International Conference on Cloud Computing, Big Data and Blockchain

Evolutionary game analysis on permission request policy of service providers

Junlin Jin
Key Lab of Network Security and Cryptology
Fujian Normal University, China
e-mail: 396295937@qq.com

Ayong Ye
Key Lab of Network Security and Cryptology
Fujian Normal University, China
e-mail: yay@fjnu.edu.cn

Zhijiang Yang
Department of Computer Engineering
Zhangzhou Vocational and Technical College, China
e-mail: zjyangg@126.com

Xu Li
Key Lab of Network Security and Cryptology
Fujian Normal University, China
e-mail: xuli@fjnu.edu.cn

***Abstract*– In view of the problem of over-requesting permissions in the current smartphone terminal, it is great significant to research the factors of the service providers to select the permission request policy. In this paper, we assume that providers are bounded rational and obtain the payoff matrix based on the two groups of providers with different request policies, which are the "Over-request Permissions" and "Request basic permissions". Then we establish an evolutionary game model for privacy protection between the two groups and find out the stability policy of the model. Initial results demonstrate that whether the provider adopts the "Request basic permissions" policy depends on four factors, which are revenue increase ratio, credit loss, users churn cost and self-attractiveness when over-requesting permissions. And the establishment of privacy alarm mechanism not only can improve the users' privacy awareness, but also increase the users churn cost when providers over-requesting permissions.**

Keywords – evolutionary game, privacy protection, permission, policy

I. INTRODUCTION

Smartphone app markets have undergone explosive growth in recent years. Various app markets offer a wide range of apps in all aspects of human life, such as social life, smart travelling, health care and so forth. Android app markets, which share the largest user base, have gained a tremendous momentum over the past years since its first launch in 2008. A market research has shown that the worldwide downloads of smartphone apps have reached 19 billion in the first quarter of 2018[1]. As users rely more on smartphone apps, the privacy and security problems become more prominent. For service providers and users, over-requesting permissions is one of the most serious problems in the current smartphone terminal. Previous research[2] has shown that more than 70% of smartphone apps request to collect information irrelevant to the main function of the app. Rich personal information has a significant economic value that constitutes an incentive for increasing the amount of user information collected. Thus, in the absence of external constraints, the economic value drives the providers to request more permissions than the minimum required to deploy a given effectively and securely. These providers can not only steal user's privacy information, but also bring about financial loss of the users by making phone calls and sending messages secretively. Indeed, many smartphone users are concerned about the behavior of service providers over-requesting permissions, and researchers also suggest that privacy has become an important factor in the competitive market for service providers[3].

In this paper, we assume that each provider is bounded rationality and introduce the evolutionary game theory to construct the evolutionary game model of the two providers on the choice of request policy. With using the stability principle of the differential equation to analyze the mechanism of action between the providers, we can find out the evolutionary stability policy and the corresponding condition. Finally, we use Matlab to carry out the simulation research, which can intuitively reflect the evolution direction and verify the correctness of the evolutionary game model. The corresponding privacy protection policies and recommendations can be put forward based on the

results of our analysis. Compared with existing protection methods for smartphones, our main contributions are as:

• To the best of our knowledge, we are the first to apply evolutionary game into research permission request policy of service providers, which can fundamentally solve the problem of over-requesting permissions.

• The results of our analysis have proven that establishing a privacy alarm mechanism can spontaneously push service providers to only request basic permissions.

II. REALATED WORK

Previous research more emphasis on privacy issues in the android operating system because of its huge market and the vulnerability of Android application. From the perspective of life cycle, these applications usually go through the 5 phases which are development, download, installation, runtime and uninstallation phases. And the current research on privacy protection focuses on the download, installation, runtime phases. During the download phase, many researchers propose a number of alternative privacy instructions aiming at guiding users to download apps which are less intrusive. For example, Kraus et al.[4] provided a visualization of permission-related statistical data to enable the users to assess the security of the app. The approach proposed by Harbach[5] to leverage the rich set of personal information available on smartphones and use personalized examples to communicate risks. Moreover, Lin et al.[6] explored users' mental models of smartphone privacy by crowdsourcing users' expectations of apps' sensitive resource usage. During the installation and runtime phases, Enck et al.[7] presented a security service named Kirin in Android, where they pre-define a set of potentially dangerous combinations of permissions and refuse to install the apps which request such combinations. They also proposed TaintDroid[8], a system-wide dynamic taint tracking multiple sources of privacy information. In addition, Thanigaivelan et al.[9] proposed CoDRA, an access control system that offers context-based highly fine-grained policy and dynamically reconfigurable control to enforce various policy configurations at different levels of system operations.

As an important branch of economics, game theory has been widely used in the research of predicting individual behavior and analyzing their optimization policies. Zhou et al.[10] surveyed the theories, methods and applications on how game theory is applied in privacy protection. Piero et al.[3] revealed that provider competition can reduce such information requests with a game-theoretic approach. Zhang et al.[11] proposed a pricacy protection model based on game theory from the point of view of realizing benefits from the access with the goal of allowing access to a certain extent while denying further access when disclosure of privacy is about to happen.

III. BASIC ASSUMPTIONS AND MODEL BUILDING

In a natural environment that does not consider other constraints, the providers of the same service are treated as a system in which there are two different bounded rationality groups 1 and 2, and the app developed by each provider is highly homogeneous. The providers in group 1 and 2 are randomly sampled to match and game. The members extracted from Group 1 are called provider A, and the members extracted from group 2 are called provider B. Because both the provider A and B are bounded rationality, it is difficult to make the optimal permission request policy in a decision. Therefore, the policy adjustment between A and B is a dynamic process that is constantly changing. To simplify the problem, we only consider a 2×2 game, that is, the policy space of providers in group 1 and 2 is {Over-request permissions, Request basic permissions}. "Over-request Permissions" indicates that the most of permissions are not necessary for the purpose of providing the service, while "Request basic permissions" indicates that the app developed by the provider only requests permissions dependent on the provision of personalized services. Next we further make the following assumptions:

(1) The proportion of providers which Over-request permissions is x ($0 \le x \le 1$), and that of providers which request basic permission is $1- x$ in group 1. Similarly in group 2, the proportion of providers which Over-request permissions is y ($0 \le y \le 1$), and that of providers which request basic permission is $1- y$.

(2) Suppose both the provider A and B adopt the "Request basic permissions" policy, their normal payoffs are $R_a, R_b, R_a > 0, R_b > 0$;

(3) Suppose both the provider A and B adopt the "Over-request Permissions" policy, their payoffs are $R_a+\alpha R_a-C_a-V_a$, $R_b+\beta R_b-C_b-V_b$. This is the reason that providers can acquire and mine users' privacy information more, but need to take some risks of users churn and credit loss when requesting permissions excessively. α and β indicate the ability of the provider A and B to increase their own payoff by requesting more permissions respectively. The higher the value is, the stronger the ability to increase payoffs. C_a and C_b indicate the risks of users churn of the provider A and B, while V_a and V_b indicate the risks of credit loss of the provider A and B respectively. C is an increasing function of V.

(4) When the provider A and B adopt the "Over-request permissions" and "Request basic permissions" policies respectively, the payoff of the provider A is $R_a+\alpha R_a-C_a-V_a$. Some of the users who have been lost from the customers of the provider A have two choices. One is no longer using the similar service provided by any provider, and the other is to use the same service provided by the provider B. As a result, the payoff of the provider B is $R_b+k_bC_a$, where k_b represents

the attractiveness of the provider B to the users lost by the provider A.

(5) When the provider A and B adopt the "Request basic permissions" and "Over-request permissions" policies respectively, similar to (4), the payoffs of the provider A and B is $R_a+k_aC_b$, $(1+\beta)R_b-C_b-V_b$.

Based on the above hypothesis, the payoff matrix of evolutionary game is constructed, as shown in table 1.

Table 1 The payoff matrix of evolutionary game.

Provider A \ Provider B	Over-request Permissions	Request basic permissions
Over-request Permissions	$(1+\alpha)R_a-C_a-V_a$, $(1+\beta)R_b-C_b-V_b$	$(1+\alpha)R_a-C_a-V_a$, $R_b+k_bC_a$
Request basic permissions	R_a+kC_b, $(1+\beta)R_b-C_b-V_b$	R_a, R_b

IV. ECOLUTIONARY GAME ANALYSIS

A. *The equilibrium point of evolutionary game*

The expected payoffs U_{A1} and U_{A2} of the provider A adopting the "Over-request permissions" and "Request basic permissions" policy are:

$$U_{A1} = y[(1+\alpha)R_a-C_a-V_a]+(1-y)[(1+\alpha)R_a-C_a-V_a] \quad (1)$$

$$U_{A2} = y(R_a+k_aC_b)+ (1-y)R_a \quad (2)$$

Then the average payoff U_A of the provider A is:

$$U_A = xU_{A1}+(1-x)\ U_{A2} \quad (3)$$

According to the Malthusian dynamic equation, the replicated dynamic equation of the provider A is:

$$F(x)=\frac{dx}{dt}=x(U_{A1}-U_A)=x(1-x)(\alpha R_a-C_a-V_a-yk_aC_b) \quad (4)$$

Similarly, the expected payoffs U_{B1}, U_{B2} and the average payoff U_B are respectively:

$$U_{B1} = x[(1+\beta)R_b-C_b-V_b]+(1-x)[(1+\beta)R_b-C_b-V_b] \quad (5)$$

$$U_{B2} = x(\ R_b+k_bC_a)+ (1-x)R_b \quad (6)$$

$$U_B = yU_{B1}+(1-y)\ U_{B2} \quad (7)$$

Then the replicated dynamic equation of the provider B is:

$$F(y)=\frac{dy}{dt}=y(U_{B1}-U_B)=y(1-y)(\beta R_b-C_b-V_b-xk_bC_a) \quad (8)$$

According to the above two replicated dynamic equation, the two-dimensional dynamical system (*I*) of the evolutionary game can be obtained:

$$\begin{cases}\dfrac{dx}{dt}=x(U_{A1}-U_A)=x(1-x)(\alpha R_a-C_a-V_a-yk_aC_b)\\ \dfrac{dy}{dt}=y(U_{B1}-U_B)=y(1-y)(\beta R_b-C_b-V_b-xk_bC_a)\end{cases} \quad (9)$$

To facilitate the following analysis, let $x=\frac{\beta R_b-C_b-V_b}{k_bC_a}$, $y=\frac{\alpha R_a-C_a-V_a}{k_aC_b}$, $\alpha_1=\frac{C_a+V_a}{R_a}$, $\alpha_2=\frac{k_aC_b+C_a+V_a}{R_a}$, $\beta_1=\frac{C_b+V_b}{R_b}$, $\beta_2=\frac{k_bC_a+C_b+V_b}{R_b}$. And it is easy to derive the following properties.

Proposition 1

The equilibrium points of the system (*I*) are (0,0), (0,1), (1,0), and (1,1), and when $\alpha_1<\alpha<\alpha_2$, $\beta_1<\beta<\beta_2$, (x_D, y_D) is also the equilibrium point of the system (*I*).

Prove: For the system (*I*), let $F(x)=\frac{dx}{dt}=0$, $F(y)=\frac{dy}{dt}=0$, we can find out that (0,0), (0,1), (1,0), (1,1) are the equilibrium point of the system (*I*). When $\alpha_1<\alpha<\alpha_2$ and $\beta_1<\beta<\beta_2$, $0<x_D<1$, $0<y_D<1$. As seen by $F(x)=\frac{dx}{dt}=0$, $F(y)=\frac{dy}{dt}=0$, (x_D, y_D) is also the equilibrium point of the system (*I*).

B. *Stability analysis of equilibrium points*

The five equilibrium points calculated by the replicated dynamic equations are not necessarily the evolutionary stability policy of the System (*I*). The stability of equilibrium points can be obtained by analyzing the local stability of the Jacobian matrix1[12], which can be formulated as:

$$J=\begin{bmatrix}\dfrac{\partial F(x)}{\partial x} & \dfrac{\partial F(x)}{\partial y}\\ \dfrac{\partial F(y)}{\partial x} & \dfrac{\partial F(y)}{\partial y}\end{bmatrix}=\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix} \quad (10)$$

Where $a_{11}, a_{12}, a_{21}, a_{22}$ are respectively:

$a_{11} = (1-2x)(\alpha R_a - C_a - yk_aC_b)$, $a_{12} = -x(1-x)k_aC_b$,

$a_{21} = -y(1-y)k_bC_a$, $a_{22} = (1-2y)(\beta R_b - C_b - xk_bC_a)$.

If the elements in *J* satisfy the following two conditions, the equilibrium point of replicated dynamic equation is called the evolutionary stability policy.

(1) $tr(J)= a_{11} + a_{12} < 0$; (11)

(2) $\det(J)=\begin{vmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix}=a_{11}a_{22}-a_{12}a_{21}>0$; (12)

Proposition 2

(1) When $0<\alpha<\alpha_1$, $0<\beta<\beta_1$, (0,0) is the evolutionary stability point of the game model.

(2) When $0<\alpha<\alpha_1$, $\beta_1<\beta<\beta_2$, (0,1) is the evolutionary stability point of the game model.

(3) When $\alpha_1<\alpha<\alpha_2$, $0<\beta<\beta_1$, (1,0) is the evolutionary stability point of the game model.

(4) When $\alpha>\alpha_2$, $\beta>\beta_2$, (1,1) is the evolutionary stability point of the game model.

(5) When $\alpha_1<\alpha<\alpha_2$, $\beta_1<\beta<\beta_2$, both (0,1) and (1,0) are the evolutionary stability points of the game model.

Prove: According to the above prove method, the symbol of the trace and determinant of the Jacobian matrix *J* in

each equilibrium point can be calculated to determine its local stability. The evolutionary stability analyses in 5 cases are shown in table 2, based on different value of α and β, where "ESS" represents evolutionary stability policy or point, "SP" represents saddle point and "USP" represents unstable point.

Table 2 The evolutionary stability analyses.

	Condition	number	equilibrium points	*tr*(*J*)	*det*(*J*)	conclusion
Case 1	$0<\alpha<\alpha_1$ $0<\beta<\beta_1$	4	(0,0)	–	+	ESS
			(0,1)	uncertain	–	SP
			(1,0)	uncertain	–	SP
			(1,1)	+	+	USP
Case 2	$0<\alpha<\alpha_1$ $\beta_1<\beta<\beta_2$	4	(0,0)	uncertain	–	SP
			(0,1)	uncertain	–	ESS
			(1,0)	–	+	SP
			(1,1)	+	+	USP
Case 3	$\alpha_1<\alpha<\alpha_2$ $0<\beta<\beta_1$	4	(0,0)	uncertain	–	SP
			(0,1)	uncertain	–	SP
			(1,0)	–	+	ESS
			(1,1)	+	+	USP
Case 4	$\alpha>\alpha_2$ $\beta>\beta_2$	4	(0,0)	+	+	USP
			(0,1)	uncertain	–	SP
			(1,0)	uncertain	–	SP
			(1,1)	–	+	ESS
Case 5	$\alpha_1<\alpha<\alpha_2$ $\beta_1<\beta<\beta_2$	5	(0,0)	+	+	USP
			(0,1)	–	+	ESS
			(1,0)	–	+	ESS
			(1,1)	+	+	USP
			(x_D,y_D)	uncertain	–	SP

V. SIMULATION ANALYSIS

In order to show the evolutionary game process of two providers more intuitively, and verify the correctness of the evolutionary game model, the evolutionary stability policy of different model parameters in the game process is analyzed by using MATLAB r2015b.

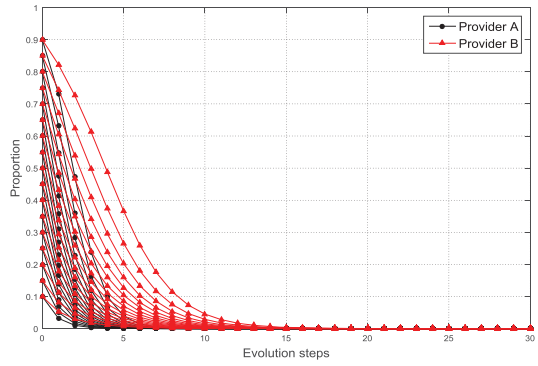

Figure 1. Simulation results for stability point (0,0)

When $0<\alpha<\alpha_1$, $0<\beta<\beta_1$, the evolutionary stability point of the game model is (0,0). Supposing $R_a = R_b = 5$, $C_a = C_b = 1$, $V_a = V_b = 0.5$, $k_a = k_b = 0.5$, $\alpha = 0.1$, $\beta = 0.2$, it can meet $0<\alpha<\alpha_1$, $0<\beta<\beta_1$. In order to verify the effectiveness of the evolutionary game model, the initial ratio of the provider A (group 1) and B (group 2) using the "Over-request permission" policy set to [10%, 90%] as step size is 0.05. The evolutionary results are shown in Figure 1. It can be obviously observed that the ratio of the "Over-request permissions" policy begins to decline gradually and tend to the evolutionary stability point (0,0) from the initial point with the increase of evolutionary steps. This means that the providers in both groups ultimately adopt the "Request basic permissions" policy. This phenomenon can be further explained as follows. When two groups are relatively low in their ability to increase their own payoffs, the providers who request permissions independent the service can't bring more benefits to themselves, instead of taking the risks of users churn and credit loss. Therefore, all providers will eventually adopt the "Request basic permissions" policy after constantly adjusting the policy. In addition, we can find that the proportion of the "Over-

request Permissions" policy in a group and the providers' ability to increase their payoffs are important factors that affect the convergence rate.

When $0 < \alpha < \alpha_1$, $\beta_1 < \beta < \beta_2$, the evolutionary stability point of the game model is (0,1). Supposing that $\alpha = 0.2$, $\beta = 0.36$ and other parameter settings are consistent with the above conditions, it can meet $0 < \alpha < \alpha_1$, $\beta_1 < \beta < \beta_2$. Similarly, the initial ratio of the provider A (group 1) and B (group 2) using the "Over-request permission" policy also set to [10%, 90%] as step size is 0.05. The evolutionary results are shown in Figure 2. The ratio of the "Over-request permissions" policy that the provider A adopted begins to decline gradually with the increase of evolutionary steps. On the contrary, the ratio of the provider B adopting the "Over-request permissions" policy begins to rise steadily and tend to the evolutionary stability point (0,1). It can be seen from the figure that when the gap between the two providers of the ability to increase the payoffs is relatively large, the advantage policy of the providers with higher ability is "Over-request permissions". They can unlock more value of users by requesting more permission and ignore the risks of users churn and credit loss. While the advantage policy of the others is "Request basic permissions", they can adopt the policy to attract the users who highly value the privacy information and provide their credibility, thereby increasing their revenues.

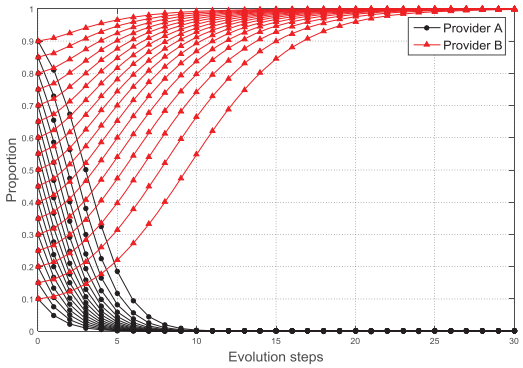

Figure 2. Simulation results for stability point (0,1)

When $\alpha > \alpha_2$, $\beta > \beta_2$, the evolutionary stability point of the game model is (1,1). Supposing that $\alpha = 0.5$, $\beta = 0.6$ and other parameter settings are consistent with the above two conditions, it can meet $\alpha > \alpha_2$, $\beta > \beta_2$. The evolutionary results are shown in Figure 3. The ratio of the "Over-request permissions" policy begins to rise gradually and tend to the evolutionary stability point (1,1) from the initial point with the increase of evolutionary steps. In this case, the revenues of the providers by requesting more permissions are greater than that by adopting "Request basic permissions" policy to attract high-sensitivity users. Therefore, all providers will eventually adopt the "Over-request permissions" policy after constantly adjusting the policy.

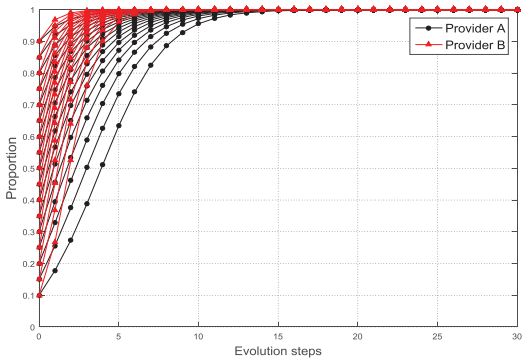

Figure 3. Simulation results for stability point (1,1)

VI. CONCLUSION

In this paper, we apply evolutionary game method to the privacy protection of smartphone and establish the evolutionary game model between service providers. Then we carry out an evolutionary simulation analysis by obtaining the replicated dynamic equation and evolutionary stability policy. In the process of repeated games, the two sides constantly adjust their policies according to their own profits and finally reach the stability policy. The results show that whether the provider adopts the "request basic permission" policy is closely related to the revenue increase ratio when over-requesting permissions. The revenue increase ratio is also collected with the cost of users churn and credibility loss and self-attractiveness. Whit the increase of the revenue increase ratio, it may occur that four evolutionary stability policies. In order to promote the evolution of the game model toward "Request basic permissions", the following two decisions can be taken.

(1) Set up the privacy alarm mechanism to improve the users' privacy awareness and increase the cost of users churn and credibility loss when the providers adopt the "Over-request Permissions" policy, which can spontaneously and effectively push providers to adopt the "Over-request Permissions" policy. The privacy alarm mechanism can be achieved through the improved methods such as Majid[13], G€okhan[14], etc.

(2) When the user churn of the provider's competitor with adopting the "Over-request Permissions" policy is large enough, the provider can increase their revenues by increasing their attractiveness, thereby guaranteeing their own benefits without violating users' privacy.

We have demonstrated that the privacy alarm mechanism can not only improve the users' privacy awareness, but also in turn to promote the provider to adopt the "Request basic permissions" policy. In our future work, we intend to consider how to establish a personalized and reasonable alarm mechanism.

REFERENCES

[1] A. Annie, “https://www.appannie.com/cn/insights/market-data/q1-2018-apps-record-downloads-spend/,” 2018.

[2] Cam, “http://www.cam.ac.uk/research/news/what-is-the-price-of-free.,” 2015.

[3] P. A. Bonatti, M. Faella, C. Galdi et al., "Towards a Mechanism for Incentivating Privacy." pp. 472-488.

[4] L. Kraus, I. Wechsung, and S. Moller, "Using Statistical Information to Communicate Android Permission Risks to Users." pp. 48-55.

[5] M. Harbach, M. Hettig, S. Weber et al., "Using personal examples to improve risk communication for security & privacy decisions." pp. 2647-2656.

[6] J. Lin, S. Amini, J. I. Hong et al., "Expectation and purpose:understanding users' mental models of mobile app privacy through crowdsourcing." pp. 501-510.

[7] W. Enck, M. Ongtang, and P. Mcdaniel, "On lightweight mobile phone application certification." pp. 235-245.

[8] W. Enck, P. Gilbert, B. G. Chun et al., “TaintDroid: an information flow tracking system for real-time privacy monitoring on smartphones,” Acm Transactions on Computer Systems, vol. 32, no. 2, pp. 1-29, 2010.

[9] N. K. Thanigaivelan, E. Nigussie, A. Hakkala et al., “CoDRA: Context-based Dynamically Reconfigurable Access Control System for Android,” Journal of Network & Computer Applications, vol. 101, 2017.

[10] Zhou D D, Li W W, Sun Y Q. “Survey on game theory based on privacy protection” Journal of Chinese Computers Systems, vol. 36, no. 12, pp. 2696-2700, 2015.

[11] Zhang Y X, He J S, Zhao B, Zhu N F. “A model of privacy protection based on game theory.” Chinese Journal of Computers, vol. 39, no. 3, pp. 615-627, 2016.

[12] D. Friedman, “Evolutionary Game in Economics,” Econometrica, vol. 59, no. 3, pp. 637-666, 1991.

[13] M. Hatamian, J. Serna, R. Kai et al., FAIR: Fuzzy Alarming Index Rule for Privacy Analysis in Smartphone Apps, 2017.

[14] G. Bal, R. Kai, and J. I. Hong, “Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns,” Computers & Security, vol. 53, pp. 187-202, 2015.