Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence (AAAI-17)

Optimal Personalized Defense Strategy Against Man-In-The-Middle Attack

Xiaohong Li and **Shuxin Li**
School of Computer Science and Technology
Tianjin University, China
{xiaohongli,lishuxin}@tju.edu.cn

Jianye Hao* and **Zhiyong Feng**
School of Computer Software
Tianjin University, China
{jianye.hao,zyfeng}@tju.edu.cn

Bo An
School of Computer Engineering
Nanyang Technological University, Singapore
boan@ntu.edu.sg

Abstract

The Man-In-The-Middle (MITM) attack is one of the most common attacks employed in the network hacking. MITM attackers can successfully invoke attacks such as denial of service (DoS) and port stealing, and lead to surprisingly harmful consequences for users in terms of both financial loss and security issues. The conventional defense approaches mainly consider how to detect and eliminate those attacks or how to prevent those attacks from being launched in the first place. This paper proposes a game-theoretic defense strategy from a different perspective, which aims at minimizing the loss that the whole system sustains given that the MITM attacks are inevitable. We model the interaction between the attacker and the defender as a Stackelberg security game and adopt the Strong Stackelberg Equilibrium (SSE) as the defender's strategy. Since the defender's strategy space is infinite in our model, we employ a novel method to reduce the searching space of computing the optimal defense strategy. Finally, we empirically evaluate our optimal defense strategy by comparing it with non-strategic defense strategies. The results indicate that our game-theoretic defense strategy significantly outperforms other non-strategic defense strategies in terms of decreasing the total losses against MITM attacks.

Introduction

While the World Wide Web brings the convenience for people, it has also brought in an immense risk of cyber attacks. Especially, more and more transactions are done online ranging from home banking, e-commerce, and e-procurement to those that involve sensitive information. The leak of those sensitive information might result in tremendous loss to users in terms of both finance and privacy. One of the major types of attacks to intercept sensitive information is the Man-In-The-Middle (MITM) attack.

Nowadays, the MITM attack has penetrated into our daily life. Recent news points out that 95% of HTTPS servers are vulnerable to trivial MITM attacks (Mutton 2016). Some incidents like the github in China (Martin 2013) and the MITM attack against google in Iranian (Seth Schoen 2011) indicate the endangerment of the MITM attacks. Meanwhile, attackers also commit MITM attacks in Internet of Things (IoT). There have been reported cases where hackers attacked connected intelligent devices within smart cars (Simko 2016). MITM attacks usually exhibit two major characteristics: 1) invisibility: very difficult to detect if it only sniffs information and does not take other obvious actions (Kapil M, Manoj V, and Jay L 2016); 2) targeted attack: an MITM attack usually only targets at a carefully selected set of users due to resource limitations (Gangan 2015).

At present, there are many technologies to launch MITM attacks, such as DNS poisoning, denial of service (DoS), and https sniffing through fake SSL certificate (Nayak and Samaddar 2010). The current defense technologies against MITM attacks can be classified into two categories. The first is encryption, which aims at increasing the difficulty of decoding packets by applying complicated encryption algorithms (Albina et al. 2013). The second is to design effective detection techniques and corresponding countermeasures. The major research efforts focus on detection techniques, such as the method of certificate validation (Dacosta, Ahamad, and Traynor 2012) and using the characteristic of TCP packet (e.g., timestamp) (Vallivaara, Sailio, and Halunen 2014). The measures taken after detection are relatively straightforward, such as enhancing the defense for weak points and invoking reconnection. To summarize, all the above work aims at either minimizing the attack success rate or maximizing detection rate.

However, few work considers the problem of how to decrease the loss under the MITM attacks from the system's perspective. Since complete elimination of the MITM attacks seems an impossible task, we revisit the MITM attack defending problem by addressing the following question: how can we minimize the total losses within a system, given that MITM attacks are inevitable? We model this problem as the strategic interaction between the MITM attacker and the defender under the Stackelberg game-theoretic framework. We show that computing the optimal defense strategy can be transformed equivalently into calculating the Strong Stackelberg Equilibrium (SSE) of the underlying Stackelberg game. However, the traditional searching techniques (e.g., integer/linear programming) can be computationally inefficient since the defender's strategy space is N-dimensional and infinite in our model. Therefore, we employ a novel method to compute the optimal personalized defense strategy by reducing the searching space to one di-

*corresponding author

mension. In order to demonstrate the performance of our defense strategy, extensive experiments are performed by comparing with other non-strategic strategies. The results show that our strategy significantly outperforms other strategies in decreasing the system's overall losses.

Background

Security Game Theory

In the last decade, significant research efforts have been devoted to employ security game theory to protect critical infrastructures with limited resources against physical attacks (Jain et al. 2010; Shieh et al. 2012; An et al. 2012; Kiekintveld, Islam, and Kreinovich 2013). Recently, several works apply security game theory to address the cyber attack defense problem. One representative example is applying the Stackelberg game to solve the spear-phishing attack(Laszka, Vorobeychik, and Koutsoukos 2015; Zhao, An, and Kiekintveld 2015; Laszka, Lou, and Vorobeychik 2016).

The model we adopt here to model the strategic interaction between a defender and an attacker is the Stackelberg security game. A Stackelberg game is a two-player extensive game with perfect information in which a defender chooses an action from a set A_1 and an attacker, informed of the defender's choice, chooses an action from a set A_2 (Osborne and Rubinstein 1994). The solution usually applied to Stackelberg games is called Strong Stackelberg Equilibrium (SSE) (Korzhyk et al. 2011). A strategy profile is a SSE if it satisfies both the defender and the attacker play their best responses and the attacker chooses actions in the best interest of the defender in case of a tie. Here, we adopt the SSE solution and refer to the defender's equilibrium strategy in SSE as its optimal strategy in the remainder of the paper.

Man-In-The-Middle Attack

An MITM attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of MITM attacks is active eavesdropping, in which an attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, while in fact the entire conversation is controlled by the attacker. The attacker is able to intercept all relevant messages passing between the two parties.

The Server/Client model is the major communication framework employed in current computer networks, and the servers are the major targets of the MITM attackers. Each type of services is usually associated with a default port of server, and any client in request of the particular service exchanges packets with the server through the default port. For example, port 80 is usually assigned for providing web service. An attacker usually attacks the default port of a particular service purposely and obtains all information exchanged. The commonly adopted defense approach is to detect the attack and take countermeasures accordingly. The detection methods mainly focus on certificate validations, for example, determining whether the server certificate received matches the legitimate certificate (Huang et al. 2014). Other detection methods may utilize the difference of characteristics under the attack, such as the timestamps of TCP packet headers (Vallivaara, Sailio, and Halunen 2014). After an MITM attack is detected, the countermeasures, such as enhancing the vulnerability and invoking reconnection are usually taken accordingly. Another line of defense approaches is to resort to the complicated encryption algorithms and take safety measures in key exchange (Kumar et al. 2012). Recently the idea of port hopping is proposed to confuse the attacker (Luo, Wang, and Cai 2014), which dynamically maps a service's port to an unused pseudo-random ports.

In summary, all previous work aims at either minimizing the attack success rate or maximizing detection rate. However, none of the existing work considers the problem of minimizing the attack loss given the fact that it is impossible to eliminate the MITM attack completely. To this end, here we revisit the problem from a different perspective by attempting to answering the following question: how the total losses of a system can be minimized given that the MITM attacks are inevitable? Our approach thus complements the existing MITM attack defense approaches.

Game-theoretic Modeling

Following the setting in (Luo, Wang, and Cai 2014), we classify all available ports into different groups by the type of service it can provide. For each service s, there exists a corresponding set S_s of ports available for providing this service. Note that although each service is usually associated with a port by default, a service can be provided by multiple ports using the technology of port hopping. In our model, we only focus on one group of ports that provide one particular service, and the other group of ports for other services can be analyzed similarly. For all the users in request of the same service s, we attempt to distribute them to different ports within the group S_s. To make the model description clear, we assume that each port provides service to only one user, which, however, can be easily extended to the case of multiple clients sharing one port. Different from the port hopping approach, we aim at designing an effective defense strategy to minimize the total losses of all users in request of the same service in the system in case MITM attacks occur. Note that an attacker practically can only launch the MITM attack against a selected set of ports due to its capacity limitations (Luo, Wang, and Cai 2015).

Since an attacker is mainly interested in obtaining the sensitive information, one natural way of avoiding users' information from being acquired and further exploited is to insert some noise packets during communication to confuse the attacker. When an attacker is faced with the mix of valid and noise packets, the difficulty of obtaining useful information increases accordingly. Intuitively, the higher percentage of inserted noise packets, the less useful information that the attacker can obtain. This would also result in the side effect of additional communication delay to the users, which is also modeled and explained later.

Formally, for each port we propose that noise packets are inserted to the original valid packets at a certain frequency. Each port's frequency of inserting noise packets determines

the probability of the attacker retrieving the useful information from this port given that the communication protocol has been attacked successfully. The higher frequency f the noise packets are inserted at, the lower probability p that useful information an attacker can obtain. Here, we adopt the simplest linear form of $f = 1 - p$, under which the probability of obtaining the useful information is 1 when no noise packets is inserted and vice versa. However, it is straightforward to extend this assumption by taking into consideration the effect of employing any existing encryption techniques.

On the other hand, inserting noise packets during communication would result in certain communication delay. We use $q \in [0, 1]$ to denote the extent of losses caused by communication delay, which is determined by the frequency f of inserting noise packets during communication. The higher frequency f of inserting noise packets, the lower percentage of useful packets a user can exchange within a fixed time period and thus the greater losses it would suffer from.

The relationship between the probability p of obtaining useful information and the extent of losses q caused by communication delay can be represented by a function $F(p) : [0, 1] \mapsto [0, 1]$, which can be obtained through empirical simulations. Intuitively, if there are no noise packets during communication, then there should be no additional delay caused by the noise injection mechanism. Conversely, if all packets are noise data, it indicates that the user suffers the maximum degree of losses. Therefore we set the value of q to 0 and 1 when the value of p is 1 and 0, respectively. For those non-extreme cases, the longer communication time results in the greater extent of losses. Therefore we compute the value of q according to the required communication time. Suppose that the amount of information that a user exchanges is unchanged. By varying the probability p between the range of [0,1], we can get the communication time corresponding to every probability p through simulation. After that, the communication times are normalized to the range of [0,1], which can be estimated as the extent of losses caused by communication delay. Figure 1 gives an example of the relationship between p and q, in which $F(p)$ is a non-increasing function of p. For analytical tractability, in the following analysis, we assume that $F(p)$ is a continuous, strictly decreasing, and strictly convex function of p.

If an attacker successfully launches the MITM attack against port i, we use v_i to represent the utility gain of the attacker, i.e., the value of information that the user exchanges with server through port i. The value of v_i is mainly determined by the user's relative social level and status among all users in the organization. Similarly, we use c_i to denote the cost inflicted on the user using port i if valid information is not be exchanged with server side timely.

Stackelberg security game modeling

In practice, for an attacker, sophisticated investigations on the currently deployed defense strategy are usually conducted before a personalized attack is launched. Therefore, it is reasonable to assume that the defender's strategy is priori known to the attacker before an attack is launched. To this end, we model the interaction between the MITM attacker and the defender as a two-player Stackelberg security game.

In this model, the attacker's strategic choice is to select a subset S of ports from which he intercepts valuable information. Considering the capacity limitation (time and computational resources) of the attacker, we assume that the attacker can only select a limited number of ports to attack. Formally, we model this limitation by assuming that the attacker's strategy has to satisfy $|S| \leq K$, where K is a constant. The defender's strategic choice is to determine the probability p_i for each port i, which is denoted as vector $\mathbf{P}$.

Given a strategy profile ($\mathbf{P}$, S), the attacker's payoff can be defined as follows,

$$U_{\text{attacker}} = \sum_{i \in S} p_i v_i \tag{1}$$

and the defender's loss (i.e., the inverse of its payoff) is the sum of all ports' losses. Formally, the loss of an attacked port i is defined as follows,

$$l_i^A = p_i v_i + F(p_i) c_i \tag{2}$$

and the loss of a port i which is not under attacked is defined as follows,

$$l_i^N = F(p_i) c_i. \tag{3}$$

Finally, we have the defender's loss defined as follows,

$$L_{\text{defender}} = \sum_{i \in S} l_i^A + \sum_{i \notin S} l_i^N \tag{4}$$

$$= \sum_{i \in S} p_i v_i + \sum_{i \in N} F(p_i) c_i \tag{5}$$

$$= U_{\text{attacker}} + \sum_{i \in N} F(p_i) c_i \tag{6}$$

where N is the set of all ports.

Our goal is to identify the optimal defense strategy given that the attacker always makes the best response. In case of ties, the attacker might break it arbitrarily. However, from our model (Equation (1) and (6)), we know that no matter how the attacker break the ties, all of them would yield the same payoffs for the defender. This indicates breaking ties randomly is equivalent with breaking ties optimally towards the defender. Thus, this is equivalent with finding the Strong Strakelberg Equilibria (SSE) of the Stackelberg game.

Analysis

Since we need to find the SSE of the underlying Stackelberg game, a natural approach is to employ backward induction. In this way, we need to compute the best response for the attacker under every defense strategy, and then the defender selects a defense strategy which can minimize its loss among all possible strategies based on the attacker's best response. However, the set of defender's strategy is infinite in our model. It is practically infeasible to search for the optimal strategy in the above manner. This problem might also be tackled using mixed integer linear programing, which, however, might be computational expensive when the game size becomes too large. To this end, we propose a new and

efficient algorithm to compute the optimal strategy. We begin with characterizing an attacker's best response.

An attacker's best response is the strategy that maximizes his payoff. From the attacker's payoff function in Equation (1), we can easily know that, against a given defense strategy, the attacker's best response is to choose a set S of ports with the highest $p_i v_i$ values.

All the symbols used in our model are listed in Table 1 for convenience purpose. From the Table 1, we can know that for each port i, p_i^A and p_i^T are the values at which the minima of l_i^A and l_i^N are attained, respectively. From Equations (2) and (3), it is straightforward to know that these values are well-defined and unique for each port. The analysis for the defender's optimal strategies will be described in the following sections.

Table 1: symbols of our model

Symbol	Description
p_i	probability of getting the useful information from the port i
$F(p_i)$	extent of losses caused by communication delay when using the port i
v_i	value of the information of the user who use the port i
c_i	cost inflicted on the user using port i if valid information is not be received by the server side timely
l_i^A	expected losses of port i which is be attacked
l_i^N	expected losses of port i which is not be attacked
p_i^A	optimal value of p_i given that the port i is attacked
p_i^N	optimal value of p_i given that the port i is not be attacked

Optimal Defense Subproblem

Firstly, we study an important subproblem of finding an optimal defense strategy by assuming that the attacker's best response is already given. Recall that the attacker's best response is a set S of ports with the highest $p_i v_i$ values. So we restrict our search space to defense strategy in which the ports in S have the highest $p_i v_i$ values. Let's consider a special case in which the parameter values of the ports in S differ substantially from those of the remaining ports.

Proposition 1. *Suppose that the set S which is the best-response strategy for the attacker is given, and the defender's objective is to select an optimal strategy against the set S. If $\min_{i\in S} p_i^A v_i \geq \max_{i\notin S} p_i^N v_i$, then the optimal defense strategy against S is choosing p_i^A for every $i \in S$ and choosing p_i^N for every $i \notin S$.*

Proof. Firstly, the set S is the best-response strategy for attacker, so the ports in S have the highest $p_i v_i$ values. The formula form is $\min_{i\in S} p_i v_i \geq \max_{i\notin S} p_i v_i$. Next, the p_i^A is the optimal value for each port $i \in S$ and the p_i^N is the optimal value for each port $i \notin S$ by the defined above. According to the condition, p_i^A and p_i^N satisfy $\min_{i\in S} p_i^A v_i \geq \max_{i\notin S} p_i^N v_i$. Finally, the defender's loss is the sum of losses for every ports. So the defense strategy in Proposition 1 must be optimal for the given set S. □

Proposition 1 computes the optimal strategy given that the attacker's best-response strategy is known. Both sides' strategies are the best responses. So it is obvious that the strategy profile (i.e., the defender's strategy $\mathbf{P}$ given by Proposition 1 and the attacker's strategy S) is a unique Nash equilibrium in simultaneous version of the game. But in our Stackelberg game model, this Nash equilibrium is not necessarily a Strong Stackelberg Equilibrium. Proposition 1 just describes a special case. Next, we move to consider the general case and provide necessary conditions on the optimal defense strategy.

Theorem 1. *Suppose that the set S which is the best-response strategy for the attacker is given, and the defender's objective is to select an optimal strategy against the set S. Then, in an optimal defense strategy there exist a value λ such that*

- *for every $i \in S$, if $p_i^A v_i < \lambda$, then $p_i v_i = \lambda$; otherwise, $p_i = p_i^A$.*
- *for every $i \notin S$, if $p_i^N v_i > \lambda$, then $p_i v_i = \lambda$; otherwise, $p_i = p_i^N$.*

Proof. From the proof of Proposition 1, we know that $\min_{i\in S} p_i v_i \geq \max_{i\notin S} p_i v_i$ is a necessary and sufficient condition for S to be the best-response strategy. Now, let $\lambda = \max_{i\notin S} p_i v_i$. Firstly, if the port i is attacked, i.e., i is in the set S. According to the necessary and sufficient condition for best-response strategy, the value of $p_i v_i$ ca not be less than λ. So, if $p_i^A v_i > \lambda$, and by the definition of p_i^A, then $p_i = p_i^A$ is the optimal choice for port i. But when $p_i^A v_i < \lambda$, using the convexity of $F(p)$, it can be seen that $p_i v_i = \lambda$ is the optimal choice for port i.

Next, if the port i is not be attacked, i.e., i is not in the set S. Similarly, the value of $p_i v_i$ ca not larger than λ. So, if $p_i^N v_i < \lambda$, and following the definition of p_i^N, then $p_i = p_i^N$ is the optimal choice for port i. But when $p_i^N v_i > \lambda$, Recall that $l^N = F(p_i)c_i$ and $F(p)$ is a decreasing function. It can be seen that $p_i v_i = \lambda$ is the optimal choice for port i. □

Following the above theorem, we can find the optimal λ value for any given set S using searching techniques. In more detail, we can seek an optimal defense strategy by solving each defense subproblem over all K-sized subsets of the ports. However, in practice, this is infeasible due to the extensive search space. Next we provide an efficient and feasible approach in finding an optimal defense strategy.

Optimal Defense Strategy

The following theorem describes how to compute an optimal strategy given that the value of λ is known.

Theorem 2. *Suppose that λ is given, and the defender's optimal strategy is a strategy that satisfies $\min_{i \in S} p_i v_i \geq \lambda$ and $\max_{i \notin S} p_i v_i \leq \lambda$ against the set S which is the best response for attacker. The output of the following algorithm is an optimal defense strategy.*
1. Compute l_i^N for every port i as follows: if $p_i^N v_i < \lambda$, then $l_i^N = F(p_i^N)c_i$; otherwise, $l_i^N = F(\frac{\lambda}{v_i})c_i$.
2. Compute l_i^A for every port i as follows: if $p_i^A v_i > \lambda$, then $l_i^A = p_i^A v_i + F(p_i^A)c_i$; otherwise, $l_i^A = \frac{\lambda}{v_i} v_i + F(\frac{\lambda}{v_i})c_i$.
3. Compute D_i for every port i as follows: $D_i = l_i^A - l_i^N$.
4. Select the set S of ports with the lowest D_i values.
5. For every $i \in S$, if $p_i^A v_i > \lambda$, then $p_i = p_i^A$; otherwise, $p_i = \frac{\lambda}{v_i}$.
6. For every $i \notin S$, if $p_i^N v_i < \lambda$, then $p_i = p_i^N$; otherwise, $p_i = \frac{\lambda}{v_i}$.

Proof. Firstly, suppose that the attacker's best response S is also given. Then this situation is similar to Theorem 1. According to the proof of Theorem 1, we can learn that the Steps 5 and 6 of the above algorithm ensure that the output is an optimal defense strategy against S.

Next, we need to determine whether Steps 1 to 4 yield an optimal set S. Let us prove it using the reduction to absurdity. Suppose that there exists a set S^* that results in the lower expected losses. Since we know that Steps 5 and 6 give an optimal assignment for any given set, we can assume that the defense strategies corresponding to the sets S and S^* are given by Steps 5 and 6. Let i^+ be the set of ports that are in S^* but not in S, and let i^- be the set of ports that are in S but not in S^*. Now, the expected loss of defender corresponding to the sets S and S^* is $L_{\text{defender}} = \sum_{j \in S} l_j^A + \sum_{j \notin S} l_j^N$ and $L^*_{\text{defender}} = \sum_{j \in S^*} l_j^A + \sum_{j \notin S^*} l_j^N$ respectively. Then compute the difference ΔL .

$$
\begin{aligned}
\Delta L &= L_{\text{defender}} - L^*_{\text{defender}} \\
&= \sum_{j \in S} l_j^A - \sum_{j \in S^*} l_j^A + \sum_{j \notin S} l_i^N - \sum_{j \notin S^*} l_j^N \\
&= \sum_{j \in i^-} l_j^A - \sum_{j \in i^+} l_j^A + \sum_{j \in i^+} l_j^N - \sum_{j \in i^-} l_j^N \\
&= \sum_{j \in i^-} l_j^A - \sum_{j \in i^-} l_j^N - (\sum_{j \in i^+} l_j^A - \sum_{j \in i^+} l_j^N) \\
&= \sum_{j \in i^-} D_j - \sum_{j \in i^+} D_j
\end{aligned}
$$

From Steps 4, we know that the ports in the set S have the lowest D_i values. So, we learn that $\sum_{j \in i^-} D_j - \sum_{j \in i^+} D_j < 0$. Then, $\Delta L < 0$ and $L_{\text{defender}} < L^*_{\text{defender}}$. This contradicts the assumption that the set S^* results in the lower expected loss than S; therefore, the original claim must hold. □

We represent the minimum loss that the defender can achieve for a given λ value using the symbol $L_{\text{defender}}(\lambda)$. Theorem 2 shows that we have reduced the problem of finding an optimal defense strategy to the problem of searching the optimal value of λ which minimizes $L_{\text{defender}}(\lambda)$. Given the optimal value of λ, we can easily compute the optimal defense strategy $\mathbf{P}$ following Step 5 and 6 in Theorem 2.

Experimental Evaluations

The goal of experiments is to demonstrate the practical feasibility of our approach and to show that it outperforms non-strategic solutions in term of decreasing the losses.

Finding Optimal Defense Strategy

In the previous section, we have shown that the problem of finding an optimal defense strategy can be reduced to the problem of searching the optimal value of λ which can minimize $L_{\text{defender}}(\lambda)$. Therefore, the key problem is to find the optimal value of λ, which requires computing the value of p_i^A and p_i^N first.

We should obtain the relationship between p and q (i.e., the function $F(p)$) through simulations before computing the value of p_i^A and p_i^N. In the simulation, the communication protocol that we adopt is the Hyper Text Transport Protocol(HTTP) and the contents of packets are stochastic words. Note that the time of generating packets is not considered. After that, we only need to record the corresponding communication time by varying the probability p within the range of [0,1]. Finally, the function curve of $F(p)$ can be obtained after normalizing the communication times to the range of [0,1], and one example is illustrated in Figure 1.

After obtaining the function $F(p)$, the next step is to compute the value of p_i^A and p_i^N. Since $F(p)$ is a decreasing function and $p \in [0, 1]$, we know that $p_i^N = 1$ would be optimal for all the ports whatever the value of c_i is on the basis of Equation 3. Different from p_i^N, the value of p_i^A can be represented as $\arg\min_p (pv_i + F(p)c_i)$. Given that the function $F(p)$ is given by a set of data points and the overall function is convex, it allows us to compute the value of p_i^A by exhaustive search.

Finding the optimal value of λ is the last challenge. Figure 2 shows how the defender's expected loss changes as a function of λ following the procedures in Theorem 2, which is obtained by sampling sufficient amount of data points. The two curves correspond to the settings of c_i and v_i following the power law distribution and normal distribution, respectively. From Figure 2, we can see that the function is relatively smooth in practice. Therefore, we can use an exhaustive search to find the minimum point of λ. After finding the optimal value of λ, we can easily acquire the optimal defense strategy by following the steps of Theorem 2.

Performance Comparision

In this section, we compare our defense strategy with a number of general defense strategies. We first introduce how a set of 30 user profiles are generated. Recall that the value of v_i can be determined by the user's relative social level and status among all users in the organization. To make it concrete, we consider the following two different cases. In the first case, we assume that the values of v_i follow the power

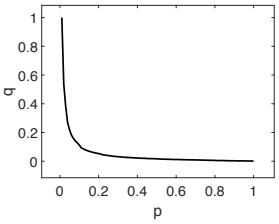


Figure 1: The relationship between p and q (F(p))

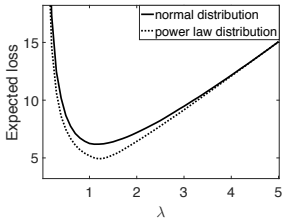


Figure 2: Expected loss as a function of λ for K = 3

law distribution. The motivation behind this hypothesis is the ubiquitous hierarchical structure in organizations (Griffin 2016). Very few people have high social status in terms of power, while the social status of most people is relatively low. In the second case, there are relatively few people who have very high or very low social status, while most people share similarly middle levels of social status. This naturally fits the normal distribution.

The value of c_i is closely related with the characteristic of the user's current job at hand. The more urgent a user i's current job is, the larger value of c_i can be assigned to the user. Since each user may have different jobs at hand, we assume that the values of c_i may also follow either normal or power law distribution. However, there may not necessarily exist any correlation between c_i and v_i. We perform the experiments under two different cases: 1) the parameter of the distribution of c_i follows the same setting as that of v_i; 2) the parameter of the distribution of c_i follows a different setting as that of v_i.

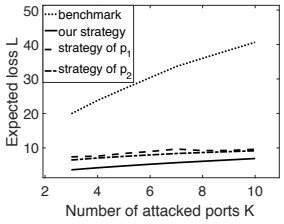
Now, we study the major question regarding our results: can our strategic defense strategy (i.e., $\mathbf{P}$) decrease the expected total amount of losses? To answer this question, we compare our strategic strategy with other non-strategic strategies with uniform probability for each port. One extreme non-strategic strategy is to assign uniform probability $p = 1$, in which it is equivalent with the defenseless status since no noise package is injected. We set this strategy as the benchmark strategy. Another extreme strategy is to set p to 0, which indicates no useful packets are transmitted and thus is not compared. Additionally, we compare our strategic defense strategy with two non-strategic strategies as follows.

The first strategic defense strategy assumes that the attacker attacks the ports uniformly at random. Given this hypothesis, the defender computes the optimal value of p to minimize its expected loss. Formally, the optimal value of p_1 is computed as follows,

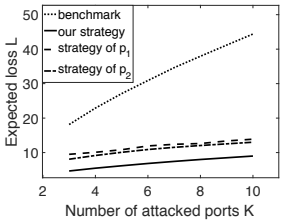
$$\arg\min_{p} \left(\frac{K}{|i|} \sum_{i \in N} v_i \right) p + F(p) \sum_{i \in N} c_i.$$

The second defense strategy assumes that the attacker only targets at the ports with the highest value of information value. Hence, the value of p_2 is computed as follows,

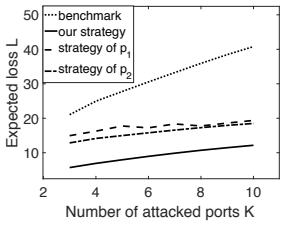
$$\arg\min_{p} \left(\max_{S:|S|=K} \sum_{i \in S} v_i \right) p + F(p) \sum_{i \in N} c_i.$$



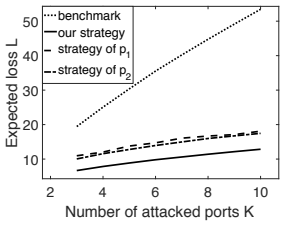
(a) power law distribution (same parameters)



(b) normal distribution (same parameters)



(c) power law distribution (different parameters)



(d) normal distribution (different parameters)

Figure 3: Expected loss L as a function of K

We compute the defender's expected loss against the attacker's best response for every defense strategy. Our purpose is to compare how different defense strategies perform against the MITM attack. Figure 3 shows the comparison results. Figure 3(a), 3(c), 3(b) and 3(d) present the experimental results where the c_i and v_i of users are following the power law distribution with the same parameters and different parameters and the normal distribution with the same parameters and different parameters, respectively.

We can see that the baseline case which sets the uniform probability $p = 1$ is always on the top in Figure 3. It indicates that our personalized defender's strategy and other two defense strategies can decrease the expected total losses against MITM attack. Further, compared with the two additional defense strategies carefully, it can be observed that the strategy with uniform probability p_2 is superior to the uniform probability p_1, however, the curve of our defense strategy always is the lowest in Figure 3. It indicates that our defense strategy can always achieve the lowest losses regardless of the distributions of c_i and v_i. Meanwhile, it is worth noting that the parameters of the distributions that c_i and v_i follow do not affect the performance of our optimal defense strategy, which illustrates that our defense strategy is robust in different practical environments.

Conclusion

We are the first to propose an strategic personalized defense strategy against MITM attacks to minimize the total losses of system under the Stackelberg game-theoretic framework. Simulation results prove that our personalized defense strategy significantly outperforms general non-strategic defense strategy. We only focus on the analysis of one particular service, and the results can be naturally applied to defend any

other services. Besides, our model can also be extended to the case where multiple clients shares one port. As future work, more comparisons against other non-strategic practical strategies will be conducted.

Acknowledgement

This work has partially been sponsored by the National Science Foundation of China (No. 61572349, No. 61272106), Tianjin Research Program of Application Foundation and Advanced Technology (No.: 16JCQNJC00100), Tianjin Key Laboratory of Advanced Networking, and Tianjin Key Laboratory of Cognitive Computing and Application.

References

Albina, M. N.; Raju, U.; Revathi, G. K.; and Raghava Rao, K. 2013. Protection against man-in-the-middle attack in banking transaction using steganography. *International Journal of Scientific & Engineering Research*.

An, B.; Shieh, E.; Yang, R.; Tambe, M.; Baldwin, C.; Direnzo, J.; Maule, B.; and Meyer, G. 2012. Protect - a deployed game-theoretic system for strategic security allocation for the united states coast guard. *Ai Magazine* 33(4):96–110.

Dacosta, I.; Ahamad, M.; and Traynor, P. 2012. *Trust No One Else: Detecting MITM Attacks against SSL/TLS without Third-Parties*.

Gangan, S. 2015. A review of man-in-the-middle attacks. *Computer Science*.

Griffin, D. 2016. A hierarchical organizational structure. http://smallbusiness.chron.com/hierarchical-organizational-structure-3799.html.

Huang, L. S.; Rice, A.; Ellingsen, E.; and Jackson, C. 2014. Analyzing forged ssl certificates in the wild. In *IEEE Symposium on Security and Privacy*, 83–97.

Jain, M.; Tsai, J.; Pita, J.; Kiekintveld, C.; Rathi, S.; Tambe, M.; Ordonez; and Ez, F. 2010. Software assistants for randomized patrol planning for the lax airport police and the federal air marshal service. *Interfaces* 40(4):267–290.

Kapil M, J.; Manoj V, J.; and Jay L, B. 2016. A survey on man in the middle attack. *International Journal of Science Technology & Engineering* 2:277–280.

Kiekintveld, C.; Islam, T.; and Kreinovich, V. 2013. Security games with interval uncertainty. In *International Conference on Autonomous Agents and Multi-Agent Systems*, 231–238.

Korzhyk, D.; Yin, Z.; Kiekintveld, C.; Conitzer, V.; and Tambe, M. 2011. Stackelberg vs. nash in security games: an extended investigation of interchangeability, equivalence, and uniqueness. *Journal of Artificial Intelligence Research* 41(2):297–327.

Kumar, C. K.; Jose, G. J. A.; Sajeev, C.; and Suyambulingom, C. 2012. Safety measures against man-in-the-middle attack in key exchange. *Journal of Engineering & Applied Sciences* 7(2):243–246.

Laszka, A.; Lou, J.; and Vorobeychik, Y. 2016. Multi-defender strategic filtering against spear-phishing attacks. In *Thirtieth AAAI Conference on Artificial Intelligence*.

Laszka, A.; Vorobeychik, Y.; and Koutsoukos, X. D. 2015. Optimal personalized filtering against spear-phishing attacks. In *Twenty-Ninth AAAI Conference on Artificial Intelligence*, 958–964.

Luo, Y. B.; Wang, B. S.; and Cai, G. L. 2014. Effectiveness of port hopping as a moving target defense. In *2014 7th International Conference on Security Technology (SecTech)*, 7–10.

Luo, Y. B.; Wang, B. S.; and Cai, G. L. 2015. Analysis of port hopping for proactive cyber defense. *International Journal of Security & Its Applications* 9(2):123–134.

Martin. 2013. China, github and the man-in-the-middle. https://en.greatfire.org/blog/2013/jan/china-github-and-man-middle.

Mutton, P. 2016. 95% of https servers vulnerable to trivial mitm attacks. https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html.

Nayak, G. N., and Samaddar, S. G. 2010. Different flavours of man-in-the-middle attack, consequences and feasible solutions. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, volume 5, 491–495. IEEE.

Osborne, M. J., and Rubinstein, A. 1994. *A course in game theory*. MIT press.

Seth Schoen, E. G. 2011. Iranian man-in-the-middle attack against google demonstrates dangerous weakness of certificate authorities. https://www.eff.org/deeplinks/2011/08/iranian-man-middle-attack-against-google.

Shieh, E. A.; An, B.; Yang, R.; Tambe, M.; Baldwin, C.; DiRenzo, J.; Maule, B.; and Meyer, G. 2012. Protect: An application of computational game theory for the security of the ports of the united states. In *AAAI*.

Simko, C. 2016. Man-in-the-middle attacks in the iot. https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/.

Vallivaara, V. A.; Sailio, M.; and Halunen, K. 2014. Detecting man-in-the-middle attacks on non-mobile systems. In *ACM Conference on Data and Application Security and Privacy*, 131–134.

Zhao, M.; An, B.; and Kiekintveld, C. 2015. An initial study on personalized filtering thresholds in defending sequential spear phishing attacks. In *Proceedings of the 2015 IJCAI Workshop on Behavioral, Economic and Computational Intelligence for Security*.