The University of Texas at Austin
Center for Identity

A Survival Game Analysis to Common Personal Identity Protection Strategies

David Liau
Razieh Nokhbeh Zaeem
K. Suzanne Barber

UTCID Report #20-12

July 2020

A Survival Game Analysis to Common Personal Identity Protection Strategies

No Author Given

No Institute Given

Abstract. Throughout the years, authentication processes of individuals' identities have become essential parts of our modern daily life. These authentication processes also introduced the heavy use of Personally Identifiable Information (PII) in various applications. On the other hand, the continuous increase of identity–the unauthorized use of such PII–has created rich business opportunities for identity protection service providers. These services usually consist of a monitoring system that continuously searches through the Internet for incidents that supposedly indicates identity theft activities. However, these solutions are largely based on case studies and a quantified method is missing among different identity protection services.

This research offers a tool that provides quantitative analysis among different identity protection services. By bringing together previous work in the field, namely the UT Center for Identity (CID) Identity Ecosystem (a Bayesian network mathematical representation of a person's identity), real world identity theft data, stochastic game theory, and Markov decision processes, we generate and evaluate the best strategy for defending against the theft of personal identity information. One of the research problems that this paper addresses is the computation complexity of quantitatively evaluating identity protection strategies with *real world data*. In a real world database like Identity Threat Assessment and Prediction (ITAP) project which the UT CID Identity Ecosystem is built on, the number of PII attributes in use are normally in the order of 10^3. We propose a reinforcement learning algorithm for solving the optimal strategy to protect the user's identity against a malicious and efficient attacker. We aim to understand how initial individual PII exposure evolves into crucial PII breaches over time in terms of the dynamic integrity of the Identity Ecosystem. Real world identity protection strategies are then translated into the system and fight against the malicious attacker for quantitative comparison in our experiment. We present the survival analysis to these strategies and calculate the survival gap between these strategies against our active protection strategy as our experiment result. This study is aimed to understand the evolutionary process of identity under attack which may inspire a new direction for future identity protection strategies.

Keywords: Privacy Protection, Identity Protection Service, Personally Identifiable Information, Stochastic Game, Identity Ecosystem, Reinforcement Learning

1 Introduction

Today, more and more authentication and authorization processes are involved in our daily lives. At the same time, specific combinations of Personally Identifiable Information attributes, known as PII, are used to enable these processes. According to [8] PII is defined as 1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or bio-metric records; and 2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Modern authentication and authorization processes usually have strong involvement of multiple PII attributes to ensure reliability and integrity.

According to the 2016 U.S. National Crime Victimization Survey [10], at least 25.9 million Americans were affected by identity fraud–the breach and illegal use of victims' PII–in the previous year. In the consumer sentinel network from the Federal Trade Commission (FTC), identity theft and fraud are one of the top categories of scam reported to the agency, to which people lost more than \$1.9 billions in 2019. The number of identity fraud, theft and other scams reached an all time high in the past year, making itself a clear and present threat to our modern society.

Companies like Lifelock[14], identityforce[9], and ID watchdog[21], which often refer to their services as identity theft protection services, have become popular to solve the problem of personal identity theft. However, no service can guarantee a total protection against having crucial PII attributes being stolen. What these companies are offering is actually monitoring as well as recovery services. The monitoring services use several identity theft indicators to probe for identity theft. On the other hand, the recovery services focus on minimizing the impact of an identity theft after the incident has taken place [6]. We can easily find qualitative comparison among many of these identity theft protection services while there are little quantitative results available in the literature.

Recently, Liau et al. [13] proposed a quantitative evaluation framework for different identity protection systems which utilized the combination of UT CID Ecosystem, a Bayesian network representation of a person's identity, and stochastic shortest path games to evaluate different identity protection systems with survival analysis. Although the results are promising, the evaluation was done artificially on a sampled network due to the large number of PII attributes involved in human daily activities. In this work, we wish to further extend the results so that the full data of over 6,000 identity theft and fraud news reports in the Identity Threat Assessment and Prediction (ITAP) project can be utilized to give us a real-world evaluation of different protection strategies.

In this research, we build on various previous work: 1) the UT CID Identity Ecosystem, 2) the UT CID ITAP 3) Stochastic Game Theory, and 4) Reinforcement Learning. Figure 1 provides a high-level summary of our contribution. ITAP provides a comprehensive list of 627 real-world PII attributes to the UT CID Identity Ecosystem to formulate the Bayesian Network representation of a person's identity. We simulate the evolutionary process of identity theft as a

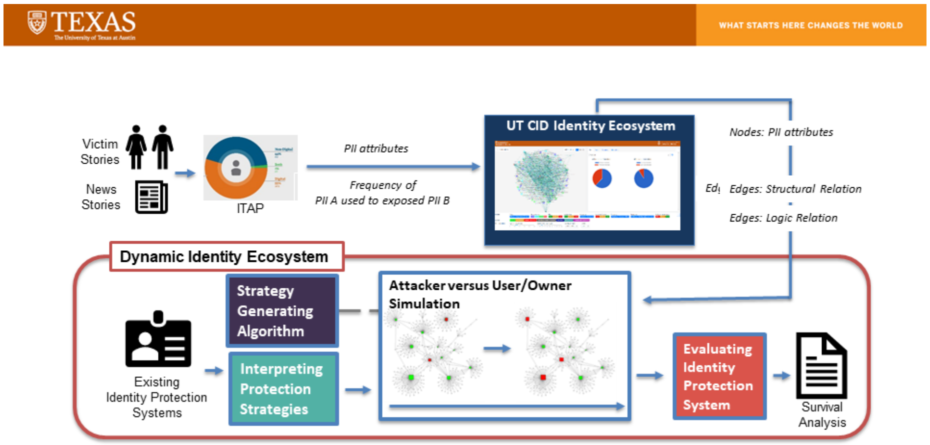
TEXAS
The University of Texas at Austin
WHAT STARTS HERE CHANGES THE WORLD
Victim Stories
News Stories
ITAP
PII attributes
Frequency of
PII A used to exposed PII B
UT CID Identity Ecosystem
Nodes: PII attributes
Ed
Edges: Structural Relation
Edges: Logic Relation
Dynamic Identity Ecosystem
Strategy Generating Algorithm
Attacker versus User/Owner Simulation
Existing Identity Protection Systems
Interpreting Protection Strategies
Evaluating Identity Protection System
Survival Analysis

Fig. 1. High-level structure of our identity protection system evaluation.

stochastic shortest path game played between the identity owner and the attacker while the owner's identity evolves over the Bayesian network model through time. In order to quantitatively evaluate an existing identity protection system, we interpret it as a protection strategy for the owner. We then further generate a minimax strategy for the attacker through the optimal strategy generating algorithm. We simulate the game and finally produce a survival analysis—how the given identity protection system *survives* in the face of an optimal identity attacker. **The application of reinforcement learning is particularly novel in this paper, as it enables our game between the attacker and PII owner on the Identity Ecosystem to scale to real-world situations.**

The UT Center for Identity, [23], developed the **Identity Ecosystem**, which is a Bayesian network representation of a person's identity, to study how personal identities are constructed and used in daily lives [24, 18, 17, 4]. It also articulates the relationships between PII attributes, and the dynamics of identity when the condition of these relationships and PII attributes change. For instance, one could analyze the security level of an authentication method utilizing the power of the UT CID Identity Ecosystem [3]. In short, three main queries of the real world are answered by the UT CID Ecosystem: 1) the risk of exposure of a certain PII attribute, 2) the cause of an exposure, and 3) the cost/liability of an exposure.

The UT CID **Identity Threat Assessment and Prediction (ITAP)** Project [26, 25] is a longitudinal study of about 6,000 identity theft and fraud stories over the past twenty years. A team of modelers manually investigate identity theft and fraud news stories collected online and record various aspects of them, including how the theft/fraud happened, its consequences, and importantly PII exploited. Through ITAP, we obtain a comprehensive list of over 627 real-life PII attributes.

Stochastic games are a special type of games that were first introduced by Shapley [19]. Unlike the usual game setup, the basic version of stochastic games takes the form of a Markov Decision Process. A stochastic shortest path game is a special class of games in the family of zero-sum stochastic games. In previous work from Patek [16], the sufficient condition for existence of a unique solution and the convergence results were established for the finite-state compact control stochastic shortest path games. More recent results can be found in [22] which extends the results of Patek [16] to a broader class of stochastic shortest path games.

A **reinforcement learning** problem [15] traditionally involves an agent in a dynamic environment where the agent is trying to maximize its payoff through solving a problem. The process involves learning a mapping from optimal actions to situations of the environment the agent can observe. These problems are often considered closed-loop problems since the action of the agent can result in changing the environment around it. Mathematically speaking, a reinforcement learning problem is equivalent to the optimal control problem of Markov Decision Processes (MDP). In our work, the identity attacker and the identity owner are the agents and we utilize *function approximation* to develop the algorithm that can find an optimal strategy in the protection game.

In this paper, we develop a reinforcement learning algorithm to solve a stochastic shortest path game based on the UT CID Identity Ecosystem with its full ITAP data set and provide the survival evaluation of different popular identity protection services used by companies in the real world. In addition, we provide some extended quantitative analysis of the original UT CID Ecosystem as in [5, 17] to further understand how modern PII attributes are associated with one another.

In Section 2, we cover the topics of various foundations of this work including the UT CID ITAP and Identity Ecosystem, stochastic shortest path games, and reinforcement learning with state approximation. Section 3 highlights our main contributions. We then present our evaluation results in Sections 4 and 5 where different identity protection strategies are compared and the insights we learn are discussed. Finally, we conclude the paper in Section 6.

2 Background

In this section we cover the foundations of our work, including UT CID ITAP and Identity Ecosystem which we obtained from their respective authors[26, 23], stochastic shortest path games, and reinforcement learning with state approximation.

2.1 Identity Threat Assessment and Prediction (ITAP) Project

The UT CID ITAP[26] gathers identity theft data, including exploited PII, through the analysis of over 6,000 actual identity theft and fraud news reports.

The ITAP project models “business” processes employed in real world identity theft and fraud cases to construct a risk assessment of identity threat patterns and consequences. Not only does the ITAP tool provide statistics about how and what kind of identity theft takes place on a daily basis across the 16 Department of Homeland Security (DHS) critical infrastructure sectors, but ITAP also captures methods and resources used to carry out identity theft and fraud. Significant to our work is ITAP’s list of 627 actual PII attributes and the frequency of each PII attribute being used to expose another.

2.2 UT CID Identity Ecosystem

The UT CID Identity Ecosystem[23], as shown in Figure 2, is a Bayesian model of PII attributes and their relationships. The version of the UT CID Identity Ecosystem model examined in this research is populated with real-world data from approximately 6,000 reported identity theft and fraud cases collected as part of the UT CID ITAP project. We leverage this populated Ecosystem model to provide unique, empirically-based insights into the variety of PII, their properties, and how they interact. Each of the 627 PII from ITAP (e.g., social security number, address, fingerprint) becomes a node in the UT CID Identity Ecosystem graph. The “probabilistically determines” relationship from PII A to PII B in the UT CID Identity Ecosystem indicates that PII attribute A was used to discover or create PII attribute B in some of the 6,000 identity theft and fraud cases of ITAP. The weight of such an edge between A and B is extracted from the *frequency* of A being used to discover/create B. Through the UT CID Identity Ecosystem, we understand how each PII attribute interacts with another as a consequence of exposure. For example, exposure or theft of a person’s social security number or a credit card number might result in very different consequences. Informed by the real-world data, this research investigates the ecosystem of personal identifiable information in which criminals compromise and misuse PII.

2.3 Stochastic Shortest Path Games

Stochastic games are a special type of games that were first introduced by Shapley [19]. Unlike the usual game setup, the basic version of stochastic games takes the form of a Markov Decision Process. Consider a two-player game where there are a finite number N positions, or states, and a finite number u_k,v_k of actions to all positions $k \in [1, N]$ for players u and v, respectively. Within a round of the game, each player chooses a valid action according to the position of the game. The game then moves to another position l with some probability distribution depending on the actions that the players chose. Players then receive payoffs according to the actions they chose and the position. The game would be played continuously until the game ends in some terminal position. Without the loss of generality, there is a possibility that such a game would continue forever. In Shapley’s original paper, the existence of an optimal strategy for such a game is established. In previous work from Kushner and Chamberlain[12], a variety

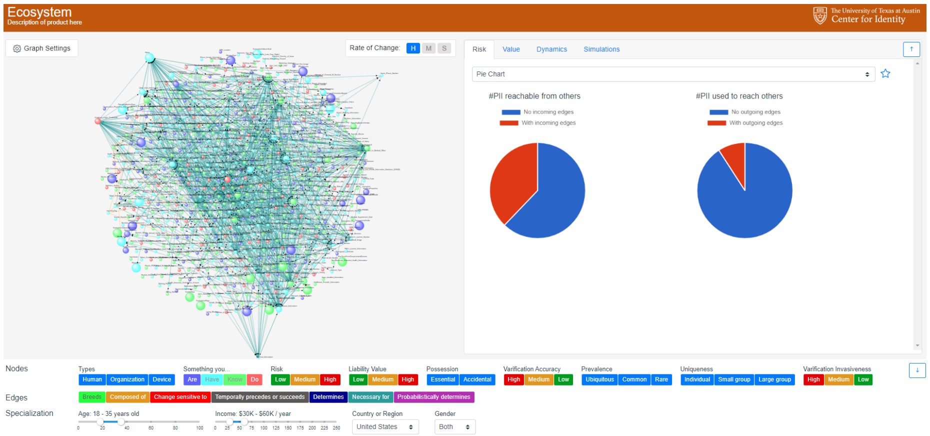

Fig. 2. A snapshot of the Identity Ecosystem [23]. In this particular example, the size of a PII node is determined by its risk of exposure and different colors are used to distinguish the types of PII.

of cost functions as well as other constraints of stochastic games are studied in detail. In this work, we shall borrow the results from Shapley and solve the optimal strategy with the policy iteration algorithm. One special class of the stochastic games is the stochastic shortest path games.

In stochastic shortest path games, the players have the exact opposite objective with respect to one another. In our case, consider an identity owner referred to as the user and a malicious person as the attacker. If the goal of the user now is to prevent some crucial PII from being exposed (e.g., bank account password), the goal of the attacker is to acquire/expose that piece of information as soon as possible while the user is trying to prolong this process as long as possible. The game ends/terminates immediately if the bank account password is exposed. In other words, the attacker is trying to end the game in the fastest manner while the objective of the user is exactly the opposite. This problem has been studied by Patek[16] while Huizhen [22] studied the problem in a finite state space with results for Q-Learning algorithms. In our work, we utilize the results to construct a workable strategy solving algorithm that solves the problem at a bigger scale where the state space is the size of the *power set* of the PII attributes extracted from ITAP.

2.4 Reinforcement Learning with Linear State Approximation

In [13], the authors established a value iteration (VI) algorithm and convergence result for a general identity network with a small size. The problem with a VI algorithm is that in the real world, the PII attributes used by regular Americans are of a considerably larger size. In addition to that, as we are entering the era of the Internet of Things (IoT), the PII attribute in use is guaranteed to surpass previous numbers dramatically. A simple VI algorithm is simply not powerful enough to solve the optimal strategy of the identity protection game. To further illustrate the idea, consider the identity protection game mentioned in the last section and the set of 627 PII from ITAP. The state of the MDP problem is $O(2^{627})$ in the worst case given that there are two status for each PII attribute (i.e., exposed and unexposed). Thus we need to involve reinforcement learning techniques in order to solve the problem.

Reinforcement learning [2] has been one of the research areas of interest in machine learning research. Mathematically, reinforcement learning problems are often formed as optimal control problem of an MDP problem. A MDP model consists of five essential elements: decision epochs, states, actions, transition probabilities, and rewards. A decision maker, at certain time epochs, is given a opportunity to make influence to the evolve of the system. The goal is to find a rule to these sequence of actions that will make the system to evolve in a way that maximize some predetermined utility. In our case, we do have the information of the transition probability but unfortunately due to the complexity and the size of the problem, we cannot solve the problem using naive reinforcement learning framework such as the basic version of value iteration or policy iteration algorithm.

Luckily, this problem is like many of the practical problems that exist in the reinforcement context [1] where the natural representation of the system is simply too larger to memorize. Consider a system where the observations are simultaneous binary measurements from n different sensors, in which the natural representation of the system would be of size 2^n. If we want to solve any MDP problem for this example, the problem simply becomes unsolvable provided n is sufficiently large. The idea of state representation is that depending on the exact problem we are solving, we are not stuck with the natural representation of the system but finding good indicators and a function of these indicators to represent the state. Take the common Q-Learning algorithm from [7], from which we have the general idea of what could be considered as a good representation. Comparing between different representation choices, one important concept is coverage which is the portion of the state space for which feature's value is not zero. Features with low coverage provide better accuracy, while features with high coverage offer better generalization. In practice, it is important to decide the balance between the two given different problems or goals. Proper choices of accuracy result in preciseness of the value function, while good generalization results in an acceptable convergence time of the algorithm.

3 Our contribution: Real World Identity Protection Strategy Evaluation with Dynamic Identity Ecosystem

The main contribution of this work is that we bring together various works in the field to form a quantitative identity protection strategy evaluation. From Fig 1, the core of the evaluation system, naming the Dynamic Identity Ecosystem, takes input from a UT CID Identity Ecosystem constructed from real world identity theft stories and domain knowledge of PII attributes to capture the dynamic nature of our personal identity. Although a value iteration algorithm was built [13] to solve for the optimal defense and attack strategies, the algorithm was not capable of solving the problem when we includes the whole ITAP database, since the number of PII attributes in use are normally in the order of 10^3.

We propose a Q-learning algorithm with state approximation in this work to fill in the gap and evaluate identity protection strategies adopted by different companies in the real world. The survival analysis result are given in Sec 5. By interpreting real world strategies into the system, we are able to obtain valuable knowledge to efficiently defend against identity theft in the real world. One key idea in our work is the concept of a pro-active protection strategy which had already been used in some scenarios to provide enhanced security. To give an example, many companies requires the password of the account to be changed every given period of time instead of monitoring the Internet for breaching events. Similar ideas can be applied to daily PII attributes in use to enhance the integrity of personal identity. We would also like to have an estimate of the gap between the real world monitoring strategy and a pro-active protection strategy.

4 Experiments

In this section, some details related to the actual implementation is provided which establishes the progress of choosing good indicators for state approximation. First, we provide statistics about the UT CID Identity Ecosystem with ITAP data which gives some quantitative discrimination about how PII attributes are connected to one another in practice. Based on the statistics, we then choose and present the indicators that in practice leads to good learning results in the proposed study case.

4.1 Statistics of the UT CID Ecosystem

In order to choose appropriate indicators for our system, we analyze the data in the UT CID Ecosystem from various view points, beyond what its authors have already reported [5]. For PII attributes in the ecosystem, the number of directed connected PII attributes (children and parent nodes) are at an average of 1.34. We have 67% of the PII attributes that are used only as a single breaching point to identity theft which means the status of these PII attributes does not contribute to the risk of other PII attributes. Below 10% of the PII attributes have more than 10 children PII attributes in the Ecosystem. The total number of edges in the UT CID Ecosystem is 844. Combine the statistics from above, we can describe the UT CID Ecosystem which represents a person's identity as a centric-wise network, meaning that most of the nodes are connected to few edges in the network while there exists a small group of nodes that are highly connected. Imagine a network in which there exists a small cluster consisting of a small portion of nodes in the network while other nodes are sparsely connected to the nodes in the cluster. This description gives us the imagination of how a UT CID Identity Ecosystem looks like (Figure 2). Transforming these properties in the real world, one can give a conjecture to the ways that our PII attributes relate to each other as follows: Since one of the sources that the UT CID Identity Ecosystem is constructed from is identity theft criminal history, it is at some level representing how identities are being stolen. There are PII attributes like names or addresses that are commonly used in many of the daily authentication/authorization processes while PII attributes like salary or call history are connected to these highly connected PII attributes. If these highly connected or core PII attributes were exposed to malicious people in the real world, the attackers can leverage the connection to significantly increase their ability to expose any other PII attributes. On the contrary, if the sparsely connected PII attribute were exposed, the total number of PII attributes at risk of exposure would be limited.

Figure 3 displays how PII attributes are connected in the Ecosystem. About 92.8% of the 627 PII attributes are without children, meaning that they have not been found to be used to acquire other PII attributes. As a result, only 7.2% of PII attributes have impact on the risk of exposure of other PII attributes. Furthermore, 33.7% of the PII attributes are directly connected to, from another (parent) PII attribute. Notice that overall, 65.4% of the PII attributes are isolated from other PII attributes.

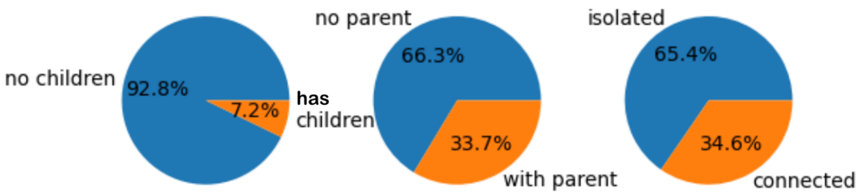

Fig. 3. How PII attributes are connected in the Ecosystem. 7.2% of the total PII attributes have a direct effect on exposure of other PII attributes. 66.3% of the total PII attributes are not directly affected by exposure of other PII attributes. This indicates that some PII attributes are heavily used in our daily lives while others are not.

To choose good indicators, we need PII attributes that preserve the most state information while maintaining the complexity requirement for the problem. In our case, we have tried different number and different kinds of indicators for our algorithm. The final indicators in Table 1 for the experiments in Section 5. Note that depending on different target PII attributes to protect, these indicators can be replaced by others. For this particular experiment setup, there are roughly two kinds of them. Indicators 1,2,3,4,7 are universal indicators that preserve that its properties that are independent of the target PII attributes set, while the rest are target dependent indicators. We utilize this hybrid approach for the learning framework in this work.

	Indicator of Choice
1	The number of highly important PII attributes.
2	The number of moderately important PII attributes.
3	The number of exposed PII attributes that have 10+ children.
4	The number of exposed PII attributes that have 10+ parent.
5	The number of PII attributes that are on the driver's license.
6	The number of PII attributes to perform a credit card fraud.
7	The number of PII attributes to that has a high (top 10%) prior probability of being exposed.

Table 1. The indicator of choice in our financial data breach experiment. Two kinds of indicators are used, indicator $1, 2, 3, 4$ and 7 are universal indicators that may be reused for other data breach scenario. Indicator $4, 5$ and 6 are experiment related indicators. For different kinds of identity theft categories, these indicators can be swapped to other ones for better learning results.

4.2 Temporal Difference Reinforcement Learning

As mentioned in the previous section, in the dynamic Identity Ecosystem, a person's identity status is defined by the combination of 627 PII attributes. However, just as any other real world reinforcement learning problem, it is impossible to apply naive learning algorithms directly to solve the optimal strategy since we have $O(2^{627})$ of these states to cover.

In our case, in which we conduct a Monte Carlo type of simulation, we have the estimated transition distribution to every connected state in the system through querying the original UT CID Identity Ecosystem. In this case, the problem is more like solving the optimal strategy of a game where the state space is extremely large. Some common approaches to these type of problems are value function approximation [11], sparse sampling techniques, and policy gradient [20] in which the complexity of the algorithm is independent of the size of the state space. In this work, we adopt the temporal difference (TD) reinforcement learning with function approximator to solve the problem. While other techniques may have different results in performance, we choose this method to incorporate our existing knowledge of a person's identity [26]. For example, in most of the states of a person's identity, the probability of a PII attribute being exposed in the near future is mostly low with the order of 10^{-3}. The number of PII attributes that have a decent probability compared to the others (which we refer to as "at risk") is limited in most cases. In this case, approximating the state as related to low risk PII attributes can be very helpful. In the reinforcement learning context, these type of network structure are often referred to as indicators. We pick 7 indicators as follows based on the knowledge and analysis of the UT CID Identity Ecosystem to fit in our algorithm.

5 Results

In this section, we discuss the results of the experiments as well as its real world interpretation. In the first part, results for understanding the strategies we are producing are provided. We show that the generated strategy is indeed better in performance in some common sense reference strategies like idling or pure random strategy. Finally, we transform three different popular real world defense strategy into our system against an efficient attacker utilizing the minimax attack strategy. The result are compared to the active protection strategy for the final evaluation to determine the performance gap.

5.1 What are we learning from the experiments?

First, we demonstrate a financial PII evaluation utilizing dynamic Identity ecosystem and the proposed learning algorithm. Notice that for every identity theft incident in the real world, it can translate to different target PII attributes set in our analysis. From ITAP, we have 627 different PII attributes which we choose the ones that are closely related to credit card frauds as our target PII attributes. The selected PII attributes are listed in Table 1. In the experiment, the target PII attributes are supposed to be protected from the malicious attacker with various defense strategies that the user adopt. The goal is to benchmark different defense strategies against the effective attack strategies targeting these crucial PII attributes. In our first evaluation, we compared three different which the detailed description of the strategies are presented in Table 2.

	Defense Strategy
Optimal defense	Strategy from solving the stochastic shortest path game indicates the best PII attributes to recover
Random	From all the PII attribute it can choose, uniformly choose one to recover.
No defense	No PII attributes were selected during the game

Table 2. Artificial Strategies Comparison: Three artificial strategies used in the experiment.

First, we look at how a person's identity behaves in real life. In this scenario, we do not adopt any defense strategies to the identity and there is no attacker in the system. PII attributes are exposed due to daily life activities like filling out forms on the Internet or taking a survey. The identity on average survives 100.16 rounds in the setup. Next, we add in the attacker. Note that in this case, the attacker is adopting the minimax strategy as explained in the previous section. In short, rather than aggressively maximizing the effort of identity attacking, the strategy is instead guaranteeing the result of each attack as if there is someone on the other side actively protecting the target PII attributes. When the identity is under attack without any defense measure, the round of survival is down to

34.47. Next, a defense strategy is adopted by the identity owner. The defender in this case took advantage of the knowledge to the structure of the UT CID Identity Ecosystem. In this case, the rounds of survival goes up to 49.48 as shown in Figure 4. We also put in a random defense strategy from the user to adapt as a reference case. The average round of survival in this case is 36.54. As one might expect, it is almost as bad as no defense for the identity we wish to protect.

The round of survival evaluation is averaged from repeating the experiment for 100 times for each scenario. In order to claim that one strategy is significantly stronger than the other, we conduct hypothesis testing with the ones we are interested to show that one is statistically larger than the other.

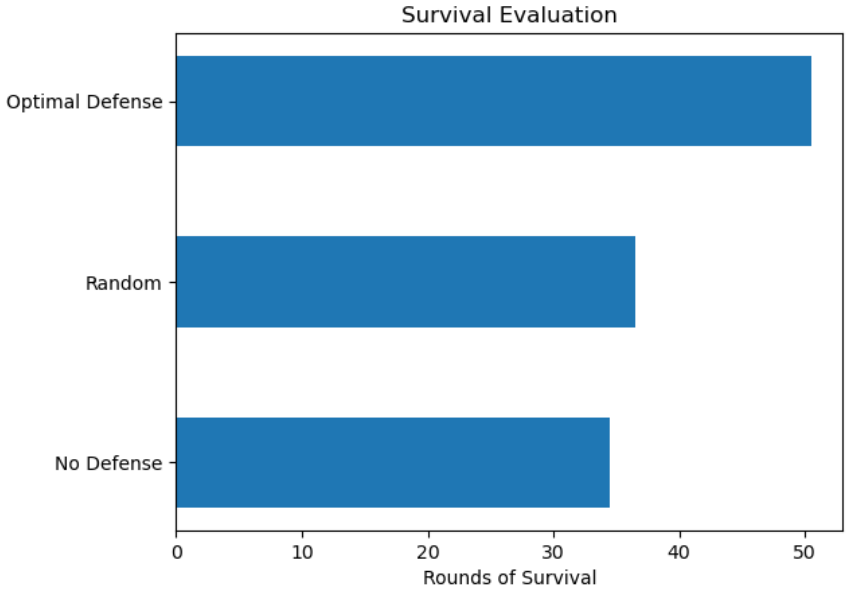

Fig. 4. The survival analysis result of three artificial strategies. Given that the attacker is using its optimal strategy, if the user does not take action, the number of rounds of survival goes from 100.16 to 34.47. If a random strategy is adopted by the user, the number of round of survival is 36.54. In the case that a good defense strategy is adopted, the number of round of survival can go up to 49.48.

We also introduce three different strategies that are closely representing what most commercial company are adopting today. The major difference between the three is the choice of PII attributes to monitor which the choices are often different from company to company. The PII attributes to monitor in each of the passive defense strategies are listed in Table 3. Passive A and B corresponds to strategies adopted by paid identity protection service while Passive C corresponds to a free identity protection service.

	Monitored PII attributes List
Passive A	’Bank_Account_Information’, ’Name’, ’Social_Security_Number’, ’Credit_Card_Number’, ’Line_of_Credit’, ’Wire_Transfer_Amount’, ’Court_Documents’, ’1099_Form_Information’, ’Employment_Status’
Passive B	’Social_Security_Number’, ’Court_Documents’, ’1099_Form_Information’, ’Bankruptcy_Report’, ’Forged_Document_Information’, ’Employment_Status’, ’Voiceprint’, ’Arrest_History’, ’Court_Document’, ’Name’
Passive C	’Name’, ’Address’, ’Social_Security_Number’, ’Line_of_Credit’, ’e-Medical_Record’, ’Financial_Statement’

Table 3. Real world passive monitor strategy setup.

The survival evaluation compared to optimal strategy Figure 5 shows that how these strategies are performing against a smart attacker who has the knowledge of how PII attributes associate with one another. We can see these strategies are not performing well compared to the optimal strategy generated from the algorithm. Suppose we are only evaluating these strategies with their corresponding survival rounds. One rule of thumb we can observe immediately is that the more connected PII attributes a specific passive strategy is monitoring, the better the protection it is. Notice here in order to defend the identity network efficiently, covering as many strongly connected PII attributes as possible is obviously a good choice. For a specific type of criminal activity, which corresponds to a specific target PII attribute set in our analysis, it is also very important that the PII attributes covered by surveillance should include as many PII attributes that are connected to target PII attributes as possible. Passive strategy A is the one has the most coverage and the most covered PII attributes that are connected to target PII set. Although Passive B is also a strategy with large coverage, most of the coverage from the set are more connected to court related PII attributes. Passive C is the strategy used by some free protection service with the most basic coverage hence the poor performance. It is worth mentioning that these strategies are all real world related as they are all passive monitor strategies that current real world companies are using.

5.2 Discussion

From the results in the previous section, there are several interesting results that we want to point out. First of all, there exists a gap between the optimal active protection strategy and common passive monitor protection strategies. This suggests there is room to improve these strategies the companies are adopting right now. Such improvement can be done by carefully choose the PII attributes to monitor. For example, from UT CID Identity Ecosystem, we can actually find PII attributes that are closely related to certain identity theft incidents to better enhance the defense against certain type of incident. On the other hand, the experiment result from last section only shows the capability of these real world strategies against a credit card fraud type of identity theft incident. How

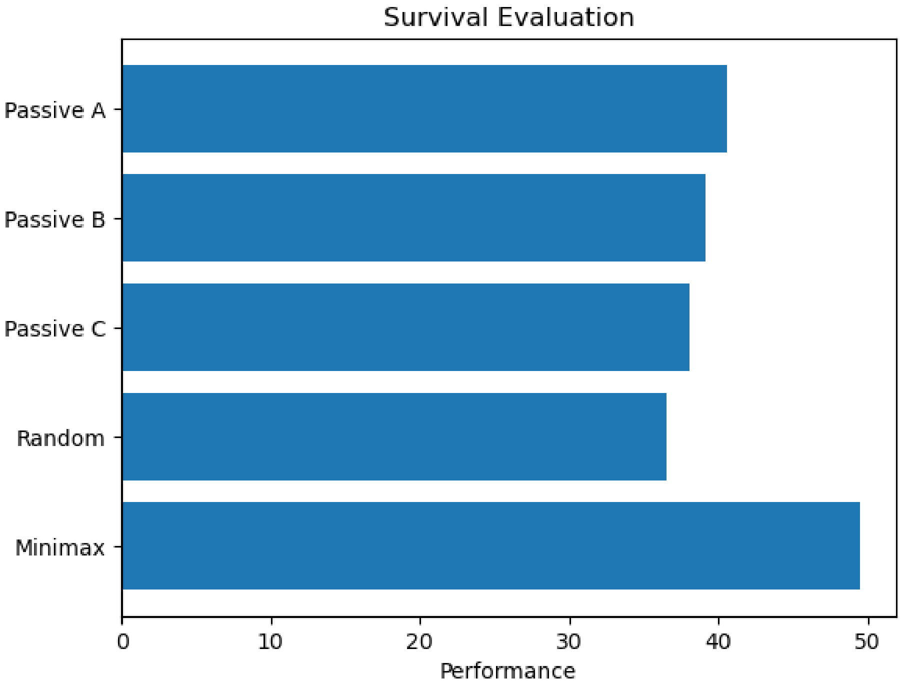

Fig. 5. The survival analysis result of three real world strategies against a malicious attacker in a financial fraud scenario. The actual PII attributes under surveillance for different strategies are provided in Table 3. In this experiment, Passive A is the most effective it has a average survival round difference of 2 compared to the strategy that is not effective. We can also observe a clear gap between the optimal defense strategy and these passive monitor strategies.

these different identity protection service provider strategies performed against identity theft in general needs more work and criminal story analysis to justify.

Second, we can now compare and analyze different strategies quantitatively utilizing the framework. We can further estimate the effectiveness of strategies against different kinds of identity theft incidence like credit card theft or medical identity theft. This also suggests that one can utilize the framework to exploit the weakness of a strategy while improving it.

We would also like to point out that our random strategy in the experiment is actually not a practical strategy which is why it is categorized as an artificial strategy. It is listed here as a reference to better understand the identity theft defense problem. As mentioned in the previous section, it is nearly impossible or cost-heavy to recover some of the PII attributes because its nature. For instance, we seldom see a person change his/her name because of identity theft and fraud. In our experiment, we do exclude some of the PII attributes so that once it is exposed, it cannot be recovered while we did not have enough data to classify the level of cost to recover. This is also the main reason why in the real world, the monitoring list for important PII assets are usually a relatively small subset of the PII attributes in the UT CID Ecosystem.

6 Conclusion

This research offers a tool bringing together the UT Center for Identity Ecosystem, game theory, Markov decision processes, and reinforcement learning to generate and evaluate the best strategy in the real world for defending against the theft of personal identity information. This research proposes a simulation-based Dynamic UT CID Identity Ecosystem to evaluate and evolve the efficacy of different identity protection strategies, mainly comparing different strategies to passive strategies employed in many commercially offered identity protection products. The system can also be a universally applicable tool for evaluating and recommending identity protection strategies. It can also be used as an evaluation of one system against different types of identity theft incidents. In the future, the work can develop into a foundation to understand how initial exposure of individual PII attributes evolves into crucial PII breaches over time in terms of the dynamic integrity of a person's identity ecosystem.

References

1. Abouheaf, M.I., Lewis, F.L., Mahmoud, M.S., Mikulski, D.G.: Discrete-time dynamic graphical games: model-free reinforcement learning solution. Control Theory and Technology **13**, 55–69 (2015)
2. Bertsekas, D.P.: Reinforcement learning and optimal control. Athena Scientific Belmont, MA (2019)
3. Chang, K.C., Zaeem, R.N., Barber, K.S.: Enhancing and evaluating identity privacy and authentication strength by utilizing the identity ecosystem. In: Proceedings of the 2018 Workshop on Privacy in the Electronic Society. pp. 114–120. ACM (2018)
4. Chang, K.C., Zaeem, R.N., Barber, K.S.: Internet of things: Securing the identity by analyzing ecosystem models of devices and organizations. In: 2018 AAAI Spring Symposium Series. pp. 111–116 (2018)
5. Chen, C.J., Zaeem, R.N., Barber, K.S.: Statistical analysis of identity risk of exposure and cost using the ecosystem of identity attributes. In: 2019 European Intelligence and Security Informatics Conference (EISIC). pp. 32–39. IEEE (2019)
6. Federal, T.C.: Consumer sentinel network data book 2019 (2020), https://www.ftc.gov/enforcement/consumer-sentinel-network/reports
7. Geramifard, A., Walsh, T.J., Stefanie, T., Chowdhary, G., Roy, N., How, J.P.: A Tutorial on Linear Function Approximators for Dynamic Programming and Reinforcement Learning. Now Foundations and Trends (2013)
8. House, T.W.: Safeguarding against and responding to the breach of personally identifiable information. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf
9. IdentityForce: https://www.identityforce.com/

10. of Justice Statistics, U.S.D.o.J.O.o.J.P.B.: National crime victimization survey: Identity theft supplement, 2016 (2019). https://doi.org/10.3886/ICPSR36829.v1, https://doi.org/10.3886/ICPSR36829.v1
11. Konidaris, G., Osentoski, S., Thomas, P.: Value function approximation in reinforcement learning using the fourier basis. In: Proceedings of the Twenty-Fifth AAAI Conference on Artificial Intelligence. p. 380–385. AAAI'11, AAAI Press (2011)
12. Kushner, H.J., Chamberlain, S.G.: On stochastic differential games: Sufficient conditions that a given strategy be a saddle point, and numerical procedures for the solution of the game. Journal of Mathematical Analysis and Applications **26**(3), 560 – 575 (1969). https://doi.org/https://doi.org/10.1016/0022-247X(69)90199-1, http://www.sciencedirect.com/science/article/pii/0022247X69901991
13. Liau, D., Zaeem, R.N., Barber, K.S.: An evaluation framework for future privacy protection systems: A dynamic identity ecosystem approach. In: Proceedings of the 12th International Conference on Agents and Artificial Intelligence, ICAART 2020, Volume 1, Valletta, Malta, February 22-24, 2020. pp. 136–143 (2020). https://doi.org/10.5220/0008913501360143
14. Lifelock: https://www.lifelock.com/
15. Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A.A., Veness, J., Bellemare, M.G., Graves, A., Riedmiller, M., Fidjeland, A.K., Ostrovski, G., Petersen, S., Beattie, C., Sadik, A., Antonoglou, I., King, H., Kumaran, D., Wierstra, D., Legg, S., Hassabis, D.: Human-level control through deep reinforcement learning. Nature **518**(7540), 529–533 (Feb 2015). https://doi.org/10.1038/nature14236, https://doi.org/10.1038/nature14236
16. Patek, S., Bertsekas, D.: Stochastic shortest path games. SIAM Journal on Control and Optimization **37**(3), 804–824 (1999). https://doi.org/10.1137/S0363012996299557, https://doi.org/10.1137/S0363012996299557
17. Rana, R., Zaeem, R.N., Barber, K.S.: Us-centric vs. international personally identifiable information: A comparison using the ut cid identity ecosystem. In: 2018 International Carnahan Conference on Security Technology (ICCST). pp. 1–5. IEEE (2018)
18. Rana, R., Zaeem, R.N., Barber, K.S.: An assessment of blockchain identity solutions: Minimizing risk and liability of authentication. In: 2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI). pp. 26–33. IEEE (2019)
19. Shapley, L.S.: Stochastic games. Proceedings of the National Academy of Sciences **39**(10), 1095–1100 (1953). https://doi.org/10.1073/pnas.39.10.1095, http://www.pnas.org/content/39/10/1095
20. Sutton, R.S., McAllester, D., Singh, S., Mansour, Y.: Policy gradient methods for reinforcement learning with function approximation. In: Proceedings of the 12th International Conference on Neural Information Processing Systems. p. 1057–1063. NIPS'99, MIT Press, Cambridge, MA, USA (1999)
21. Watchdog, I.: https://www.idwatchdog.com/home
22. Yu, H.: Stochastic shortest path games and q-learning (2014)
23. Zaeem, R.N., Budalakoti, S., Barber, K.S., Rasheed, M., Bajaj, C.: Predicting and explaining identity risk, exposure and cost using the ecosystem of identity attributes. In: 2016 IEEE International Carnahan Conference on Security Technology (ICCST). pp. 1–8 (Oct 2016). https://doi.org/10.1109/CCST.2016.7815701
24. Zaeem, R.N., Manoharan, M., Barber, K.S.: Risk kit: Highlighting vulnerable identity assets for specific age groups. In: 2016 European Intelligence and Security Informatics Conference (EISIC). pp. 32–38. IEEE (2016)

25. Zaeem, R.N., Manoharan, M., Yang, Y., Barber, K.S.: Modeling and analysis of identity threat behaviors through text mining of identity theft stories. Computers & Security **65**, 50–63 (2017)
26. Zaiss, J., Zaeem, R.N., Barber, K.S.: Identity Threat Assessment and Prediction. Journal of Consumer Affairs **53**(1), 58–70 (March 2019). https://doi.org/10.1111/joca.12191, https://ideas.repec.org/a/bla/jconsa/v53y2019i1p58-70.html

WWW.IDENTITY.UTEXAS.EDU