Enhancing Anonymity via Market Competition

Shouhuai Xu
Department of Computer Science
University of Texas at San Antonio
shxu@cs.utsa.edu

William Robert Nelson Jr.
School of Management
University at Buffalo
wrnelson@buffalo.edu

Ravi Sandhu
George Mason University and
NSD Security
sandhu@gmu.edu

Abstract

Anonymity is an important issue in the cyberspace community. Previous solutions typically rely on a well-defined trust structure – a set of distributed trustees among whom at least a quorum are supposed to be honest. We argue that the establishment of such a distributed trust structure is beyond the scope of technology itself. We propose an institutional framework within which service providers compete to provide high quality anonymity, and users can customize their anonymity according to their personal priorities. The major contribution of this paper is the incorporation of market competition into anonymity system models.

1. Introduction

People trust post offices not to open their letters and trust banks not to open their safe deposit boxes, though both the post office and the banks are technically capable of corrupting their customers' privacy. In the brick and mortar world, this kind of trust has historically played a larger role than technology in providing anonymity. However, such a trust structure is currently not available in the internetworked digital world. In this paper, we argue that *market competition* can facilitate the provision of anonymity in cyberspace, and develop an institutional framework in which service providers (at application layer and/or communication layer) compete to provide high quality anonymity service.

1.1. Background

Anonymous communications. The acceptance of the Internet as a means of communication is creating previously inconceivable opportunities for gathering information about individuals due to properties of the Internet Protocol (IP). While an IP address does not necessarily identify an individual, it is possible to link even dynamically configured IP addresses to an average customer. A lot of attention has been paid to the issue of anonymous communication [4, 18, 15, 16]. Perhaps the simplest solution to anonymity is to use a proxy, a single server that accepts connections from an initiator and forwards them to the responder (i.e., the host that the initiator wants to contact anonymously). The initiator's anonymity is preserved, since all the receivers learn only the proxy's address.

There have been some proposals to enhance the anonymity provided by the single proxy solution. One is Onion Routing [18], which is based on Chaumian MIX-network [4]. In Onion Routing, an initiator begins by choosing a route consisting of onion routers to the responder such that the routers communicating over an encrypted channel cooperate by forwarding data to the responder. Data is wrapped in a series of encrypted layers that are peeled-off by the onion routers along the path towards the responder. For each router on the path, the initiator constructs a layer of data consisting of the IP address of the next onion router and other cryptographic information. The inner-most layer of the onion contains the identity of the responder and the data to be sent. When the packet reaches the last onion router in the path, the data is forwarded directly to the responder.

Anonymous applications. In many application systems, user anonymity is always desirable. However, perfect anonymity may be impractical to deploy due to legal and national security reasons [19, 10]. Therefore, researchers have been pursuing conditional anonymity at the application layer (e.g., conditionally anonymous e-cash [2] and authentication [10]). In such an application, if there exists a single party that is able to revoke the users' anonymity,

Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)
0-7695-2108-8/04 $ 20.00 © 2004 IEEE

this party has to be completely trusted. To avoid this single point of anonymity failure, cryptographic techniques like threshold cryptosystems [5] have been used to implement more robust anonymity. We call this enhanced anonymity *parallel anonymity*. Another approach to enhancing anonymity, which we call *sequential anonymity*, is typically used in anonymous e-cash systems [17, 9, 13] to emulate the chain of paper money in circulation (therefore, a user can gain better anonymity via a chain of sequential exchanges).

1.2. Motivation and Contribution

Let's first consider a typical scenario in the context of anonymous communications. When you point URL to the (hypothetical) website $www.fun.com$ that releases free digital content, the server can easily get your IP address as well as track the information you download. Since you worry about your privacy, you want to hide the facts "when you visit it" and "what you download from it." The next step for you is to find some service like "hiding your IP address when you surf the Internet." Suppose you find from some search engine an (also hypothetical) website called $www.hideyourIP.com$, which is supposed to play the role of a (say, http) mix server or proxy. Now the problem is: "why should you trust this website?" Since everybody can easily establish many websites (in contrast to the difficulty of establishing a malicious post office or bank in the physical world), its owner may gain profits by trading your privacy secretly. Even if you find another website $www.reallyhideyourIP.com$ and you naively think using both of them in sequence will give you better anonymity, what will happen if they are owned by the same bad guy?

In the context of anonymous applications, each one in a set of the so-called trustees (e.g., parallel anonymity) is equipped with partial revocation capability. In spite of its appearance, this does not enhance customers' anonymity at all if they are under the jurisdiction of a single authority. Another simple yet typical threshold structure of $(t+1, 2t+1)$ is also problematic if the trustees are under the control of two different parties, since one of them is able to revoke anonymity without the participation of the other. Even if the trustees are under the jurisdiction of multiple parties, they may still collude for certain purposes.

The above analysis shows that current solutions to anonymous communications and applications are based on the assumption that a certain quorum of parties are trusted (i.e., either the very single proxy, or a quorum of proxies). However, such a well-defined trust structure is currently not available and it may take a long time to establish. This is justified by the controversy in the *key escrow* initiative [1] (just imagine what will happen if two government agencies can technically corrupt people's privacy!). Inspired by these observations, we propose incorporating *market competition* into anonymity system models to discourage parties having partial revocation capability from colluding. Specifically, we propose an institutional framework in which service providers compete (for their own profits or revenues) to provide high quality anonymity, and users can customize their anonymity according to their personal priorities.

Outline. In section 2, we present our framework and analyze its feasibility from an economics perspective. In section 3, we demonstrate how to incorporate market competition into anonymous communication systems. We conclude in section 4 with some open questions. Due to space limitation, we leave to the full version of this paper [20] the discussions on incorporating market competition into anonymous application systems.

2. Enhancing Anonymity via Market Competition: A Framework

2.1. The Framework

We propose an institutional framework in which market competition facilitates the provision of anonymity and customers pay service providers for providing anonymity service. The discipline imposed by market competition will force providers to provide high quality anonymity service. Competitive markets are generally characterized by large numbers of buyers (or customers) and sellers (or service providers) such that service providers compete for customers on the basis of price and quality.

Suppose there are a set of service providers P_1, P_2, $\cdots$, P_n and a set of customers $C_1, C_2, \cdots, C_m$. The P_i's compete for customers and each C_i is able to select her service providers. More specifically, P_i competes on the price p_i it offers and the quality q_i of anonymity service S_i it provides, where q_i may be based on multiple factors (see detailed discussions in Section 2.2). Suppose there is a price mechanism PM for determining the prices p_1, p_2, $\cdots$, p_n for the service S_1, S_2, $\cdots$, S_n provided by P_1, P_2, $\cdots$, P_n, respectively. That is, $p_i = PM(i, \langle P_1, S_1, q_1\rangle, \cdots, \langle P_n, S_n, q_n\rangle, C_1, \cdots, C_m)$. Prospective profit motivates P_i to provide high quality anonymity service. Collusion among providers is one threat to individual anonymity, but this is unlikely to persist if many providers are competing in the market (see "economics analysis" below).

Remark. In our market competition framework, no single service provider is technically able to revoke the anonymity of any customer, unlike in a single proxy system. Many competitive service providers will prevent the emergence of monopoly in this competition model.

2.2. Economics Analysis of the Framework

We analyze the feasibility of the above framework from an economic perspective. Although the customers currently may not have perfect information concerning the quality of anonymity they are being served, we argue with both theory and empirics that the providers will still compete for customers by offering high quality anonymity service.

Economic theory states that service providers that are making money will not rip off current customers thereby risking their future cash flow. The necessary condition for the producer to provide high quality products (when selling low quality products is referred to as cheating) is [11]: "Cheating will be prevented and high quality products will be supplied only if firms are earning a continual stream of rental income that will be lost if low quality output is deceptively produced. The present discounted value of this rental stream must be greater than the one-time wealth increase obtained from low quality production." Denote by C_h the service provider's cost of producing a high quality product, C_l the firm's cost of producing a low quality product, F_t^h the cash flow the firm anticipates earning in future periods if it provides high quality goods in the current period, F_t^l the cash flow the firm anticipates earning in future periods if it provides low quality goods in the current period, K_t the rate at which a firm discounts future cash flows, and N the final period under consideration by the firm. If $C_h - C_l < \sum_{t=1}^{N} \frac{F_t^h - F_t^l}{(1+K_t)^t}$, then firms will sell a high quality product in the current period. The left side of the inequality, the difference between the cost of producing a high rather than a low quality product, describes the immediate increase in cash flow a firm will receive if it sells a low quality product. The right side of the inequality describes the difference in the present value of future cash flows a firm is expected to earn if it sells a high quality rather that a low quality product. If a service provider reaps an immediate benefit by selling a low quality product in this period, it will suffer the long-term consequences of reduced discounted future cash flow.

This inequality clarifies two insights. One, the greater the immediate gain by cheating the more likely a service provider is to provide low quality service. Two, the more sensitive future cash flow is to current cheating, the less likely a service provider is to provide low quality service. For the above inequality to be true the future cash flow must be sensitive to current service quality which in turn requires that consumers are able to learn about service quality. Consumers often learn about service quality in one of three ways: learn from experience, learn from others, or learn from professional rating agencies.

- It has been shown that if a single repeat customer can occasionally identify service quality, then a service provider has the incentive to provide high quality service, because if consumers know the probability with which they can detect low quality, then they can calculate the true percentage of the time that a service provider is providing low quality. As a result, the incentive for a service provider to provide high quality service remains [6].
- Similarly, if customers share service quality information with each other, cheating one customer is like cheating them all and will have a greater adverse effect on future business than if consumers do not communicate [11].
- Professional rating agencies also provide service quality information, linking service providers' future sales to their current service quality. Such rating agencies are Underwriters Laboratories (paid for by providers) and Consumer Reports (paid for by consumers). So long as service quality information is received by future customers, from current customers, service providers will provide high quality service, even if consumers often fail to identify service quality. See [12] for an excellent discussion. If consumer to consumer information channels are ineffective because consumers are unwilling to identify themselves, then the quality monitoring role of professional rating agencies relative to information transmitted between consumers will increase.

In addition to the above theoretical argument, we present an example, in which agents and merchants are respectively analogous to service providers and customers in the context of this paper. The Maghribi merchants of the middle ages formed coalitions to facilitate information sharing and to punish cheaters. Trusted agents could conduct merchants' shipping, quality assessment, and bribery more efficiently than merchants could themselves. But the agents had to be trusted. Due to the uncertainty involved in shipping across the Mediterranean Sea in the middle-ages, merchants were often unable to identify cheating agents. Merchants formed coalitions to provide agents the incentive to act in a trustworthy manner. Typically, the rules of a coalition stated that if an overseas agent ever cheated any member of the coalition, no member of the coalition would ever employ that agent again. This rule increased the expected cost of cheating for agents by insuring that merchants shared information and reduced the use of cheating agents. Merchants apparently understood the condition stated above. The merchant will offer the agent an optimal premium—the lowest cost premium for which the long-run gain is not less that the short-run gain [8]. The Maghribi merchants were able to use reputation to increase opportunities for trade and efficiency.

There are many modern examples where customers rely on reputation to motivate the sale of high quality service.

Universities are relied upon to certify the quality of students. When a firm hires a new lawyer, clients trust that the firm would not damage its own reputation by providing low quality legal services. The American Automobile Association certifies towing companies and garages, thereby helping consumers locate high quality goods [12]. Similar incentives will bear on service providers promising anonymity. The ease of sharing information and the plethora of choices consumers now enjoy will allow reputation to function even without formal coalitions.

In summary, if customers can learn about service quality, service providers will provide high quality service. Customers can be informed about service quality in several ways. They can make repeat purchases, share information on quality with each other, and use professional rating services that report product quality. Such rating agencies for anonymity do not yet exist, but the profit motive of both service providers and the rating agencies is the incentive for finding an innovative solution. The inability for customers to identify the anonymity of each transaction does not remove the incentive for service providers to compete to provide high quality of anonymity, so long as quality can be occasionally identified.

3. How to Enhance Anonymity at the Communication Layer

3.1. Chaumian MIX-Network

Suppose a route consists of l mix servers, $M_1, M_2, \cdots, M_l$, where M_i, $1 \leq i \leq l$, has a pair of public and private keys (pk_i, sk_i) with respect to some secure public key cryptosystem [7, 14]. Denote by $E_{pk_i}(\cdot)$, $1 \leq i \leq l$, the encryption function using public key pk_i. Let m be the message the user wants to send to the destination server $www.fun.com$, where m (e.g., a http request) may also be encrypted using the destination server's public key. Chaumian MIX-network works as follows.

- The user prepares and sends $E_{pk_1}(M_2, E_{pk_2}(\cdots(M_l, E_{pk_l}(www.fun.com, m))))$ to mix server M_1.
- M_1 decrypts the message received from the user to get $(M_2, E_{pk_2}(\cdots(M_l, E_{pk_l}(www.fun.com, m))))$. After appropriate processing (e.g., permuting the set of incoming messages after certain time of delay), M_1 sends $E_{pk_2}(M_3, E_{pk_3}(\cdots(M_l, E_{pk_l}(www.fun.com, m))))$ to mix server M_2.
- M_i, $2 \leq i \leq l-1$, decrypts the message received from M_{i-1} to get $(M_{i+1}, E_{pk_{i+1}}(\cdots(M_l, E_{pk_l}(www.fun.com, m))))$. After appropriate processing, M_i sends $E_{pk_{i+1}}(M_{i+2}, E_{pk_{i+2}}(\cdots(M_l, E_{pk_l}(www.fun.com, m))))$ to mix server M_{i+1}.
- The last mix server M_l decrypts the message received from M_{l-1} to get $(www.fun.com, m)$. After appropriate processing, M_l sends m to the destination server $www.fun.com$.

3.2. Incorporate Market Competition into Chaumian MIX-network

Without loss of generality, we assume there are n mix servers, $M_1, M_2, \cdots, M_n$, which are owned by n different parties, respectively. Moreover, we assume there is a price mechanism, according to which M_i charges a user $\$c_i$ for its anonymous communication service, where $1 \leq i \leq n$. A user can customize her anonymity by choosing (and paying) the mix servers based on her own personal priorities.

In order to simplify the presentation, we adopt a payment mechanism based on the perfectly anonymous e-cash scheme [3], by which a user can withdraw unconditionally anonymous e-coins $coin_i$ of denomination $\$c_i$, where $1 \leq i \leq n$. The e-coins can be issued by some bank, or even by the respective owners of the mix servers. In the following description, by paying an e-coin to M_i, we simply let a user send $coin_i$ to M_i without stating the details (e.g., which information of $coin_i$ is presented).

When a user wants to send a message m (e.g., a http request) to server $www.fun.com$, she chooses a route of $l \geq 1$ mix servers according to her preferences. Suppose the route consists of mix servers $M_{u_1}, M_{u_2}, \cdots, M_{u_l}$, where $1 \leq u_i \leq n$, $1 \leq i \leq l$. The extended Chaumian MIX-network works as follows.

- The user prepares and sends $E_{pk_{u_1}}(coin_{u_1}, M_{u_2}, E_{pk_{u_2}}(\cdots(coin_{u_{l-1}}, M_{u_l}, E_{pk_{u_l}}(coin_{u_l}, www.fun.com, m))))$ to mix server M_{u_1}.
- M_{u_1} decrypts the message received from the user to get $(coin_{u_1}, M_{u_2}, E_{pk_{u_2}}(\cdots(coin_{u_{l-1}}, M_{u_l}, E_{pk_{u_l}}(coin_{u_l}, www.fun.com, m))))$. M_{u_1} is paid $\$c_{u_1}$ via e-coin $coin_{u_1}$. After appropriate processing, M_{u_1} sends $E_{pk_{u_2}}(coin_{u_2}, M_{u_3}, E_{pk_{u_3}}(\cdots(coin_{u_{l-1}}, M_{u_l}, E_{pk_{u_l}}(coin_{u_l}, www.fun.com, m))))$ to mix server M_{u_2}.
- M_{u_i} decrypts the message received from $M_{u_{i-1}}$ to get $(coin_{u_i}, M_{u_{i+1}}, E_{pk_{u_{i+1}}}(\cdots(coin_{u_{l-1}}, M_{u_l}, E_{pk_{u_l}}(coin_{u_l}, www.fun.com, m))))$, where $1 \leq u_i \leq n$ and $2 \leq i \leq l-1$. M_{u_i} is paid $\$c_{u_i}$ via e-coin $coin_{u_i}$. After appropriate processing, M_{u_i} sends $E_{pk_{u_{i+1}}}(coin_{u_{i+1}}, M_{u_{i+2}}, E_{pk_{u_{i+2}}}(\cdots(coin_{u_{l-1}}, M_{u_l}, E_{pk_{u_l}}(coin_{u_l}, www.fun.com, m))))$ to mix server $M_{u_{i+1}}$.

- The last mix server M_{u_l} decrypts the message received from $M_{u_{l-1}}$ to get $(coin_{u_l}, www.fun.com, m)$. M_{u_l} is paid $\$c_{u_l}$ via e-coin $coin_{u_l}$. After appropriate processing, M_{u_l} sends m to the destination server $www.fun.com$.

3.3. Gain in Anonymity

Recall that each mix server is owned by a different party, which is paid for its anonymous communication service. On the other hand, users can customize their anonymity by choosing routes or mix servers according to their own priorities. Since no anonymity is possible if all the mix servers collude, we argue that our framework realizes the optimal anonymity one can expect. To see this, we need to guarantee that anonymity implemented in the extended anonymous communication system is at least as good as the underlying Chaumian MIX-network. This is true because the coins obtained in a perfectly anonymous withdrawal protocol leak no information (in an information-theoretical sense) of the users. Therefore, the nice property of Chaumian MIX-network [4] – any single constituent mix server is able to provide the secrecy of the correspondence between the inputs and the outputs of the entire route – is naturally inherited into our extension. (Note that one "honest" MIX server is indeed not enough, although this server knowing the users' private information will not leak it. This also suggests the need of multiple honest MIX servers inspired by their own revenues in market competition.) Additional gain in anonymity can be expected according to the economics analysis in section 2 (i.e., the parties are motivated not to collude).

4. Conclusion and Future Work

We have presented an institutional framework within which service providers compete for providing high quality anonymity service, and users are able to customize their anonymity according to their personal priorities. Our framework can be used to enhance anonymity in anonymous applications and/or anonymous communications.

There are two interesting questions for further investigation:

- How can an independent rating system evaluate the anonymity quality of different service providers? This is not trivial, since the rating system must also simultaneously preserve the anonymity of the system being evaluated.
- How can one detect the source of a privacy compromise? Unlike a bank abusing your money, the compromise of anonymity carries no information about its source.

References

[1] H. Abelson, R. Anderson, S. Bellovin, and et al. The risks of key recovery, key escrow, and trusted third-party encryption (second edition), available at http://www.cdt.org/crypto/risks98/.

[2] E. Brickell, P. Gemmell, and D. Kravitz. A forward-secure digital signature scheme. In *ACM-SIAM SODA*, pages 457–466, 1995.

[3] D. Chaum. Blind signatures for untraceable payments. In *Crypto'82*, pages 199–203.

[4] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *C. ACM*, 24:84–88, Feb. 1981.

[5] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In *Crypto'89*, pages 307–315.

[6] D. Fudenberg and D. Levine. Maintaining a reputation when strategies are imperfectly observed. *The Review of Economic Studies*, 59(3):561–579, 1992.

[7] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal on Computer and System Sciences*, 28(2):270–299, Apr. 1984.

[8] S. Greif. Reputation and coalitions is medieval trade: Evidence on the maghribi traders. *Journal of Economic History*, 49(4):857–882, 1989.

[9] M. Jakobsson. Mini-cash: A minimalistic approach to e-commerce. In *International Workshop on Public Key Cryptography*, pages 122–135.

[10] J. Kilian and E. Petrank. Identity escrow. In *Crypto'98*, pages 169–185.

[11] B. Klein and K. Leffler. The role of market forces in assuring contractual performance. *Journal of Political Economy*, 89(4):615–641, 1981.

[12] D. Klein. Quality and safety assurance: How voluntary social processes remedy their own shortcomings. *The Independent Review*, 2(4):537–555, 1998.

[13] D. Pointcheval. Self-scrambling anonymizers. In *Financial Cryptography'00*.

[14] C. Rackoff and D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Crypto'91*, pages 433–444.

[15] M. Reiter and A. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[16] C. Shields and B. Levine. A protocol for anonymous communication over the internet. In *ACM Computer and Communication Security*, pages 33–42, 2000.

[17] D. Simon. Anonymous communication and anonymous cash. In *Crypto'96*, pages 61–73.

[18] P. Syverson, D. Goldchlag, and M. Reed. Anonymous connections and onion routing. In *IEEE Security and Privacy'97*, pages 44–54.

[19] B. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computers & Security*, 11(6):581–583, 1992.

[20] S. Xu, W. Nelson, and R. Sandhu. Enhancing anonymity via market competition, full version of the present paper (available from the authors).