CSC 790 A: Project 1
Deception Game v1.0

Due
12:30pm Thursday, 2/20

Project Description

As discussed in class, deception conceals or obscures an entity's existence or attributes so to intentionally mislead adversaries. Several deception methods for computer systems have been developed and researched; examples include address hopping/shuffling, honeypots, and honeynets. One aspect of deception that has not been fully considered is the deployment and subsequent management of these methods. For example given a computer network to protect, what type of deception is best? How often should address shuffling be performed? What is the minimum number of honeypots required to be effective? Will address shuffling and honeypots in combination provide better security? For this project you will develop a mathematical model to analyze the performance of deception to better understand deployment and management. In other words, the best defense strategies for a set of defense and attacker options.

Network and Attacker Description

Assume you are the administrator of a computer network consisting of vulnerable computers (like Fletcher's), secure computers, and empty addresses. The attacker seeks to map your network and find the vulnerable computers using a *scan* which may or may not be followed by an *exploit attempt*. Instead of using specific amounts for the number addresses, number of computer, etc... use variables. We're creating models after all.

- There are n total addresses available to the administrator.
- There are m computers in the network, of which v are vulnerable; therefore $v \leq m \leq n$.
- The attacker is aware of the address space n and seeks to find at least α percent of the v vulnerable computers; therefore, $0 < \alpha \leq 1$.
- The attacker will try k scans of the network to find vulnerable systems.

Available Deception Techniques

Several deception techniques are possible, however this assignment will only consider address shuffling and honeypots. Furthermore to help analysis you can ignore some implementation details however you will still need to consider the revenue and costs (administrative and attacker) of each technique. Revenue and costs are difficult to quantify. Identifying the cost of deployment is possible, although there are fixed costs, variable costs, ... *What is the administrative revenue associated with a successful defense? What is administrative the cost of a failed defense?* One possible solution is to consider utility instead of actual monetary amounts.

Address Shuffling

Address shuffling (or hopping, I can't decide) simply replaces a system's IP address with another. Once this occurs attacker reconnaissance information becomes invalid. An important administrative cost to consider is the loss of legitimate connections.

Honeypots

Honeypots are systems designed to detect unauthorized access. The system mimics an actual computer server and can record the source of an attacker (IP address) and type of exploit. As a result attackers seek to avoid these systems (so there is a high attacker cost). There is also a nontrivial administrative cost associated deploying and managing honeypots.

Models and Games

As previously described, you will develop mathematical models of defense strategies for a computer network. Such models are very useful for predicting the performance of a system that cannot be easily tested empirically. Verifying the model with empirical results an important, and necessary step, but will not be done for this assignment.

What type of model should you consider? We are interested in the likelihood of attacker success and given the amount of chance associated with a scan, probabilistic models are probably best suited. For example the NASR paper modeled the probability of attacker success as $\frac{v}{n}$, which is the probability that attacker will randomly scan one of the v vulnerable machines[1]. This is a start, but this simple equation does not take into account k scans are probably performed. Specifically each scan can provide the attacker knowledge (for example, whether or not to attempt the address again). If no defense is provided and the attacker can attempt n scans, then the probability that the attacker will find v vulnerable computers is 1. The NASR model does not directly provide this insight.

Developing the probability equations for different scenarios is possible, but perhaps a better approach would associate another known model with the network system. *Can the system be modeled as a dice game?* Selecting a computer to scan (attackers point of view) could be modeled as rolling a n sided die, where each side represents an address. Consider the implication of shuffling and how that would map to a dice game. *Can the system be modeled as a card game, a roulette wheel, keno game*[2]*, ...?* Using these known models an equation for the attacker success probability can be determined, *I think.* I hope you will select one model for all the defense strategies.

Applying a Bad Introduction to Game Theory

This project is interested in determining the best defense strategy given a set of attacker strategies. As such, game theory is best suited for determining the best strategies if they are described mathematically (the point of the previous section). You will consider the system as a two player (administrator and attacker), non-cooperative, competitive game.

Player Actions, Payoffs, and Best Strategies

Using game theory you must define the actions (strategies) available to each player. For example depending on the question asked in the assignment, the administrator could have the following strategies: do nothing, address shuffling, or honeypot. The attacker may have the option to do nothing, scan, or scan and attempt exploit. Using this information a *payoff* matrix can be developed where the matrix entries are the payoff values for the defender and attacker. An example payoff matrix is given below.

Admin / Attacker	Static (no deception)	Shuffle	Honeypot
Scan	(E_s^d, E_s^a)	(E_{sh}^d, E_s^a)	(E_h^d, E_s^a)
Scan & Attack	(E_s^d, E_a^a)	(E_{sh}^d, E_a^a)	(E_h^d, E_a^a)

The values E_j^i is the expected payoff for player i using strategy j, for example E_s^d is the expected payoff for the defender using static addressing. This value is dependent on the attacker success probability and can be calculated as

$$E_s^d = (1 - \beta_s) \cdot r_s - \beta_s \cdot c_s$$

where β_s is the probability the attacker is successful given a static defense, r_s is the revenue of the defense, and c_s is the cost of the defense. The remaining expected payoffs can be determined in a similar fashion. Using the completed matrix the best strategies (dominate, Nash-equilbria) can be found, *I hope.*

[1] In all fairness, the NASR paper defended against hitlist attacks, so there were no scans and as a result their simple model is correct. But how was the list acquired?

[2] Maybe not keno, as according to Cody, you never lose in keno.

Project Requirements

The deliverable for this project will be a report describing your model (probabilistic and game) and your answers to the following sections. Your report must be written succinctly and neatly (yes, typeset).

1 Static Addressing

Develop a model to analyze static addressing which is equivalent to no defense. An important part of the model will be the probability of attacker success (β) for finding at least α percent of v vulnerable computers in a network of n addresses and m computers total given k attacker scans. Yes, a lot of variables to consider.

Questions (*15 points*)

You must correctly answer the following questions to receive full credit for this part of the project.

1. What is the equation for attacker success (β) for static addressing? Describe the equation and how it correctly models the system.

2. Assume the attacker only needs to find one vulnerable machine. Graph the attacker success rate as the number of scans (k) increases given a \16 (class B) network, where 25% of the addresses have machines and 10% of these machines are vulnerable. Comment on your results.

3. Provide a 3-D graph of the attacker success rate (z-axis) as the number of scans (k, x-axis) and attacker find percentage increases (α, y-axis). Assume a \16 (class B) network, where 25% of the addresses have machines and 10% of these machines are vulnerable. Comment on your results.

2 Address Shuffling

Develop a model for address shuffling where all n addresses are shuffled. An important part of the model will be the probability of attacker success (β) for finding α percent of v vulnerable computers. Again, the a network consists of n addresses and m computers, and the attacker can perform k scans. In addition your model should consider the frequency of shuffling denoted as γ.

Shuffling frequency does imply a temporal component to the model, which is a non-trivial addition. To simplify your initial analysis, you can consider the frequency to be associated with the scan attempts instead of over fixed time intervals (although you can use intervals if you like, *it might be easier*). Therefore $0 \leq \gamma \leq 1$ where $\gamma = 0$ is static addressing and $\gamma = 1$ is *perfect shuffling* which means the addresses are shuffled after each scan attempt. Therefore with *perfect shuffling* given k scans, k shuffles would occur which provides the best shuffle defense but has a very high cost.

Questions (*25 points*)

You must also correctly answer the following questions to receive full credit for this part of the project.

1. What is the equation for attacker success (β) for perfect address shuffling? Describe the equation and how it correctly models the system.

2. Assume the attacker only needs to find one vulnerable machine and the system is defended with perfect shuffling. Graph the attacker success rate as the number of scans (k) increases given a \16 (class B) network, where 25% of the addresses have machines and 10% of these machines are vulnerable. Compare with static addressing and comment on your results.

3. What is the equation for attacker success (β) for shuffling with frequency γ? Describe the equation and how it correctly models the system.

4. Provide a 3-D graph of the attacker success rate (z-axis) as the number of scans (k, x-axis) and shuffling frequency increases (γ, y-axis). Assume a \16 (class B) network, where 25% of the addresses have machines, 10% of these machines are vulnerable, and the attacker is required to find at least 25% of the vulnerable computers. Comment on your results.

5. An interesting question is how many of the addresses should be shuffled. Would only shuffling vulnerable machines with empty addresses provide the same protection as shuffling the entire network? Defend your position, graphs can help the argument.

3 D-Quan's Dance Groves and Address Shuffling

Researchers from UNCC created a MT system that relies on Software Defined Networks (SDN) to provide a MT defense. One requirement of their approach is that computers must hop/shuffle in a subnet (which is a portion of the complete network). For this part of the assignment, you will create a model of this approach to determine the defense performance, then compare it to a more traditional notion of address shuffling (defined in the previous section).

Assume the address space consists of n addresses and are divided into s equal subnets. In addition, assume that each subnet will consist of the same number of computers, $\frac{m}{s}$, and vulnerable $\frac{v}{s}$ per subnet, where m and v are multiples of s (so everything divides evenly). Develop a model for subnet address shuffling where all n addresses are shuffled. An important part of the model will be the probability of attacker success (β) for finding α percent of v vulnerable computers. Again, the attacker can perform k scans. In addition your model should consider the frequency of shuffling denoted as γ.

Questions (*15 points*)

You must also correctly answer the following questions to receive full credit for this part of the project.

1. What is the equation for attacker success (β) for D-Quan's perfect address shuffling? Describe the equation and how it correctly models the system.

2. Assume the attacker only needs to find one vulnerable machine and the system is defended with perfect shuffling. Graph the attacker success rate as the number of scans (k) increases given a \16 (class B) network, where 25% of the addresses have machines and 10% of these machines are vulnerable. Compare with static addressing and traditional (no subnet) shuffling, then comment on your results.

3. Is this method better, worse, or the same as traditional shuffling? Are your results consistent with the results reported in the UNCC paper?

4 Honeypot

Develop a model for honeypots. In this system the attacker must avoid honeypots, if a honeypot is contacted the attack must stop (very high cost to the attacker). Therefore an important part of the model will be the probability of attacker success (β) for finding α percent of v vulnerable computers using k scan without contacting any honeypots. This will depend on the number of honeypots deployed which will be denoted as h, where $m + h \leq n$.

Questions (*30 points*)

You must also correctly answer the following questions to receive full credit for this part of the project.

1. What is the equation for attacker success (β) for h honeypots? Describe the equation and how it correctly models the system.

2. Assume the attacker only needs to find one vulnerable machine and the system is defended with honeypots. Graph the attacker success rate as the number of honeypots (h) increases given a \16 (class B) network, where 25% of the addresses have machines, 10% of these machines are vulnerable, and the attacker is allowed to scan 10% of the network. Compare with no defense and shuffling, then comment on your results.

3. Provide a 3-D graph of the attacker success rate (z-axis) as the number of scans (k, x-axis) and number of honeypots increases (h, y-axis). Assume a \16 (class B) network, where 25% of the addresses have machines, 10% of these machines are vulnerable, and the attacker is required to find at least 25% of the vulnerable computers. Comment on your results.

5 Shuffle or Honeypots

The probabilities of success for the different defenses can be used to determine the expected payoffs, and complete the payoff matrix. The matrix can then identify the best defense (or attack) strategy given the alternatives. As described earlier, an important part for developing the matrix will be to identify utility values for defenses and attacks. Using a generic security credit, instead of `US AMERICAN DOOLARS`, can simplify this process. If you decide to take this approach you will need to justify the various values associated with deploying defenses, attempting an attack, attacker success, and defender loss, etc...

Questions (*15 points*)

You must also correctly answer the following questions to receive full credit for this part of the project.

1. Assign revenue and cost variables for the different attacks and defenses, then determine the payoff equations and complete the matrix.
2. Make realistic assumptions about the comparative revenue and costs (for example shuffling is less expensive than honeypots) and determine the best strategies. Comment on your results, note graphs help.

Solutions

1.1

In this mathematical model, we need to assume that αv is an integer and $k \geq \alpha v$.
So, the whole question is equivalent to this: consider that there are n candy boxes in total (the IP address space), m of which have candies inside (each box contains either only one candy or is empty). There are two kinds of candies among them, the red ones (the vulnerable computers, with the number v) and the green ones (the secure computers, with the number $m-v$). Now, a boy randomly picks k boxes and only those red candies can meet his interest because he is so naughty (attacker), so those boxes contain green candies are the same with those empty boxes to him (IP addresses associated with secure computers and no computers are the same to the attacker). His choice space is $\binom{n}{k}$, suppose $x(0 \leq x \leq k)$ of his picks have red candies, then the target space is $\binom{v}{x}\binom{n-v}{k-x}$. To make this naught boy happy, there must be at least αv red candies, thus the possibility β that he is happy (attacker success) is:

$$\beta = \sum_{x=\alpha v}^{\min(k,v)} \frac{\binom{v}{x}\binom{n-v}{k-x}}{\binom{n}{k}}.$$

1.2

Here, $n = 2^{16} - 2 = 65534$, $m = \frac{n}{4} = 16383.5$, $v = \frac{m}{10} = 4096.875 \doteq 4097$ and $\alpha v = 1$, in R we have:

1.3

In R we have:

2.1

For the perfect shuffling where $\gamma = 1$, now we have k shuffles, each shuffle after each scan.

Using the same analog we stated in the question 1.1, the naughty boy will play the "seeking for red candies" game k times, but instead of picking all k boxes at the same time in one game, he will pick only one box at each one game and he is given n brand new boxes at each game. Since the number of red candies at each game are always v, thus the possibility of the boy gets a red candy at each game is $\frac{v}{n}$, then the possibility that he get x red candies in those k games is $\binom{k}{x}(\frac{v}{n})^x(1-\frac{v}{n})^{k-x}$. Still, at least αv red candies can make him happy, thus:

$$\beta = \sum_{x=\alpha v}^{\min(k,v)} \binom{k}{x}(\frac{v}{n})^x(1-\frac{v}{n})^{k-x}.$$

2.2

Here, $n = 2^{16} - 2 = 65534$, $m = \frac{n}{4} = 16383.5$, $v = \frac{m}{10} = 4096.875 \doteq 4097$ and $\alpha v = 1$, in Matlab we have:

2.3

With shuffling frequency γ, then we will perform γk shuffles during the attacker's k scans, thus we will perform one shuffle after $\frac{k}{\gamma k} = \frac{1}{\gamma}$ scans. During each $\frac{1}{\gamma}$ scans before the next shuffling, the possibility that the attacker will get x vulnerable computers is: $\frac{\binom{v}{x}\binom{n-v}{\frac{1}{\gamma}-x}}{\binom{n}{\frac{1}{\gamma}}}$, thus the final total number of the vulnerable computers the attacker can get in the end is the sum of those x_is ($1 \leq i \leq \gamma k$) from each $\frac{1}{\gamma}$ scans, then the attacker success β is:

$$\beta = \sum_{x_{\gamma k}=1}^{\min(k,v,\frac{1}{\gamma})} \cdots \sum_{x_2=1}^{\min(k,v,\frac{1}{\gamma})} \sum_{x_1=1}^{\min(k,v,\frac{1}{\gamma})} \prod_{i=1}^{\gamma k} \frac{\binom{v}{x_i}\binom{n-v}{\frac{1}{\gamma}-x_i}}{\binom{n}{\frac{1}{\gamma}}}, where \sum_{1}^{\gamma k} x_i \geq \alpha v$$

2.4

...

2.5

Shuffling the entire network provide more protection. In the equation of question 2.3, only shuffling vulnerable machines with empty addresses will make the denominator smaller, hence the attacker success will become bigger, thus shuffling the entire network is better.

3.1

Assume for each subnet i, $1 \leq i \leq s$,

$$\beta = \sum_{x_{\gamma k}=1}^{\min(k,v,\frac{1}{\gamma})} \cdots \sum_{x_2=1}^{\min(k,v,\frac{1}{\gamma})} \sum_{x_1=1}^{\min(k,v,\frac{1}{\gamma})} \prod_{i=1}^{\gamma k} \frac{\binom{v}{x_i}\binom{n-v}{\frac{1}{\gamma}-x_i}}{\binom{n}{\frac{1}{\gamma}}}, where \sum_{1}^{\gamma k} x_i \geq \alpha v$$

3.2

3.3

4.1

First of all, we want to know the possibility that the attacker performed k scans without contacting any honeypots:

$$P(k - scans - without - honeypots) = \frac{\binom{n-h}{k}}{\binom{n}{k}}.$$

Thus,

$$\begin{aligned}
\beta &= P(find - \alpha v - vulnerablecomputers | k - scans - without - honeypots) P(k - scans - without - honeypots) \\
&= \sum_{x=\alpha v}^{\min(k,v)} \frac{\binom{v}{x}\binom{n-h-v}{k-x}}{\binom{n-h}{k}} \frac{\binom{n-h}{k}}{\binom{n}{k}} \\
&= \sum_{x=\alpha v}^{\min(k,v)} \frac{\binom{v}{x}\binom{n-h-v}{k-x}}{\binom{n}{k}}.
\end{aligned}$$

4.2

4.3