2004

Anonymizing Web Services through a Club Mechanism with Economic Incentives

Mamata Jenamani

Leszek Lilien

Bharat Bhargava
Purdue University, bb@cs.purdue.edu

Report Number:
04-008

ANONYMIZING WEB SERVICES THROUGH A CLUB MECHANISM WITH ECONOMIC INCENTIVES

Mamata Jenamani
Leszek Lilien
Bharat Bhargava

Department of Computer Sciences
Purdue University
West Lafayette, IN 47907

CSD TR #04-008
February 2004

Anonymizing Web Services through a Club Mechanism with Economic Incentives*

Mamata Jenamani
mamatajenamani@yahoo.co.in

Leszek Lilien
llilien@cs.purdue.edu

Bharat Bhargava
bb@cs.purdue.edu

Department of Computer Sciences
Purdue University, West Lafayette, Indiana

Abstract
Preserving privacy during Web transactions is a major concern for individuals and organizations. One of the solutions proposed in the literature for preserving privacy is by adopting a system that helps in maintaining anonymity through group cooperation during Web transactions. The lack of understanding of incentives for encouraging group cooperation is a major drawback in adopting such systems. We propose an anonymizing club mechanism, and sequential economic strategy for trusted collaboration. We model the individual transactions as a Prisoners' Dilemma, where two players either cooperate or defect while maintaining each other's anonymity. The activities of the participants over a series of transactions can be modeled as a sequential repeated game. We determine conditions to ensure cooperation among the participants in the sequential repeated game, even if defecting is a dominant strategy in each individual Prisoners' Dilemma game. Our results show that by adopting an appropriate initiation fee and adequate fine for malicious behavior, both enforced through a trusted central authority, we can sustain cooperation in the proposed anonymizing club mechanism.

Keywords: Anonymity, privacy, Web services, economic incentives, Prisoners' Dilemma, sequential repeated game.

1. INTRODUCTION

Anonymizing Web services provide a solution for preserving privacy on the Web. Many intermediaries have come forward to provide such a service to the potential customers. This scenario is described in a W3C working draft [1]:

> A developer wishes to force an explicit message path through certain intermediaries - for instance, he might use an anonymizing intermediary to make a call to a specified remote service without allowing the target service to track the identity/IP of the caller. In this case, the intermediary is responsible for calling the target service and returning the results to the caller, using its own authentication credentials if any are required by the target service.

With so much concern for privacy preservation by individuals and organizations, such services are supposed to sell like hot cakes. On the contrary, with a notable exception [14], no such commercial services have been able to succeed. Besides technical factors, many social and economic reasons contribute to the difficulties in maintaining an anonymizing infrastructure [5][6].

Anonymity cannot be created by single interested individuals or organizations themselves. It requires participation from other Web nodes owned by other entities. The more nodes participate in mixing of the traffic, the bigger is the noise and the better is anonymity. Establishing and maintaining trust among a large number of nodes is the major bottleneck in sustaining such a framework. Each node in this framework is dependent on the other nodes for protecting its privacy. Adoption of an appropriate economic incentive scheme could be one of the solutions for managing distributed trust in this framework.

The single hop proxies (like Anonymizer [14]) can protect the end user from simple threats like profile-creating Web sites, but they cannot hide from the adversaries the traffic going through their sites. Analysis of incoming traffic can provide valuable information about the users of the intermediary proxies. Moreover, the user has to trust on intermediary for preserving his anonymity. So, this kind of anonymity infrastructure does not attract many privacy-concerned users or organizations.

Since traffic analysis is a major threat for maintaining anonymity, an *anonymizing club mechanism* – in which many nodes cooperate to maintain anonymity – emerges as an interesting alternative [9]. However, the failure of a commercial solution – Freedom Networks initiated by Zero Knowledge Systems [3] – may raise a question about the viability of such a scenario. The designers of this network admit [4] that the network failed because the company could not sell its services to a sufficient number of clients to

* This research was supported in part by NSF Grants IIS-0209059 and IIS-0242840

cover its costs. It is evident that inadequate economic analysis of this service was a major contribution to its failure.

In this paper we propose an economic scheme, using a game theoretic model, that can be used in a centrally controlled club mechanism to maintain trust amongst the nodes in sequential repeated transactions. The proposed club mechanism although centrally controlled, is more decentralized than in Freedom Network, where central authority collects all the fees and redistributes them to the node operators. The proposed scheme requires the participants to submit to the central authority only a one-time initiation fee and pay to it fines for misbehavior. We assume that any two nodes get equal benefits by using each others anonymizing services and thus need not be additionally paid. Our idea is analogous to the use of trusted third parties for trust building in online auction markets [12].

2. THE PROPOSED CLUB MECHANISM WITH SEQUENTIAL STRATEGY

We model individual transactions between any two nodes as a Prisoners' Dilemma game [13], where an individual player has an incentive to cheat. More precisely, each player is afraid of being cheated, and to maximize her benefit tries to cheat herself. Cheating emerges as the most rational alternative for each single interaction. However, when this game is played sequentially in a repeated manner, each player tries to maximize her average payoff for the whole sequence. We derive the conditions under which cooperation and not defection (cheating) becomes the dominant strategy of a player in the sequential game.

Since it is much more expensive to maintain decentralized trust, we include a *central authority* whom all the parties must trust. This central authority could be an outside trusted third party, or one of the club members who volunteers or nominated to perform this task. The central authority randomly matches any two club members for an anonymizing transaction. An anonymizing transaction involves two regular transactions, one from each member of the pair matched by the central authority. The central authority also can resolve conflicts between any two nodes.

We call the proposed mechanism an *anonymity club*, since a group of nodes come together with a promise to provide each others anonymity. We call each club member an *agent.* We propose a sequential strategy analogous to [12]. We assume that each agent is rational and will try to maximize his payoff in the sequential game.

The proposed sequential strategy relies on the following rules:

1. An individual or an organization becomes a club member by paying a one time initiation fee F to the central authority.
2. Using some matching strategy [8], the central authority brings two members together to be partners for an anonymizing Web transaction during the *time period* t[1]. We assume that no cost is involved in running this matching algorithm.
3. During the *anonymizing transaction* two members receive a benefit P_t each by maintaining anonymity and using each other's service.
4. During the transaction each partner has two strategies: cooperate or defect. So, each stage represents a Prisoners' Dilemma (explained in the following section).
5. If Alice feels that Bob cheats her, she reports it to the central authority claiming a loss P_{claim} suffered by her due to violation of her privacy.
6. The central authority investigates the fraud and both parties are asked to show the evidence to prove themselves innocent.

   If fraud is confirmed, Bob pays a fine f and P_{claim}, Alice gets compensation P_{claim} and the central authority gets fine f. Otherwise, Alice is charged with a false complaint and pays fine g to the central authority.
7. The culprit who does not pay a fine or a compensation is expelled from the club.

2.1 Prisoner's Dilemma Played at Each Stage

Let P_t be the *benefit from privacy protection* received by an agent within time period t. Therefore, it is justified to treat $-P_t$ as the cost of privacy violation if it is suffered by an agent during that period. Let l_t be the *benefit from disclosing the privacy of another agent* within time period t.

We assume here that both partners have symmetric privacy needs. That is, all the parties have equal costs and benefits associated with anonymous transactions. They also have equal number of requests for anonymizing. We also assume that the benefit from privacy protection is higher than the benefits received by sacrificing the partner's privacy (i.e. $P_t > l_t$). We assume that P_t's are independently identically distributed random variables with a common distribution P. We define P_{max} as a value beyond which distribution P has no positive probability density, that is, we use the value P_{max} as an estimate of the maximum possible benefit received by a cooperating agent. $E(P)$ is the expectation of P.

We hold a similar assumption for the random variable l_t. We also define l_{max} as an estimate of the maximum possible benefit received by a defecting agent.

[1] We use t and not Δt for time period for convenience.

At each stage each agent has two choices: either to defect (D) or to cooperate (C). If agents cooperate with each other, then both are going to receive a benefit P_t resulting from privacy protection. If one of the agents defects and the other cooperates, then the cooperating agent's privacy is violated and she suffers a loss of $-P_t$. On the other hand, the defector's privacy is preserved and he receives a benefit l_t that increases his total benefits to $P_t + l_t$ during the time period t. If both defect then neither of the agents' privacy is preserved, so each bears a loss of $-P_t$ but receives a benefit of l_t. The resulting payoff matrix from this game is shown in Figure 1.

Even though cooperation maximizes the total payoff for both players taken together, the fear of cheating by the partner induces defection behavior by any of the partners at an individual stage. So, the only Nash equilibrium for both players in this game is to defect. That is, the payoff of any agent who deviates from the equilibrium strategy reduces.

	C	D
C	P_t , P_t	$-P_t$, $P_t + l_t$
D	$P_t + l_t$, $-P_t$	$-P_t + l_t$, $-P_t + l_t$

Figure 1. Payoff structure of the Prisoner's Dilemma game

2.2 An Agent's Time-Weighted Average Payoff

We have to consider an infinite repeated game for which we need to evaluate the time-weighted average payoff of an agent.

The value of the future earning expressed in today's currency is smaller (e.g with interest rate i=5% per annum, \$105 next year is equivalent to \$100 this year). Consequently, all future earnings must be discounted. We use δ as the *discount factor*, $0 < \delta < 1$. It is defined as $\delta = \frac{1}{1+i}$, where, i is the interest rate.

We can define an agent's time-weighted average payoff $\bar{v}$ over a sequence of transactions [2][12] using the following relationship:

$$V = \sum_{t=0}^{\infty} \delta^t v_t = \sum_{t=0}^{\infty} \delta^t \bar{v}$$

where V is the *total (lifetime) payoff*, and v_t is the payoff stream for time period t, where t=1,2,... . Using the formula for the sum of the geometric series we get from this:

$$\bar{v} = (1-\delta)V$$

Since the payoff stream for all time periods has a constant time-weighted average payoff, maximizing V is equivalent to maximizing $\bar{v}$. In other words, if the agent maximizes his time-weighted average payoff, he will also maximize his total payoff (i.e. his lifetime payoff). This will provide him incentive for cooperation (not cheating) in that period even though defection is the dominant strategy at each stage, as described in the discussion of the Prisoner's Dilemma game.

3. ANALYSIS OF THE ECONOMIC INCENTIVES FOR ENABLING THE CLUB MECHANISM

We now can discuss the conditions under which the agents will cooperate in a repeated sequential game, even though each non-repeated game results in defection as the equilibrium strategy.

In our propositions and proof, while evaluating total payoff sometimes we have to consider the payoff from the current transaction at time period t_0 separately from payoff from future periods starting from t_1. It is necessary because conditions like giving initiation fee or paying the fine for the malicious behavior occur only in the current time period t_0.

The total payoff starting from period t_0 is:

$$E[P_0 + P_1\delta + P_2\delta^2 + P_3\delta^3 + ...] = \frac{E(P)}{1-\delta}$$

whereas, when starting from t_1, it is:

$$E[P_1\delta + P_2\delta^2 + P_3\delta^3 + ...] = \frac{\delta E(P)}{1-\delta}$$

where P_i is the payoff in the time period t_i.

Proposition 1: An agent will join the proposed anonymizing club if the initiation fee (given at time period t_0) is less than the difference between his total future payoff from this service (starting from time period t_1) and the maximum future payoff from adopting any other privacy preserving technology, i.e. if the following inequality is satisfied:

$$F < \frac{\delta E(P) - \bar{a}}{1-\delta}.$$

where $\bar{a}$ is the maximum of all expected payoffs from any other privacy-preserving technology available at that time period.

Proof: If the agent joins the club, he contributes F to the club fund at time period t_0 and receives benefits from time period t_1 onwards making the total payoff

$$V = -F + \sum_{t=1}^{\infty} P_t \delta^t$$

So, the time-weighted average payoff of the agent is:

$$\bar{v} = -(1-\delta)F + (1-\delta)E[P_1\delta + P_2\delta^2 + P_3\delta^3 + ...]$$

As $t \to \infty$, we get:

$$\bar{v} = -(1-\delta)F + \delta E(P)$$

An agent will join the club if his lifetime average payoff is greater than the maximum of all expected payoffs, $\bar{a}$, from any other alternative privacy-preserving mechanisms available at that time period, that is, if:

$$-(1-\delta)F + \delta E(P) > \bar{a}$$

Hence, we get:

$$F < \frac{\delta E(P) - \bar{a}}{1-\delta}$$

Interestingly, since the average payoff from the alternative service is $\bar{a}$, the total payoff starting from time period t_0 from that service turns out to be $\sum_{t=0}^{\infty} \delta^t \bar{a} = \frac{\bar{a}}{1-\delta}$. □

Proposition 2: An agent will cooperate at every stage in the sequential repeated game if the maximum value of the benefit from the cheating behavior is less than the total future payoff (from t_0) minus the maximum payoff achievable in the current transaction, i.e. if the following condition is satisfied:

$$l_{max} < \frac{E(P)}{1-\delta} - P_{max}$$

Proof: If an agent at certain stage defects, is found guilty, and does not pay the fine, his club membership will be revoked. Therefore, although his present payoff is (P_t+l_t) (from Figure 1) his future payoff will be 0 for not availing the service. So, a rational agent will prefer to cooperate starting at time period t_0 if his total payoff from cooperating exceeds his total payoff from defecting, that is, if:

$$(1-\delta)E[P_0 + P_1\delta + P_2\delta^2 + P_3\delta^3 + ...] > (1-\delta)(P_0 + l_0) + 0$$

Hence, we get:

$$E(P) > (1-\delta)(P_0 + l_0)$$

Considering the upper bounds for P and l, the condition becomes:

$$E(P) > (1-\delta)(P_{max} + l_{max})$$

Hence:

$$l_{max} < \frac{E(P)}{1-\delta} - P_{max}$$ □

This result has an interesting interpretation. If an agent considers his expected benefit $E(P)$ from the proposed service to be very high, then it provides him a very high incentive for cooperation.

Proposition 3: A defector who is proven guilty is willing to pay the fine if it is lower than the difference between his total future payoff (starting from t_1) and the compensation claimed by his partner, i.e. if the following condition is satisfied:

$$f < \frac{\delta E(P)}{(1-\delta)} - P_{claim}$$

Proof: If a defector does not pay the fine, his club membership will be revoked, and he can no more avail the service. Thus, his payoff will be 0 in all future transactions. His present payoff will be (P_t+l_t) (from Figure 1). If his total payoff from not paying the fine exceeds his payoff from paying the fine, then he will prefer not to pay. Consequently the condition for paying the fine (starting from current time period t_0) is that the total payoff after paying the fine exceeds total payoff after not paying the fine, that is:

$$(1-\delta)(P_0 + l_0 - f - P_{claim}) + (1-\delta)E[P_1\delta + P_2\delta^2 + P_3\delta^3 + ...] > (1-\delta)(P_0 + l_0) + 0$$

Equivalently:

$$(1-\delta)(P_0 + l_0) - (1-\delta)(f + P_{claim}) + \delta E(P) > (1-\delta)(P_0 + l_0)$$

Hence:

$$f < \frac{\delta E(P)}{(1-\delta)} - P_{claim}$$ □

Proposition 4: If a player's complainant is proven false, he is willing to pay the fine imposed on him if it is lower than his total future payoff (starting from t_1), i.e. if the following condition is satisfied:

$$g < \frac{\delta E(P)}{(1-\delta)}$$

Proof: Arguing in the similar manner as above, we can justify that the condition for paying fine by a false complainant is that the total payoff with paying the fine exceeds total payoff after not paying the fine, i.e.:

$$(1-\delta)(P_0 - g) + (1-\delta)E[P_1\delta + P_2\delta^2 + P_3\delta^3 + ...] > (1-\delta)P_0 + 0$$

Hence:

$$g < \frac{\delta E(P)}{(1-\delta)} \qquad \square$$

Theorem: The proposed sequential strategy is an equilibrium strategy if the fine is imposed following conditions in Propositions 3 and 4, i.e., if:

$$f < \frac{\delta E(P)}{(1-\delta)} - P_{claim}$$

and

$$g < \frac{\delta E(P)}{(1-\delta)}$$

The average payoff for an agent in this strategy is:

$$\bar{v} = \delta E(P) - (1-\delta)F \, .$$

Proof: Based on Propositions 3 and 4, if the above two conditions are satisfied at each time period t_i, then - based on the optimality principle of dynamic programming [15] - we know that one time deviation from the proposed strategy will not be profitable for any rational agent. So, the agents will cooperate and will receive an average payoff $\delta E(P) - (1-\delta)F$ (following the arguments of the proof of Proposition 1). $\square$

4. RELATED WORK

In a sequential game each player is assumed to be sequentially rational. Every decision in the sequential game must be a part of an optimal strategy for the remainder of the game. So, unlike the equilibrium in a non-sequential game where each player has a single strategy, a sequential equilibrium emphasizes formation of a player's belief about the other player at each stage of the game [7].

Economics community has emphasized adopting extra legal mechanisms, like community enforcement by maintaining social norms [8]. The concept of community enforcement emphasizes that when the agents change their partners over the time, the dishonest Bob's behavior against Alice causes sanctions against Bob not only by Alice but also by other members of the society. These sanctions can be regarded as the enforcement of social norms. Such norms can be hard to maintain if no effective mechanism for information dissemination or enforcement of honest behavior is adopted. In this paper we use the central authority to disseminate information and enforce honest behavior. Similar approach has been used by Ba *et al.* [12] to build trust in the online auction markets.

Different anonymizing services adopt different types of infrastructure for providing anonymity to its users [9]. Every type of infrastructure has inherent costs and benefits associated with it. The costs include the fixed costs for deploying the service, and the dynamic cost for maintaining the service. Lack of analysis of economic incentive mechanisms is seen as a primary factor in the failures of anonymity infrastructures [4].

Acquisti *et al.* [9] built the foundation for an economic study of the viability of an anonymity infrastructure. They propose a model where messages are passed through an anonymizing mix-net. The model distinguishes between honest and dishonest nodes and captures the costs and benefits of anonymous transactions. Though they argue on the importance of a decentralized anonymity infrastructure, they admit the difficulty of providing such a structure due to the coordination problems. They suggest establishing a central coordination authority to redistribute the payments. Our strategy takes the issue further by partially decentralizing the payment structure, so the central authority is not involved in payments for individual transactions. It deals with the membership fees and fines only.

Another example of maintaining cooperation using an economic incentive mechanisms are peer-to-peer networks [10]. The trust can be maintained in such systems through the use of shared and private histories of the transactions. Also in this case the difficulty of devising decentralized mechanisms (for example, sharing the private history) is admitted.

5. CONCLUSION AND FUTURE WORK

The paper proposes the idea of an anonymizing club Web service, a rational sequential strategy, and determines the conditions for cooperation amongst the participants of this anonymizing Web service. The strategy assumes the presence of a trusted third party for information dissemination and for sustaining cooperation. The strategy is simple and independent of any underlying architecture. It may be adopted and suitably modified for any framework.

The proposed strategy can be improved in many ways.:

1. The central authority may not give fair judgment every time. The judgment may be biased towards a particular agent. So the consideration of agent's belief in the fairness of the central authority could improve the model.
2. Consideration of the fixed costs associated with starting the service would make the strategy more realistic.
3. It may be required to define the minimum number of participants starting a club so that their initiation fees cover the necessary fixed cost. This will make the implementation more realistic.
4. Our assumption of no cost involved in running the matching algorithm is also quite strong. To accommodate this cost, another variable cost, such as annual club membership, may be included.

5. The probabilistic modeling of cheating behavior of individual agents could also improve the strategy.

6. We assume that different agents, who come together to form a club, have equal privacy concerns. Therefore, all the parties have equal costs and benefits associated with anonymizing transactions. The effect of the Prisoners' Dilemma game may be substantially different if the parties have unequal benefits from utilizing the service. This issue may be investigated.

7. We also assume equal number of anonymizing transactions by all the club members. So, in a sequential repeated game scenario such inequality may bring the *tragedy of the commons* [11]. This is a situation where a "higher" beneficiary will use the resources of a "lower" beneficiary frequently. Hence, the "lower" beneficiary will end up providing services without receiving equal benefits. It will be interesting to investigate this issue.

ACKNOWLEDGEMENT: The authors gratefully acknowledge the helpful comments of Mohamed Hefeeda that improved this work.

REFERENCES:

[1] Web Services Architecture Usage Scenarios, W3C Working Draft 14 May 2003, http://www.w3.org/TR/ws-arch-scenarios/

[2] A Mas-Colell., M. Whinston, J. Green, *Microeconomic Theory*, Oxford Univ. Press, New York, NY, 1995.

[3] I. Goldberg and A. Shostack. "Freedom Network 1.0 Architecture and Protocols. Zero-Knowledge Systems," White Paper, November 1999, http://www.homeport.org/~adam/zeroknowledgewhitepapers/arch-tech.pdf

[4] A. Shostack, "People Won't Pay for Privacy," *Workshop on Privacy Enhancing Technologies PET2003* Dresden, Germany, March 2003, http://petworkshop.org/2003/slides/wip/shostack-PET2003-wip.pdf

[5] J. Feigenbaum, M. J. Freedman, T. Sander, and A. Shostack, "Economic Barriers to the Deployment of Existing Privacy Technologies" (Position Paper), *Proceedings of the Workshop on Economics and Information Security*, Berkeley, CA, May 2002, http://www.homeport.org/~adam/econbar-wes02.pdf

[6] R. Dingledine, "Why is anonymity so hard?," *Workshop on Privacy Enhancing Technologies PET2003*, Dresden, Germany, March 2003, http://www.freehaven.net/doc/blackhat02/slides-bh02.pdf

[7] D. Kreps, R. Wilson, "Sequential equilibria," *Econometrica*, 50 (1982), pp.863– 894.

[8] M. Kandori, "Social norms and community enforcement," *Review of Economic Studies*, 59 (1992), pp.63–80.

[9] A. Acquisti, R. Dingledine, P. Syverson, "On the Economics of Anonymity," *Seventh International Financial Cryptography Conference*, Gosier, Guadeloupe, January 2003.
http://freehaven.net/doc/fc03/econymics.pdf

[10] K. Lai, M. Feldman, I. Stoica, J. Chuang, "Incentives for Cooperation in Peer-to-Peer Networks," *Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, June 2003.

[11] G. Hardin, "The Tragedy of the Commons," *Science*, 162 (1968), pp.1243-1248.

[12] S. Ba; A.B. Whinston, H. Zhang, "Building trust in online auction markets through an economic incentive mechanism," *Decision Support Systems*, 35(3), 2003, pp. 273 - 286

[13] D. Fudenberg and J. Tirole, *Game Theory*, MIT Press, Cambridge, MA, 1991.

[14] Anonymizer, http://www.anonymizer.com, February 2003.

[15] Bellman, R., *Dynamic Programming*, Princeton University Press, Princeton, NJ, 1957.