2019-2020

Formal Methods for Secure Systems Project

Barsanti Nicola, Tumminelli Gianluca

Bank Robbery

**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** in whichthe opponents try to rob the bank following a planned attack and gaining the control of its safety devices
* **A cyber attack** in which 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

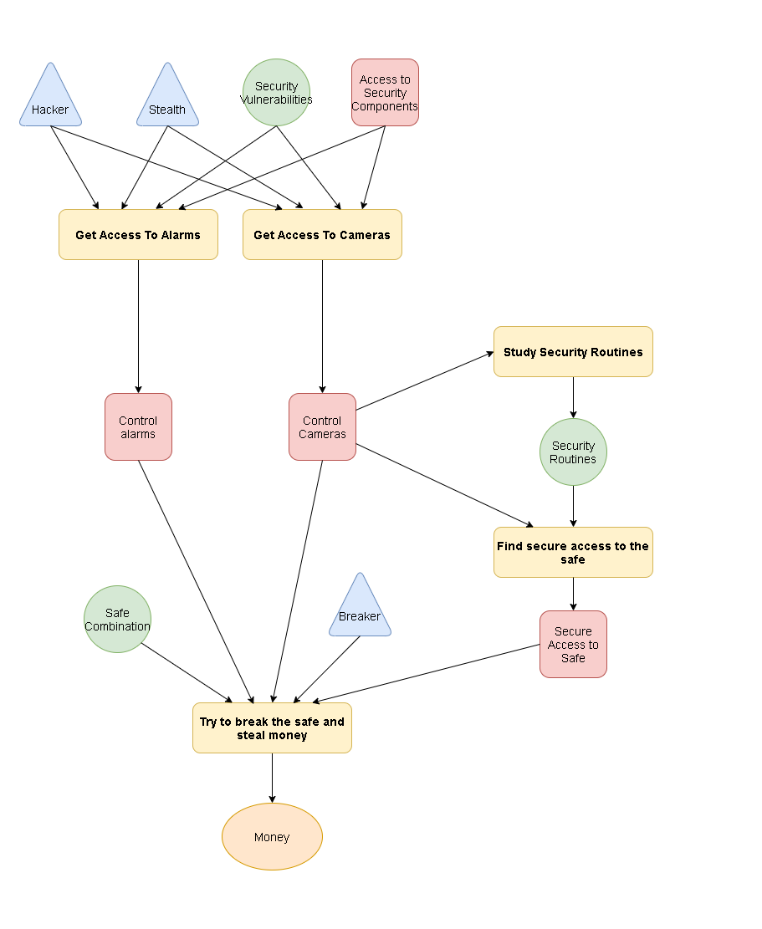
**2 Attacks**

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

Figure 2: AEG model

Immagine che contiene mappa, testo, tavolo, uomo

Descrizione generata automaticamente

**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 → 1.0

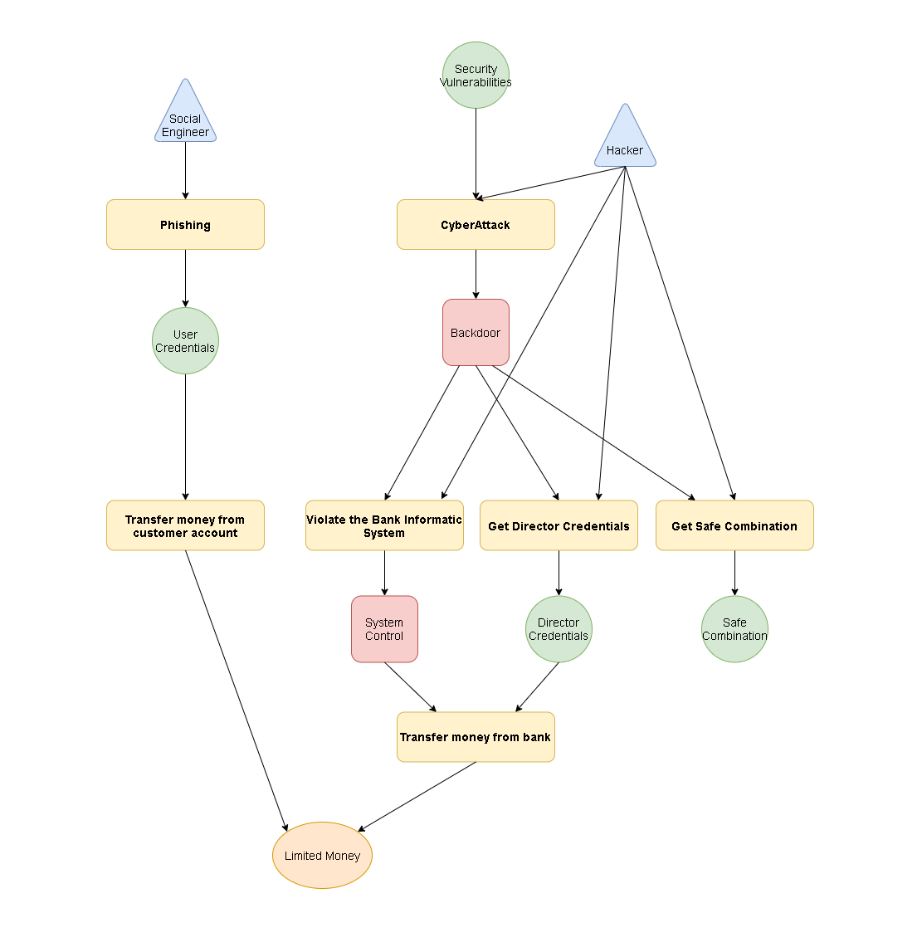
**Detection**: 0 → 0

**Payoff**: 0.6 → 1.0

Figure 3: Physical Attack AEG Model

**Steps:**

* **Get Access To Alarms**
  + **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 alarms secure system to disable them
  + **Cost**: 30
  + **Time**: 5-30m, the requested time depends on the hacker abilities of the attacker
  + **Possible outcomes**: The attack can be concluded with a success(1%) or with a failure(99%). The probability of being detected is high with 30% 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 concluded with a success(1%) or a failure(99%). The probability of being detected is high with 40% in case of failure and 5% in case of a success
* **Study Security Routines**
  + **Preconditions**: The attackers need to control the bank cameras to 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 cameras violation(10%)
* **Find Secure Access To The Safe**
  + **Preconditions**: The attackers need to control the bank cameras to see their content and to know the security guards ruotines
  + **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(5%), a failure(75%) 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. The probability of being detected is 0 of all outcomes except for the detection of the cameras violation(10%)
* **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 step is also extended in combination with the cyber Attack which permits the robbers to obtain the safe combination by violating the bank informatic systems
  + **Cost**: 40(Using safe combination),60(Using a breaker)
  + **Time**: 30(Using safe combination),60(Using a breaker)
  + **Possible** **outcomes**: The attack can be concluded with a success (65%) or with a failure(35%). In case of success the probability of being identified is low (15%) but if the attack fails the robbers will almost certainly identified (95%)

**2.2 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 → 0

**Detection**: 0.4 → 1.0

**Payoff**: 0.6 → 1.0

**Steps:**

Figure 4: Cyber Attack AEG Model

* **Phishing**
  + **Preconditions**: The attackers need social engineering skills to cheat their victims
  + **Description**: The attackers will send tons of mail on every possible customer of the bank with the hope that someone will be cheated and gives him 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(10%) or with a failure(90%), in each case the probability of being detected is 0
* **Transfer Customer Money**
  + **Preconditions**: The attacker needs a customer credential for the bank system
  + **Description**: The attacker using the customer credentials will access to the victim’ account and transfer money into an anonymous one 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% otherwise is 5%
* **Cyber Attack**
  + **Preconditions**: The attackers need to know the vulnerabilities of the system and to have hacking skills to exploit them
  + **Description**: The attacker using a vulnerability will exploit the system and generate a backdoor to perform a deeper attack into the system in a second moment
  + **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 attackers will try to infect the bank system to gain its control
  + **Cost**: 65
  + **Time**: 10-30m
  + **Possible** **outcomes**: The attack can be concluded with a success(5%), a failure(65%) or because the technician has found the backdoor into the system and close it(30%). In the last case the attackers will lose their access. The probability of being detected is the same for each outcome (5%)
* **Get Director Credentials**
  + **Preconditions**: The attackers need a backdoor into the bank system
  + **Description**: The attackers will try to steal the director credential from the bank system
  + **Cost**: 55
  + **Time**: 5-25m
  + **Possible** **outcomes**: The attack can be concluded with a success(5%), a failure(60%) or because the technician has found the backdoor into the system and close it(30%). In the last case the attackers will lose their access. The probability of being detected is the same for each outcome (5%)
* **Get Safe Combination**
  + **Preconditions**: The attackers need a backdoor into the bank system
  + **Description**: The attackers will try to steal the safe combination from the bank system. This attack is very particular because it is useful in conjunction with the Physical Attack to make easier the break of the safe
  + **Cost**: 60
  + **Time**: 5.25m
  + **Possible** **outcomes**: The attack can be concluded with a success(5%), a failure(65%) or because a technician has found the backdoor into the system and close it(30%). The probability of being detected is the 15% in the case the step has failed 5% in all the other outcomes
* **Transfer Bank Money**
  + **Preconditions**: The attackers need to control the bank informatic system or to have the director bank credentials
  + **Description**: The attackers will transfer money from the bank directly into their anonymous accounts
  + **Cost**: 5
  + **Time**: 5m
  + **Possible** **outcomes**: The attack can be concluded with a success(80%) or with a failure(20%). The probability of being detected is the 5% in case of success otherwise 10%

**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 inficiate in a general scenario on the bank security.

**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
  + Immagine che contiene mappa, testo

    Descrizione generata automaticamente**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 have an interval [0,3500] of certain security in which the value money stay always on 0. Teorically if we control periodically the bank cameras and alarms to impairment with a period low than 3500m then the security of the bank to a physical attack is guarantee with a 95% of probability.

**3.2 Cyber Attack**

* **Reward of Interest**
  + **money:** an illegitimate transfer of money has been performe
  + **backdoor:** 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

Immagine che contiene testo, mappa

Descrizione generata automaticamente

How we can see from the graph into the informatic area is easier to steal money. In particular is the phishing techniques the attack which guide the steal of money. And 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 make the phishing a serious problem for a bank. After the phishing we can see that after a reasonable time the system will be compromised or have a backdoor installed on it. The main actions which can be performed from the bank to reduce the problem on cyber attacks has to be localized on find new secure way to prevent phishing attacks to its customers and a periodically control of their system to localize possible backdoors.

**3.3 General Attack**

* **Reward of Interest**
  + **Control\_alarms:** an illegitimate transfer of money has been performed
  + **Control\_cameras:** the bank system has a backdoor installed on it
  + **Security\_routines:** the bank system is under control of an attacker
  + **Safe\_access:** a user bank credential has been stolen
  + **money:** the bank director credentials has been stolen
  + **small\_money:** the safe combination has been stolen
  + **big\_money**
  + **back\_door:**
  + **system\_access:**
  + **user\_credentials:**
  + **dir\_credentials:**
  + **safe\_combination:**

Immagine che contiene testo, mappa

Descrizione generata automaticamente

How we expect in a 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.