Stealthy Attacks with Insider Information: A Game Theoretic Model with Asymmetric Feedback

Xiaotao Feng*, Zizhan Zheng†, Derya Cansever‡, Ananthram Swami§ and Prasant Mohapatra†
*Department of Electrical and Computer Engineering, University of California, Davis, USA,
†Department of Computer Science, University of California, Davis, USA,
‡US Army CERDEC, USA
§U.S. Army Research Laboratory, USA,
Email: {xtfeng, cszheng, pmohapatra}@ucdavis.edu, {derya.h.cansever.civ, ananthram.swami.civ}@mail.mil

***Abstract*—Advanced Persistent Threats (APT) are highly motivated and persistent, and they often operate in a stealthy way to avoid detection. Moreover, an advanced attacker may choose to approach insiders within the organization. Insider information can not only reduce the attack cost significantly but also make the attack more covert. Although stealthy attacks and insider threats have been considered separately in previous works, the coupling of the two is not well understood. As both types of threats are incentive driven, game theory is an appropriate tool to reason about the strategic behavior for each participant. We propose a non-zero sum three-player game model to study the interplay between APT and insider threats. Our model is built upon the two-player FlipIt game model for stealthy takeover with two extensions. First, we consider an asymmetric feedback structure where the defender is observable, while the attacker is stealthy and obtains delayed feedback about the defender's security updates. Second, we consider a three-player setting by introducing an insider with a double role, where it can help either the attacker or the defender according to the payoffs. We characterize the subgame perfect equilibria of a sequential game with the defender as the leader, and the insider and the attacker as the followers. We derive various insights from the game model, and discuss approaches for achieving more efficient defense in the face of both a stealthy attacker and an insider with double roles.**

I. Introduction

Critical infrastructures and IT systems are increasingly threatened by incentive-driven targeted attacks [1], [2], [3]. For instance, advanced persistent threats (APT) have received a lot of attention recently. These attacks are highly motivated and persistent, and often operate in a stealth way to avoid detection to obtain long-term benefits. Traditional cyber-defense techniques focusing on one-shot attacks of known types are insufficient in the face of persistent, stealthy, and strategic attackers. To this end, game theory provides an accurate framework to reason about the incentives and strategic behavior in cybersecurity to help derive more efficient strategies against advanced attacks.

An important aspect that has been largely ignored in existing game theoretic models applied to cybersecurity is the impact of insider threats, which is especially important in the context of APT. An insider has privileged access to various sensitive data including the security measures applied, which makes them harder to detect than an outsider attacker. According to the 2014 US State of Cybercrime Survey [4], 28 percent of electronic crime events are known or suspected to have been caused by an insider. Moreover, the rise of cloud computing has significantly expanded the landscape of insider threats, and made them even more difficult to detect [5]. Insider information is invaluable to an advanced attacker as it not only reduces the cost for launching an efficient attack, but also makes it more covert. Therefore, it is crucial to study the coupling of advanced attacks and insider threats.

We propose a game theoretic model to study the strategic behavior in APT attacks assisted by insiders. Our game is built upon the FlipIt game model proposed by the RSA labs in response to an APT attack towards itself in 2011 [6]. The FlipIt game model abstracts away details about concrete attack and defense operations by focusing on the stealthy and persistent nature of players, and thus applies to a broad range of attack-defense scenarios in cybersecurity. In the basic model, there are two players, an attacker and a defender, and a single resource to be protected. Each player can make multiple moves during an infinite time horizon. Each move "flips" the state of the resource and incurs a cost to the corresponding player. The payoff of a player is defined as the fraction of time when the resource is under its control, less the total cost incurred.

The FlipIt game model captures the stealthy behavior of players in an elegant way by allowing various types of feedback structures. In the basic model, where neither player gets any feedback during the game, it is shown that periodic strategies with random starting phases form a pair of best response strategies [6]. On the other hand, in the asymmetric case where the defender is completely observable and the attacker is stealthy, periodic defense and immediate attack are shown to be a pair of best response strategies [7], [8].

We investigate two important extensions of the FlipIt game model to capture the attacker's uncertainty about the defender and the coupling between APT and insider threats. First, we consider an asymmetric feedback structure as in [7], where the attacker is stealthy and the defender is observable. But unlike [7] where the attacker gets notified by the defender's security update immediately, we consider a more general setting with delayed feedback, where the attacker learns the defender's last security update after a random *awareness time*.

Second, instead of the two-player setting as in most previous works such, we consider a three-player setting by introducing an insider into the game, where the insider can either reduce or increase the awareness time of the attacker. Note that we have expanded the definition of insider threats, by allowing the insider to help either the attacker (as most previous works do) or the defender depending on its expected payoff. To the best of our knowledge, our work is the first that considers the double roles of the insider. Due to the double roles of the insider, however, an explicit analysis of the subgame perfect equilibria of this three-player game is challenging. We therefore distinguish two cases to obtain more insights, when the defender does not know that there is an insider and when it does. We solve the game explicitly for the former case and compare it with the latter case through numerical results.

In our previous work [9], we have considered a three-player defender-attacker-insider game with symmetric feedback. Our new model has two key differences: 1) In [9], both the defender and the attacker are stealthy to each other. Thus, periodic defense and periodic attack are a pair of best response strategies. However, due to the asymmetrical setting in our model, periodic defense is undesirable for the defender as we discuss in Section 2. Instead, we consider an exponential defense strategy against a non-adaptive attack strategy; 2) The existence of the insider always hurts the defender in [9], while it may benefit the defender in our model due to the double roles of the insider.

We make the following contributions in this paper.

- We propose a three-player FlipIt game model that captures the strategic interactions between an overt defender, a covert attacker with delayed feedback, and an insider with double roles.
- We derive the subgame perfect equilibria for both two-player model and three-player model
- Based on the equilibrium solutions derived, we make suggestions on achieving more efficient defense against both advanced attacks and insider threats.

The remainder of this paper is organized as follows. We present the asymmetric three-player game model and discuss our choice of strategies in Section II. The analysis of the game is provided in Section III, where we first consider the simplified defender-attacker game without the insider, and then study the three-player case with the double role insider. We provide numerical results in Section IV. Based on the results, we make suggestions to improve defense in Section V. We conclude the paper in Section VI.

II. Game model

In this section, we present our game theoretic models. We start with the two-player defender-attacker setting with asymmetric feedback, and then consider the three-player setting by introducing an insider with double role into the game.

A. Asymmetric Two Players Game

As a beginning step, we consider a two-player non-zero sum game without the insider. In this game, two players compete for ownership of a single resource. The player who protects the resource is called the defender, denoted by D; the other player who compromises the resource is called the attacker, denoted by A. The resource has a binary state, where 0 means the resource is protected and 1 means the resource is compromised. As in FlipIt [6], both the attacker's and the defender's moves are instantaneous. That is, once a player moves, she obtains ownership immediately. The game begins at time $t = 0$ with the resource initially protected, and it lasts for a time horizon T. We consider that time is continuous and both players can move at any time, where each move has a positive cost. The game is graphically depicted in Figure 1.

In contrast to the basic FlipIt game, however, the two players have different feedback during the game. In particular, we assume that the defender does not know when the attacker moves, while the attacker can find out when the defender made the last move with a delay ω, called the "awareness time". This random delay models the time requited to detect an event (here, defender move) with some confidence. It is out of control of the attacker but can be affected by the insider as we discuss below. Consider the example of password reset. The defender can reset the password at a certain frequency to combat password compromise, without knowing whether / when the password has been stolen by the attacker. On the other hand, the attacker does not immediately know when the defender has reset the password, but it can learn this fact when it fails to log into the account using the previously compromised password. This delay can be considered as the awareness time. For simplicity, we assume that ω follows an exponential distribution with a mean rate λ_A in this paper.

The defender's action is to choose the time interval over which it will maintain its current defense posture (e.g., retain the current password). Define the defender's strategy as $\{l^i\}_{1\leq i\leq n}$, where l^i is the length of the i-th defense interval and n is the total number of moves. Among the n intervals, let S denote the subset of intervals where the attacker receives feedback before defender's next move, and then she decides either to attack or not right after receiving the feedback. In the remaining intervals, the attacker does not receive feedback before the defender's next move, and we assume that the attacker misses the feedback as well as the attack opportunity in this interval. We denote the attacker's strategy by $\{\alpha^j\}_{j\geq 0}$, where $\alpha^j = 1$ if the attacker attacks in the j-th round, and $\alpha^j = 0$ otherwise. We assume that attacks are immediately successful.

Given the strategies of the players, we are interested in the long-term expected payoffs for the defender and the attacker as defined below. See Table I for a description of the parameters.

Defender's Payoff:

$$P_{\mathcal{D}}(\{l^i\}) = \lim_{n\to\infty} \mathbb{E}\left\{1 - \frac{\sum_{j\in S}(l^j - \omega^j)\alpha^j + n\cdot C_{\mathcal{D}}}{\sum_{i=1}^{n} l^i}\right\} \tag{1}$$

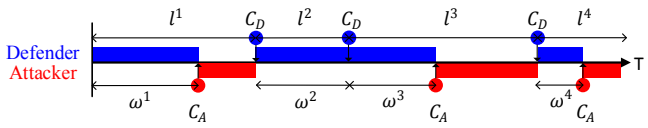


Figure 1: The proposed two players game. *Blue circles* and *red circles* represent defender's and attacker's actions, respectively. A *blue segment* denotes that the resource is under protection, and a *red segment* denotes that the resource is compromised.

Table I: List of System Parameters

Symbol	Meaning
T	time horizon
l^i	i-th defense interval
n	total number of defender's moves
ω^i	i-th awareness time
λ_A	rate of attacker's awareness time
λ_A^I	rate of attacker's awareness time impacted by insider
β	rate parameter of defender's exponential strategy
α	attacker's strategy, 1 for attack, 0 for no-attack
γ	insider's strategy
ρ	insider's power
$C_{\mathcal{A}}$	attacker's cost per move
$C_{\mathcal{D}}$	defender's cost per move
$C_{\mathcal{I}}$	insider's unit cost on affecting the awareness time
$B_{\mathcal{I}}$	insider's unit reward from helping attacker

Attacker's Payoff:

$$P_{\mathcal{A}}(\{\alpha^j\}) = \lim_{n\to\infty} \mathbb{E}\left\{\frac{\sum_{j\in S}[l^j - \omega^j - C_{\mathcal{A}}]\alpha^j}{\sum_{i=1}^n l^i}\right\} \quad (2)$$

We distinguish between several classes of defense strategies. A strategy is called *non-adaptive* if $\{l^i\}$ and n are determined at the beginning of the game. A non-adaptive strategy can be either *randomized* or *deterministic*. Among all the deterministic strategies, we will be particularly interested in *periodic strategies*, where l^i is a constant for all i, and *exponential strategies*, where l^i follows an *i.i.d.* exponential distribution. In addition, if $l^1 = \infty$, the strategy is called a *no defense strategy*. We may consider similar classes of attack strategies as we do for the defender. We will be most interested in the following simple non-adaptive attack strategies. If $\alpha^j = 1$ for all j, the strategy is called an *immediate attack strategy*. If $\alpha^j = 0$ for all j, it is called a *no attack strategy*. To simplify notation, we will say that the attacker adopts a *non-adaptive immediate strategy* if it chooses either the immediate attack strategy or no attack strategy.

B. Comparison to Other Asymmetric FlipIt Models

FlipIt game with asymmetric feedback has been studied in [6], [7], [8]. Our model has several major differences. First, in contrast to [6] where the attacker receives feedback only when it moves, the attacker may receive feedback at anytime during the game in our model regardless of whether she moves or not. In other words, the attacker is feedback driven in our model; thus, she makes decisions when she receives feedback. Moreover, the "awareness time" in our model is distinct from the "attack time" introduced in [7], [8]. In their case, the attacker receives feedback right after the defender's move, but the resource would not be successfully compromised until some random amount of time (the attack time).

Due to the uniqueness of our setting, the periodic defense strategy commonly considered in previous works [6], [7] is a poor choice. In particular, the attacker can easily figure out the exact defense period using a simple learning approach. For example, if the attacker learns that the defender has moved at both t_1 and t_2 ($t_2 > t_1$), then it can conclude that $\delta_1 = t_2 - t_1$ must be a multiple of the defense period. Therefore, the attacker could adjust her moves as a periodic strategy with period δ_1 so that she always moves right after the defender in every δ_1. Since there is no attack time, the attacker will control a whole period after her moves. If she then learns that the defender moved at $t_3 > t_2$ and $\delta_2 = t_3 - t_2$, she could further reduce the attack period to $\gcd[\delta_1, \delta_2]$. After receiving enough feedback, the attacker could learn the exact defense period.

C. Exponential Defense vs. Non-adaptive Attack

To prevent the attacker from taking advantages of the feedback, one can consider a renewal strategy with randomized defense periods to make the attacker's learning process more difficult. In this paper, we consider an exponential defense strategy. Due to the memoryless nature of the exponential distribution, the attacker can at most learn the distribution of defense intervals from the feedback but no more. In particular, knowing when the defender made the last move does not provide the attacker any information about defender's next move other than the distribution itself. As a result, the attacker makes her decision based only on the latest feedback and ignores all previous feedback about the defender's moves.

The following result shows that under an exponential strategy, it suffices to consider non-adaptive immediate attacks (see our online technical report [10] for the proof).

Theorem 1. *When the defender adopts an exponential strategy, there exits a non-adaptive immediate strategy that is the attacker's best response strategy.*

In the rest of the paper, we assume that the defense intervals follow an *i.i.d.* exponential distribution with rate β, thus, her strategy $\{l^i\}$ can be represented by β.

D. Three Players Game with Insider

We now introduce the three-player defender-attacker-insider game. We consider an insider I with double roles, which extends previous studies that focus on the adversarial aspect of the insider. On the one hand, the insider can help the attacker to compromise the system and get benefit from that. On the other hand, being a part of the organization, the insider shares its revenue; hence, it may also choose to help the defender against the attacker. In both cases, however, the insider tends to hide its existence from the defender.

We envision a setting where at the beginning of the game, the insider is approached secretely by the attacker and decides whether to help the attacker or the defender by choosing one of the following two strategies. First, help the attacker

to reduce the awareness time by notifying the attacker after the defender's last defense (immediately or with a delay). The sooner it notifies the attacker, the more it gets paid by the attacker, but also incurs a higher risk of being detected by the defender. Second, help the defender by making extra defense effort on the attacker's target. The more effort it puts in, the longer is the awareness time experienced by the attacker, but also a higher cost to the insider. Note that this might be beneficial to the insider since when the attacker approaches the insider, it might reveal part of its attack strategy including potential target to the insider. In both cases, we focus on non-adaptive strategies modeled by a single parameter γ determined at time $t = 0$ by the insider. Given insider's strategy γ, the awareness time in each round follows an *i.i.d.* exponential distribution with rate $\lambda_A^I = (1+\gamma)\lambda_A$. We assume that $\gamma \in [-\rho, \rho]$, where $\rho \in [0, 1)$ models the power of the insider. A larger ρ corresponds to a more powerful insider who has a higher share in the organization, and also a higher impact on the system. We note that for a non-adaptive insider, exponential defense and non-adaptive immediate attack are still a pair of best response strategies.

Three-Level Sequential Game: We introduce a three-level sequential game to model the interaction among the three players. In this model, the defender first determines and declares its strategy β. After observing β, the insider then decides whether to help the attacker or the defender. In the former case, it makes a "take-it-or-leave-it" offer $\gamma > 0$ to the attacker. In the latter case, it helps the defender by choosing a $\gamma \leq 0$. In both cases, the value of γ is declared to the attacker. Finally, given β and γ, the attacker decides α. We make the following assumptions in our analysis of the game:

1) Insider incurs an average cost $C_{\mathcal{I}}|\gamma|$ for a strategy γ, which includes both the cost of affecting the awareness time and the risk of being detected by the defender;
2) Insider receives an average payment from the attacker as $B_{\mathcal{I}} \max(\gamma, 0)$;
3) The defender does not know the existence of the insider; it considers the attacker as the only opponent in the game. We will numerically investigate the case when the defender knows the existence of the insider.

Define

$$p_{aware} = \int_0^{+\infty} \beta e^{-\beta t} \int_0^t \lambda_A^I e^{-\lambda_A^I \omega} \, d\omega dt = \frac{\lambda_A^I}{\lambda_A^I + \beta} \quad (3)$$

as the probability that attacker is aware of the last defense. We then calculate the long-term expected payoff as follows:

Defender' Payoff

$$P_{\mathcal{D}}(\beta, \gamma, \alpha) = \begin{cases} 1 - \frac{(\lambda_A^I - \beta)\alpha}{\lambda_A^I + \beta} - C_{\mathcal{D}}\beta, & \lambda_A^I > \beta, \\ 1 - C_{\mathcal{D}}\beta, & \lambda_A^I \leq \beta. \end{cases} \quad (4)$$

Attacker's Payoff

$$P_{\mathcal{A}}(\beta, \gamma, \alpha) = \begin{cases} \frac{\lambda_A^I \beta}{\lambda_A^I + \beta}(\frac{1}{\beta} - \frac{1}{\lambda_A^I} - C_{\mathcal{A}})\alpha - B_{\mathcal{I}} \max(\gamma, 0), & \lambda_A^I > \beta, \\ 0, & \lambda_A^I \leq \beta. \end{cases} \quad (5)$$

Insider's Payoff

$$P_{\mathcal{I}}(\beta, \gamma, \alpha) = \rho P_{\mathcal{D}}(\beta, \gamma, \alpha) - C_{\mathcal{I}} \cdot |\gamma| + B_{\mathcal{I}} \max(\gamma, 0) \quad (6)$$

where the first term denotes the profit from the protected system; the second term is the cost incurred from affecting the awareness time; and the last term is the payment from the attacker.

III. Subgame Perfect Equilibrium

In this section, we characterize the subgame perfect equilibrium of the three level sequential game. A group of strategies $(\beta^*, \gamma^*, \alpha^*)$ forms a subgame perfect equilibrium if

- $P_{\mathcal{D}}(\beta, \gamma, \alpha)$ is optimized at $\beta = \beta^*$ over every possible response from the insider and the attacker, and
- Given β^*, $P_{\mathcal{I}}(\beta^*, \gamma, \alpha)$ is optimized at $\gamma = \gamma^*$ over every possible response from the attacker, and
- Given β^* and γ^*, $P_{\mathcal{A}}(\beta^*, \gamma^*, \alpha)$ is optimized at $\alpha = \alpha^*$.

We first derive the equilibrium between the attacker and the defender where the defender is the leader and the attacker is the follower in Section III-A. Then we study the three-player defender-insider-attacker game in Section III-B. The proofs of all the lemmas and theorems can be found in our online technical report [10].

A. Two-Player Game

A subgame perfect equilibrium for the two player case is a pair of strategies (β^*, α^*) such that the defender's payoff $P_{\mathcal{D}}(\beta, \alpha)$ is optimized at $\beta = \beta^*$ over every possible response from the attacker, and then the attacker decides a strategy $\alpha = \alpha^*$ so that $P_{\mathcal{A}}(\beta^*, \alpha)$ is optimized according to the defender's strategy β^*.

We first find the best response strategy for the attacker for a given defense strategy as shown in the following lemma.

Lemma 1. *Assume that the defender adopts an exponential strategy with rate β; the attacker's best response strategies are:*

1) *If $\beta < \frac{\lambda_A}{1+C_{\mathcal{A}}\lambda_A}$, $\alpha = 1$;*
2) *If $\beta > \frac{\lambda_A}{1+C_{\mathcal{A}}\lambda_A}$, $\alpha = 0$;*
3) *If $\beta = \frac{\lambda_A}{1+C_{\mathcal{A}}\lambda_A}$, both $\alpha = 1$ or $\alpha = 0$ are the best responses for the attacker.*

We then find the subgame perfect equilibria of the game. We need the following definitions.

- $C_{\mathcal{D}}^1 \triangleq 1/\Big\{\lambda_A[3 - \frac{1}{1+C_{\mathcal{A}}\lambda_A} - 2\sqrt{2 - \frac{2}{1+C_{\mathcal{A}}\lambda_A}}]\Big\}$;
- $C_{\mathcal{D}}^2 \triangleq \frac{2}{\lambda_A}$;
- $C_{\mathcal{D}}^3 \triangleq C_{\mathcal{A}} + \frac{1}{\lambda_A}$.

Note that $C_{\mathcal{D}}^i$ $(i = 1, 2, 3)$ is a function of $C_{\mathcal{A}}$ and λ_A, and it is easy to prove that there are only two possibilities:

1) $C_{\mathcal{D}}^1 \leq C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}^2$;
2) $C_{\mathcal{D}}^2 \leq C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}^1$.

The theorem below provides a complete characterization of the set of subgame perfect equilibria of the defender-attacker game.

Theorem 2. *The defender-attacker game has the following subgame perfect equilibria and the corresponding payoffs:*

- *Class 1. If* $C_{\mathcal{D}}^1 \leq C_{\mathcal{D}} < C_{\mathcal{D}}^2$, $\beta^* = \sqrt{\frac{2\lambda_A}{C_{\mathcal{D}}}} - \lambda_A$, $\alpha^* = 1$.

$$P_{\mathcal{D}} = (\sqrt{2} - \sqrt{C_{\mathcal{D}}\lambda_A})^2,$$

$$P_{\mathcal{A}} = \sqrt{2C_{\mathcal{D}}\lambda_A} - C_{\mathcal{A}}\lambda_A(1 - \sqrt{\frac{C_{\mathcal{D}}\lambda_A}{2}}) - 1.$$

- *Class 2. If* $C_{\mathcal{D}} \leq C_{\mathcal{D}}^1 \leq C_{\mathcal{D}}^3$ *or* $C_{\mathcal{D}} \leq C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}^1$, $\beta^* = \frac{\lambda_A}{1+C_{\mathcal{A}}\lambda_A}$, $\alpha^* = 0$.

$$P_{\mathcal{D}} = 1 - \frac{C_{\mathcal{D}}\lambda_A}{1 + C_{\mathcal{A}}\lambda_A}, P_{\mathcal{A}} = 0.$$

- *Class 3. If* $C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}^2 \leq C_{\mathcal{D}}$ *or* $C_{\mathcal{D}}^2 \leq C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}$, $\beta^* = 0$, $\alpha^* = 1$.

$$P_{\mathcal{D}} = 0, P_{\mathcal{A}} = 1.$$

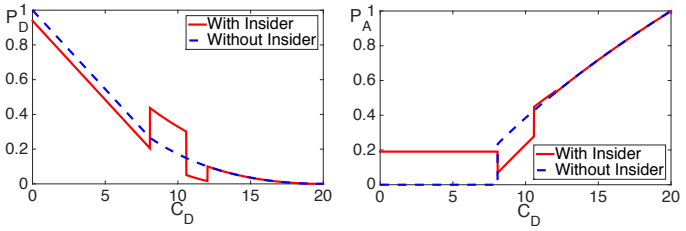
B. Three-Player Game

We then study the three-player defender-insider-attacker game. As mentioned in Section II-D, we find the subgame perfect equilibria under the assumption that the defender does not know the existence of the insider, even if the insider decides to help the defender. Therefore, the defender is not aware of the influence that the insider has on the awareness time, and chooses the same strategy as in the two-player case (although it incurs a different payoff). We will further investigate the case when the defender knows the existence of the insider via numerical study. We use backward induction to solve the game.

The theorem below provides a complete characterization of the subgame perfect equilibrium of the defender-insider-attacker game.

Theorem 3. *The subgame perfect equilibria of the defender-insider-attacker game are:*

- *Class 1. If* $C_{\mathcal{D}}^1 \leq C_{\mathcal{D}} < C_{\mathcal{D}}^2$,
  - *If* $\rho \geq \rho_1 = \frac{2-\sqrt{\frac{2}{C_{\mathcal{D}}\lambda_A}}-C_{\mathcal{A}}\sqrt{\frac{2\lambda_A}{C_{\mathcal{D}}}}+C_{\mathcal{A}}\lambda_A}{1+C_{\mathcal{A}}\lambda_A-C_{\mathcal{A}}\sqrt{\frac{2\lambda_A}{C_{\mathcal{D}}}}}$,
    $C_{\mathcal{I}} \leq \frac{\rho\sqrt{2C_{\mathcal{D}}\lambda_A}-\rho}{\rho_1}$.
    $\beta^* = \sqrt{\frac{2\lambda_A}{C_{\mathcal{D}}}} - \lambda_A$, $\gamma^* = -\rho_1$, $\alpha^* = 0$.
  - *If* $\rho < \rho_1$, $C_{\mathcal{I}} \leq \frac{2\rho(\sqrt{2C_{\mathcal{D}}\lambda_A}-C_{\mathcal{D}}\lambda_A)}{2-\rho\sqrt{2C_{\mathcal{D}}\lambda_A}}$,
    $B_{\mathcal{I}} \leq \frac{\sqrt{2C_{\mathcal{D}}\lambda_A}-C_{\mathcal{D}}\lambda_A}{\frac{2}{\rho}-\rho C_{\mathcal{D}}\lambda_A}$.
    $\beta^* = \sqrt{\frac{2\lambda_A}{C_{\mathcal{D}}}} - \lambda_A$, $\gamma^* = -\rho$, $\alpha^* = 1$.
  - *If* $\rho < \rho_1$, $\frac{\sqrt{2C_{\mathcal{D}}\lambda_A}-C_{\mathcal{D}}\lambda_A}{\frac{2}{\rho}-\rho C_{\mathcal{D}}\lambda_A} < B_{\mathcal{I}} \leq \frac{(\sqrt{2\lambda_A}-\sqrt{C_{\mathcal{D}}}\lambda_A)(2\sqrt{C_{\mathcal{D}}}-C_{\mathcal{A}}(\sqrt{2\lambda_A}-\sqrt{C_{\mathcal{D}}}\lambda_A))}{2+\sqrt{2C_{\mathcal{D}}\lambda_A}}$,
    $C_{\mathcal{I}} \leq B_{\mathcal{I}} - \frac{2\rho(\sqrt{2C_{\mathcal{D}}\lambda_A}-C_{\mathcal{D}}\lambda_A)}{2+\rho\sqrt{2C_{\mathcal{D}}\lambda_A}}$.
    $\beta^* = \sqrt{\frac{2\lambda_A}{C_{\mathcal{D}}}} - \lambda_A$, $\gamma^* = \rho$, $\alpha^* = 1$.
  - *Otherwise,* $\beta^* = \sqrt{\frac{2\lambda_A}{C_{\mathcal{D}}}} - \lambda_A$, $\gamma^* = 0$, $\alpha^* = 1$.
- *Class 2. If* $C_{\mathcal{D}} \leq C_{\mathcal{D}}^1 \leq C_{\mathcal{D}}^3$ *or* $C_{\mathcal{D}} \leq C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}^1$,
  - *If* $B_{\mathcal{I}} < \frac{1+C_{\mathcal{A}}\lambda_A}{(1+\rho)(1+C_{\mathcal{A}}\lambda_A)+1}$,
    $C_{\mathcal{I}} \leq B_{\mathcal{I}} - \frac{(1+\rho)(1+C_{\mathcal{A}}\lambda_A)-1}{(1+\rho)(1+C_{\mathcal{A}}\lambda_A)+1}$.
    $\beta^* = \frac{\lambda_A}{1+C_{\mathcal{A}}\lambda_A}$, $\gamma^* = \rho$, $\alpha^* = 1$.
  - *If* $\frac{1+C_{\mathcal{A}}\lambda_A}{(1+\rho)(1+C_{\mathcal{A}}\lambda_A)+1} < B_{\mathcal{I}} \leq \frac{1+C_{\mathcal{A}}\lambda_A}{2+C_{\mathcal{A}}\lambda_A}$,
    $C_{\mathcal{I}} \leq B_{\mathcal{I}} - \frac{\rho}{\rho_2}\frac{(1+\rho_2)(1+C_{\mathcal{A}}\lambda_A)-1}{(1+\rho_2)(1+C_{\mathcal{A}}\lambda_A)+1}$,
    where $\rho_2 = \frac{1}{B_{\mathcal{I}}} - \frac{1}{1-C_{\mathcal{A}}\lambda_A} - 1$.
    $\beta^* = \frac{\lambda_A}{1+C_{\mathcal{A}}\lambda_A}$, $\gamma^* = \rho_2$, $\alpha^* = 1$.
  - *Otherwise,* $\beta^* = \frac{\lambda_A}{1+C_{\mathcal{A}}\lambda_A}$, $\gamma^* = 0$, $\alpha^* = 0$.
- *Class 3. If* $C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}^2 \leq C_{\mathcal{D}}$ *or* $C_{\mathcal{D}}^2 \leq C_{\mathcal{D}}^3 \leq C_{\mathcal{D}}$, $\beta^* = 0$, $\gamma^* = 0$, $\alpha^* = 1$.



(a) Defender's payoff (b) Attacker's payoff

Figure 2: Payoff v.s. $C_{\mathcal{D}}$ in Defender-Attacker Game and Defender-Insider-Attacker Game, $C_{\mathcal{A}} = 1$, $\lambda_A = 0.1$, $\rho = 0.3$, $C_{\mathcal{I}} = 0.05$, $B_{\mathcal{I}} = 0.25$.

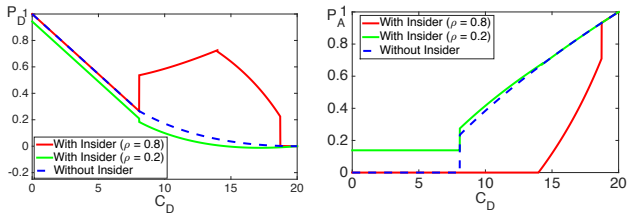
IV. Numerical Study

In this section, we examine our three-player game under different system scenarios and configurations.

Impact of System Parameters: In Figure 2a, we plot the defender's payoffs with and without the insider as a function of $C_{\mathcal{D}}$. The existence of the insider provides a negative payoff when $C_{\mathcal{D}} \in [0, 8.2]$ since the insider helping the attacker. From $C_{\mathcal{D}} = 8.2$, the insider turns to help the defender and provides a positive payoff when $C_{\mathcal{D}} \in [8.2, 10.5]$. From $C_{\mathcal{D}} = 10.5$, the insider turns to help the attacker again so the defender's payoff is reduced when $C_{\mathcal{D}} \in [10.5, 11.9]$. Therefore, unlike the two-player case, a smaller C_D is not always beneficial to the defender. We find the symmetrical phenomenon when plot the attacker's payoff under the same setting in Figure 2b.

Impact of the Insider's Power: We then demonstrate the impact of ρ by considering three cases: no insider, a less powerful insider with $\rho = 0.2$ and a more powerful insider with $\rho = 0.8$. In Figure 3a, we plot the defender's payoff as a function of $C_{\mathcal{D}}$. We observe that the green curve is always lower than the blue dashed one, which implies that the less powerful insider tends to help the attacker rather than the defender. On the other hand, the red curve is always higher than (or same as) the blue dashed one. In particular, when $C_{\mathcal{D}} \in [7.6, 18.0]$, the defender's payoff increases dramatically. This implies that the more powerful insider tends to help the defender rather than the attacker.

Similar observations can also be made about the attacker's payoffs as shown in Figure 3b. Note that where there is no insider, the attacker starts to attack at $C_{\mathcal{D}} = 7.6$. With a less



(a) Defender's payoff (b) Attacker's payoff

Figure 3: Payoff vs. $C_{\mathcal{D}}$ with $\rho = 0.2$ and $\rho = 0.8$, $C_{\mathcal{A}} = 1$, $\lambda_A = 0.1$, $C_{\mathcal{I}} = 0.05$, $B_{\mathcal{I}} = 0.4$.

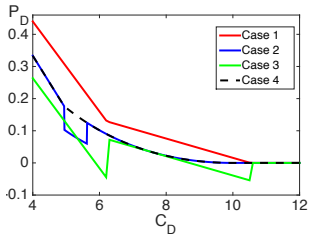


Figure 4: Defender's Payoff v.s. $C_{\mathcal{D}}$ under different knowledge about the insider, $C_{\mathcal{A}} = 1$, $\lambda_A = 0.2$, $\rho = 0.2$, $C_{\mathcal{I}} = 0.05$, $B_{\mathcal{I}} = 0.25$.

powerful insider, the attacker could obtain benefit for $C_{\mathcal{D}} \in [0, 7.6]$ where the attacker originally gets nothing in the two-player case. However, with a more powerful insider, the entry point of the attacker is delayed from $C_{\mathcal{D}} = 7.6$ to 14.2, and the payoff is significantly reduced until $C_{\mathcal{D}} = 18.0$ comparing to the two-player case.

Impact of the Defender's Knowledge about the Insider: Finally, we study how the defender's knowledge about the insider affect the payoffs in Figure 4. We consider four cases: 1. There is an insider in the system and the defender knows this; 2. There is an insider in the system but the defender does not know it; 3. There is no insider in the system but the defender assumes one; 4. There is no insider in the system and the defender knows that.

Cases 2 and 4 have been studied in Section III-B and Section III-A, respectively. We apply a searching algorithm to find the equilibrium payoffs in Case 1 and 3. In Figure 4, we observe that the red curve is higher than the black dashed one, which implies that the defender always gets more benefit by knowing the presence of the insider. The reason is that the defender as the leader can adopt a strategy to force the insider to choose $\gamma < 0$. In addition, we observe that the green curve is lower than the black dashed one, which implies that if the defender assumes that there is an insider when there is none, the defender will choose a smaller β assuming the insider will help it; consequently, the resource will be compromised more by the attacker.

V. Discussion

Based on the above results, we make the following observations:

- In contrast to the two-player game, the defender does not always obtain more benefit with smaller $C_{\mathcal{D}}$ in three-player game. Therefore, a more detailed investigation is needed in adjusting these parameters.
- Due to the attacker would be more likely to approach less powerful members, the defender should ensure effective practices (e.g., separation of duties, monitoring suspicious behavior, and secure backup) to prevent less powerful members from being compromised by the insider.
- If the defender is uncertain about the existence of the insider, it is better for the defender to adopt a β slightly larger than the best strategy in the two-player game in order to reduce the risk of severe damage.

VI. Conclusion

APT attacker with stealthy behavior and insider threats are major issues in cybersecurity. Together, they can inflict severe damage to our nation's infrastructure and information technology systems. In this paper, we present a three-player defender-insider-attacker game model to understand the interplay between stealthy attacks and insider threats. Our model extends the two-player FlipIt game by allowing the attacker to learn the last defense with an awareness time and by introducing an insider who can either help the attacker or the defender. We characterize the subgame perfect equilibria of a three-level sequential game with defender as the leader and insider and attacker as the followers. Various insights on achieving cost-effective defense are derived.

VII. Acknowledgement

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

References

[1] C. Tankard, "Advanced persistent threats and how to monitor and deter them," *Network security*, vol. 2011, no. 8, pp. 16–19, 2011.

[2] N. Virvilis and D. Gritzalis, "The big four-what we did wrong in advanced persistent threat detection?" in *ARES, 2013 Eighth International Conference on*. IEEE, 2013, pp. 248–254.

[3] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "The Cousins of Stuxnet: Duqu, Flame, and Gauss," *Future Internet*, vol. 4, pp. 971–1003, 2012.

[4] "2014 US State of Cybercrime Survey," http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml.

[5] M. Kandias, N. Virvilis, and D. Gritzalis, "The insider threat in cloud computing," in *Critical Information Infrastructure Security*. Springer, 2013, pp. 93–103.

[6] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "FlipIt: The Game of "Stealthy Takeover"," *Journal of Cryptology, 26(4)*, pp. 655–713, 2013.

[7] A. Laszka, B. Johnson, and J. Grossklags, "Mitigating Covert Compromises: A Game-Theoretic Model of Targeted and Non-Targeted Covert Attacks," in *Proc. of WINE*, 2013.

[8] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in *Proc. of GameSec*, 2015.

[9] X. Feng, Z. Zheng, P. Hu, D. Cansever, and P. Mohapatra, "Stealthy attacks meets insider threats: A three-player game model," in *Proc. of IEEE MILCOM*, Oct 2015, pp. 25–30.

[10] X. Feng, Z. Zheng, D. Cansever, A. Swami, and P. Mohapatra, "Stealthy Attacks with Insider Information: A Game Theoretic Model with Asymmetric Feedback," Technical Report, available online at http://spirit.cs.ucdavis.edu/pubs/tr/mil16.pdf.