chosen attack is the phishing even if it has very low probability of success and doesn't give a high payoff then we have many attempts to violate the bank security systems. The robbers prefer to make small attacks to obtain the money rather than a moneymaking risky one.