ANALYSIS OF POSITIVE INCENTIVES FOR PROTECTING SECRETS IN DIGITAL RIGHTS MANAGEMENT

Jianwen Xiang†, Weiqiang Kong†, Kokichi Futatsugi†
†, ‡Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi,Ishikawa 923-1292, Japan

Kazuhiro Ogata‡
‡NEC Software Hokuriku, Ltd.
1 Anyoji, Tsurugi, Ishikawa 920-2141, Japan

Keywords: Incentives, secret protection, digital rights management.

Abstract: A common problem to current DRM-based services that usually offer streaming digital content and support period pricing (monthly or yearly subscription) systems is how to prevent secret (e.g., account and password) sharing beyond authorized consumers. Traditional technical solutions such as binding the secrets with specific devices can only solve this problem to some extent at the cost of user's portability. Current legal measures also encounter some difficulties such as detecting the difference in the physical identity of the user. We propose a protocol, IBSPS (Incentives-based Secrets Protection System), to encourage the consumers to keep the secrets private rather than to share them among friends. With IBSPS, a content provider can also get more revenue by attracting more honest and authorized consumers in return, even the provider has to pay an amount of money as a positive incentive for the consumers to protect the secrets. An escrow service is used in IBSPS to receive registrations and allocate the incentive. We analyze this system and show that multiple registration and collusion between users can not get a higher payment than honest one-time registration and not sharing.

1 INTRODUCTION

In the past several years there has been an increasing interest in developing digital rights management systems (DRMSs), which make it possible for commercial publishers to distribute digital content, such as music and movie, electronically and safely. From the point of view of the content providers, they want to utilize DRMSs to distribute and sell products in a more efficient and cost-effective way, without destroying the copyright holder's revenue stream, i.e., trying to make any kind of illegal sharing and copying impossible by some technical protection measures. However, these methods usually contradict and harm the user's concerns to some extent, such as portability and fair use. In other words, current DRMSs do not take a good balance between the rights protection and convenient personal uses, and it can significantly reduce easy of use and may go *too* far by preventing generally accepted uses as concluded in (EC, 2002).

Unlike digital content files that can usually be protected from illegal copying by encryption and licenses management, sharing of account and password is more difficult to deal with and is especially a problem for providers who offer streaming content services and support period pricing (monthly or yearly subscription) methods. For instance, it is popular to share an account to watch streaming videos just for kindness or friendship, while this is not the case that the provider want to see. And with respect to streaming music service such as Napster that costs only 99¢ per month, sharing Napster passwords also seems to be a common practice among youngsters (MusicAlly, 2005).

Possible technical solutions and attempts to the password sharing problem include prohibiting simultaneous access with the same account, and binding each account with specific limited numbers of devices. The former is reasonable, but the latter again contradicts with the user's portability, which is similar to the idea of binding a license and content file with some specific devices. Moreover, both of them can only solve the problem to some extent, that is, even in an extreme case that an account can only be used on a specifical machine which largely harms the user's satisfaction, it still fails in case several guys share the common machine and account by turns.

Sharing password seems similar to the case that people share their purchased physical books or CDs among friends in a traditional way. However, it vio-

Xiang J., Kong W., Futatsugi K. and Ogata K. (2006).
ANALYSIS OF POSITIVE INCENTIVES FOR PROTECTING SECRETS IN DIGITAL RIGHTS MANAGEMENT.
In *Proceedings of WEBIST 2006 - Second International Conference on Web Information Systems and Technologies - Society, e-Business and e-Government / e-Learning*, pages 5-12
DOI: 10.5220/0001250000050012

lates most of the terms of services which usually state like that "each subscriber agrees that not to allow others to use her/his member name, password and/or account." Thus, the act could involve defeating a combination of technical and contractual access control measures (Mulligan et al., 2003).

A subtle analysis of potential legal risks for users who attempt to share account can be found in (Mulligan et al., 2003), which states that the structure of DRM applications may drive users seeking to engage in customary personal uses of copyrighted works toward legally *questionable* behavior. Unfortunately, there are also some difficulties for the providers to make a plausible claim against such account misuses, such as how to detect the difference in physical identities, and to meet some relatively high damage threshold (Mulligan et al., 2003). This is the reason that in practice, with regard to non-serious cases, the providers usually prefer contractually reserved self-help measures (e.g. terminating a suspicious account) to law.

Therefore, the point here is how to *encourage* the consumer to keep the secret (account and password) while not to share it among friends, since current technical solutions and legal measures are difficult to solve this problem perfectly as we discussed above. In the work described here, we propose an incentives-based secret protection system (IBSPS) to solve this problem. IBSPS can novelly transform the burden of secrets protection of content providers into the benefit of consumers, and thus stimulate them to keep the secrets private in their own interests.

IBSPS is suited for applications where a secret must be protected for only a limited period of time. A typical example is the accounts and passwords of online subscription services which usually have a period of validity (i.e., monthly or yearly subscription). Content files purchased from online shops are not considered in current IBSPS, because generally speaking, these files once purchased, will be valid for ever.

It should be noted that we do not want to use IBSPS to replace current terms-of-use policies, or other legal, technical protection measures. Rather, we aim to add IBSPS as an additional layer of protection for DRM systems that already have such safeguards.

1.1 Related Works

Our work was primarily inspired by SPIES (Margolin et al., 2004), which aims to provide an economic negative incentive to not share the secrets such as passwords. The main idea of SPIES is to require the consumer to place an additional security deposit into a trusted escrow account beforehand, and then if she shares the secret with other unauthorized users, she will totally lost some money in return. The mechanism is that, every one who has a copy of the secret (including the unauthorized users who got the shared copies from the authorized consumer and did not put corresponding deposits into the escrow account) can register to the escrow service and receive a share of the deposit after the secret protection period. A deposit payment function is proposed to guarantee that any kind of collisions or multiple registrations will result in totally losing money as for the authorized consumer.

The deposit idea of SPIES is derived from some traditional existing applications, such as entertainment reviews before the product is available to the general public. However, when it is applied to the password management of online subscription services, it has several limitations as follows.

First of all, the *additional* security deposit itself is a big disincentive for the user to choose such service. In SPIES, the deposit v is set to $v = c(n+1)$, where c is the price of the service, and $n(n > 2)$ is an estimated number of users sharing an account such that it will easily result in concurrent usage of the account detected by the provider. Correspondingly, SPIES assumes that the provider will not technically prevent simultaneously access to an account beforehand [1], but to allow and detect such concurrent usage in order to deactivate the account afterwards, which is also an important mechanism of SPIES to guarantee that an authorized user can never sell her account to more than n other peoples so as to make profit. Some troubles may occur in this case, for instance, how about an honest consumer forgot to log out her laptop in home, and then go to her office to open another desktop and log in again with the same account?

Secondly, SPIES shifts some potential *unexpectable* risks of secret (password) disclosures to the users, such as new virus, OS or software security bugs, and even inside leaks of the provider. In any above case, the user will risk an additional big loss of her deposit, which usually exceeds the normal price of the service itself. This punishment is too strict and may bring about some legal troubles to distinguish the responsibilities. As a remedy, in (Margolin et al., 2004), it suggests that the provider could give the consumer one day or more to report a stolen password. However, it is still too strict to require each normal user (not computer expert) has an ability to detect such security intrusions in time. In contrast, a more reasonable case may be that, even the password has been stolen due to the user's personal improper protections (e.g., not updating security packages in time), the user may accept to lose at most the cost of the service itself (i.e., could not enjoy the service anymore),

[1] In contrast, most current online subscription services just simply kick the first user out automatically if a second user logs in using the same account, or prohibit repeated log in if a user is using the account.

while not the relatively big deposit.

In addition, to address a version of the prisoner's dilemma, SPIES has been restricted to situations with only a single authorized consumer beyond the secret provider. Therefore, SPIES has to introduce a charity (the fourth party) in addition to the escrow service to spare some money of the deposit in case the consumer shares her password to others. The problem is that, the charity can take essentially all of the money in escrow if she get the content or otherwise spoof registration. This is a limitation of SPIES as acknowledged in (Margolin et al., 2004).

In short, SPIES may applicable to important and highly valuable secrets such as military and (sensitive) commercial ones, in which extra serious punishment (deposit) should be introduced in order to stimulate the possessors to protect the secrets as best as they can. However, with respect to current online subscription services which usually cost only around 10$ per month, it is doubtful how many consumers would like to bear such risks in addition to potential legal problems and arguments.

Focused on the above problems of SPIES, we propose to use a kind of *lottery* instead of deposit to encourage the consumer to keep the secret private. Our protocol, IBSPS, can *transform* some burden of secret protection of the provider into the *benefit* of the consumer, thus it provides a positive rather than negative incentive for the consumer to not share the secret. In IBSPS, we propose a novel duplication function to reward honest consumers who keep their secrets, in which the reward is shifted from the punishment of the dishonest ones who share their secrets. There is no need to introduce a fourth party such as the charity in SPIES, and thus the corresponding potential risks can be avoided. Another advantage of our proposed method is that, even in the worst case that an honest consumer lost her password unintentionally, she will only lose some possibility to win the lottery rather than a big deposit as in SPIES, which should be more reasonable and comfortable for her to enjoy the service. A detailed analysis of IBSPS is presented in Section 2.

Some other related works can be found in (Horne et al., 2001) and (Golle et al., 2001). Both of them focus on how to provide incentives for sharing legitimate content among authorized users in peer-to-peer networks: Horne et al. (Horne et al., 2001) propose a system architecture which integrates a P2P file sharing service with an escrow service that reliably pays the party that is serving up the content; while Golle et al. (Golle et al., 2001) construct a formal game theoretic model of P2P file sharing so as to solve the free-rider problem. Our work is different with these works since we focus on providing economic incentives for *keeping* secrets private rather than sharing, though escrow service is also used in our protocol.

Currently, a number of techniques and systems have been proposed to handle digital rights management, such as Microsoft Windows Media DRM system (Microsoft, 2004), IBM xCP cluster protocol (IBM, 2001), OMA (Open Mobile Alliance) DRM (OMA, 2005), and InterTrust NEMO (Networked Environment for Media Orchestration) framework (Bradley and Maher, 2004). Unlike these DRM systems, IBSPS does not focus on providing technical solutions to prevent illegal copying and transferring the protected content beyond authorized domains or devices, but to provide an economic incentive to keep the (accessing) secret private and so as to prevent illegal sharing of the content. IBSPS can be used as a complement with current DRM systems, for instance, a domain certificate of an authorized domain can be regarded as a secret in IBSPS, and thus the domain owner would not like to add her friends' machines into the domain so as to share the content files. A potential social significance of IBSPS is that it can encourage the users to foster a good custom instead of legally questionable behavior in DRM applications.

1.2 Overview

The rest of this paper is organized as follows. Section 2 presents a basic scheme of incentives-based secrets protection system (IBSPS). Section 3 discusses two strategies for the provider to set the prize of lottery, and analyzes the total utilities of the provider under the strategies. At last, some further discussions and concluding remarks are presented in Section 4.

2 BASIC SCHEME OF IBSPS

Informally speaking, IBSPS can be understood as a kind of lottery to stimulate the consumers to keep their secrets private, and it can be briefly divided into the following three phases:

1. During the *Subscription* phase, the consumer subscribes the service and receives a secret (an account and password pair, or a password for short in the following discussions) that allows access to the protected service or content. The provider also registers the password to an escrow service and places an amount of money (prize) into the escrow account.
2. During the *Registration* phase anyone who has a copy of the password can register to the escrow service, by providing proof of knowledge of the password.
3. During the *Lottery* phase anyone who provided proof in the registration phase are given a chance to win the prize in the escrow, i.e., a kind of lottery.

For clarity, we limit the basic model of IBSPS to the following situations: the provider offers online subscription services of streaming digital content, and supports period pricing systems such as monthly and yearly subscriptions (pay-per-use is not considered because generally the one-off password or access needs not to be protected). Concurrent usage of a password is technically prohibited, while there is no restriction on the portability of the consumer, i.e., she can enjoy the streaming content with the password on any computers she possess or like.

And to state the model more formally, we define the parties and variables used in IBSPS as shown in Table 1. We denote the exchange of x dollars as $\$(x)$. The formal details of IBSPS are as follows.

Table 1: Variables used in IBSPS.

Variable	*Description*
P	The service provider
$C_1 \ldots C_m$	Authorized consumers
E	A trusted escrow service
$U_1 \ldots U_n$	Unauthorized consumers
B	The total prize set for lottery
$T\{B\}$	The lottery contract signed by P
ϕ_{C_i}	The secret to C_i $(i = 1, \ldots, m)$
$d(\phi_{C_i})$	The textual description of ϕ_{C_i}
$H(\phi_{C_i})$	The hash of ϕ_{C_i}
τ	End time of secret protection
v	The price of the service (secret)
$hC_1 \ldots hC_x$	Honest registrants
$dC_1 \ldots dC_y$	Dishonest registrants

Phase 1: Subscription. Firstly, the provider P places $\$(B)$ as a prize (bonus) into a trusted escrow service E (alternatively, $\$(B)$ can be replaced with a notarized contract $T\{B\}$ signed by P, since the amount of B can be defined as a function of the total number of authorized consumers and the price of the secret, and we will further discuss this issue in Section 3). Secondly, P sends a list of hash values and descriptions of the secrets as well as the ending time to E, denoted by $d(\phi_{C_i})$, $H(\phi_{C_i})$ $(i = 1, \ldots, m)$, and τ, respectively [2]. The hash value will serve as a proof of possession of ϕ_{C_i} without revealing the secret to the escrow service. After that, the consumers $C_1 \ldots C_m$ can subscribe the service by paying the price of the service $\$(v)$ to P, and then receive the secrets $\phi_{C_i} (i = 1, \ldots, m)$, respectively. This can be done in a fare exchange manner such as described in (Bao et al., 1998; Zhou et al., 2004), but here we do not require a specific mechanism since it is not the main focus of IBSPS.

Therefore, phase 1 can be concluded as follows (shown in Figure 1):

$$\begin{aligned} P \to E &: \$(B) \qquad (1) \\ P \to E &: d(\phi_{C_i}), H(\phi_{C_i}), \tau \ (i = 1, \ldots, m)(2) \\ C_i \to P &: \$(v) \qquad (3) \\ P \to C_i &: \phi_{C_i} \qquad (4) \end{aligned}$$

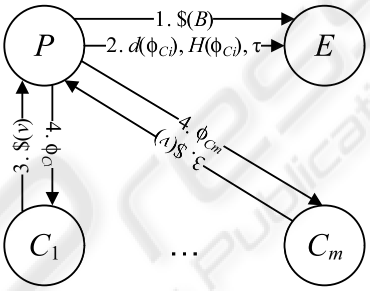

Figure 1: Phase 1: Subscription.

Phase 2: Registration At this stage, E broadcasts widely that it is seeking *anonymous* registrations from anyone holding secrets described by $d(\phi_{C_i})$ $(i = 1, \ldots, m)$. Such message can also be posted on the homepages of P and E, or as a complementary clause of the terms of service of P, so as to let it be known as wide as possible.

There are two key points here. One is that unauthorized consumers $U_1 \ldots U_n$ who obtain (share or buy) the secrets from C_i $(i = 1, \ldots, m)$ rather than P, can also participate this protocol (lottery). The other is the *anonymity* of the registration, which can stimulates the unauthorized consumers to register without revealing their identities and losing the friendship if they got the passwords by their friend's kindness. This can be implemented by using anonymous email address or other mechanisms, so that the escrow E can conform the registrations and contact with the (unauthorized) consumers (if they win the lottery) without knowing their identities.

The registration can be done by sending the hash value and description of ϕ_{C_i} $(i = 1, \ldots, m)$ to E, i.e., $H(\phi_{C_i})$ and $d(\phi_{C_i})$. For clarity, we suppose that $U_1 \ldots U_n$ get the same ϕ_{C_k} $(1 \leq k \leq m)$ from a specific authorized consumer C_k, and $C_1, \ldots, C_m$ and $U_1, \ldots U_n$ all have registered, the process is shown in

[2] For clarity, we suppose that this group of ϕ_{C_i} have the same protection time τ, e.g., a group of consumers who subscribe the service in the same period of time (day or month).

Figure 2 and described as follows :

$$\begin{aligned} C_1 \rightarrow E &: \; d(\phi_{C_1}), H(\phi_{C_1}) && (5) \\ &\vdots \\ C_m \rightarrow E &: \; d(\phi_{C_m}), H(\phi_{C_m}) \\ U_1 \rightarrow E &: \; d(\phi_{C_k}), H(\phi_{C_k}) \; (1 \leq k \leq m) && (6) \\ &\vdots \\ U_n \rightarrow E &: \; d(\phi_{C_k}), H(\phi_{C_k}) \end{aligned}$$

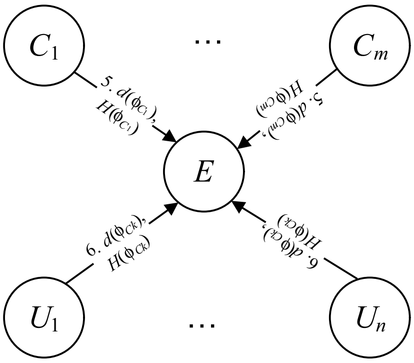

Figure 2: Phase 2: Registration.

Phase 3: Lottery. The last step, beginning at the end time of τ, is the lottery process. Each registrant will have a chance to win the prize $\$(B)$ set by P. If no password has been shared or sold, i.e., only authorized consumers have registered in Phase 2, then each C_i $(i = 1, \ldots, m)$ has an average possibility of $1/m$ to win the prize. If a consumer, say C_k $(1 \leq k \leq m)$, shares her secret to some unauthorized consumers $U_1, \ldots U_n$, the system must guarantee the following two properties:

- First, any other *honest* consumers who do not share their password, say, C_j $(j = 1, \ldots, m \wedge j \neq k)$, will not get a lower possibility than $1/m$, otherwise they also pay for the dishonest behaviour done by C_k, which is unfair for these honest consumers. In contrast, the system should reward these honest consumers in case dishonest C_k shared her password.
- Second, C_k must receive a punishment for her dishonest behaviour, i.e., a much lower possibility than $1/m$ to win the prize. Moreover, the system should also prevent any kinds of collusion and multiple registrations, such as C_k colludes with $U_1, \ldots U_n$, or she registers more than one times to get a totally higher possibility than $1/m$.

Recall that in Phase 2, E receives anonymous registrations with only $d(\phi_{C_i})$ and $H(\phi_{C_i})$ $(i = 1, \ldots, m)$, and thus it is difficult for E to distinguish who are authorized or unauthorized consumers. However, it is trivially *easy* for E to detect password sharing and multiple registrations with the same hash values and descriptions. Therefore, a novel duplication function can be proposed to solve the above two problems.

Suppose E classifies all the registrations into two categories: one is the *honest* registrations using distinct hash values, the other is the *dishonest* ones that registered with repeated hash values. We represent the number of the former (honest ones) as x, and the latter (dishonest ones) as y. And it is easy to see that $x \leq m$, $(y \geq n) \wedge (n = 0 \rightarrow y = 0) \wedge (n \geq 1 \rightarrow y \geq 2)$, and $x + y = m + n$ (the meanings of the parameters m, n, x, and y are listed in Table 2).

Table 2: Parameters used in IBSPS.

Par.	*Description*
m	The total number of authorized registrants
n	The total number of unauthorized registrants
x	The total number of honest registrants
y	The total number of dishonest registrants

Then the problem is that how to guarantee that a dishonest consumer will get a much lower possibility to win the prize even she registers y $(y \geq 2)$ times, or shares her secret with $(y - 1)$ friends and all of them (including herself) submit their registrations (a kind of collusion with the same result of multiple registration). And at the same time, to ensure that the honest registrants will receive a higher rather than lower possibility in case dishonest registrations happened, E can use a duplication function, say $f(y)$, to clone $(f(y) - 1)$ copies for each honest registration.

Therefore, each honest registrant will get a higher possibility of $\frac{f(y)}{x \cdot f(y) + y}$, while the dishonest registrant will get at most $\frac{y}{x \cdot f(y) + y}$ possibility to win the prize. The key then is to ensure that $f(y) > y$, and there are many available functions satisfying the condition. Here, to punish the dishonest behaviour and award the honest registrants more notably, we recommend to choose an exponential duplication function as follows:

Function 2.1 (Duplication Function)

$$f(y) = \rho^y \qquad (\rho \geq 2)$$

Then, it is straightforward to prove that the following important properties hold in IBSPS (given $x \leq m$, $(y \geq n) \wedge (n \geq 1 \rightarrow y \geq 2) \wedge (n = 0 \rightarrow y = 0)$, $x + y = m + n$, and $\rho \geq 2$):

- $\frac{1}{x \cdot \rho^y + y} < \frac{1}{m}$, sharing secret will lose some possibility.

- $\frac{y}{x\cdot\rho^y+y} < \frac{1}{m} < \frac{\rho^y}{x\cdot\rho^y+y}$, multiple registrations or collusion will still get a lower possibility, while the honest registrants will be rewarded a higher possibility.
- $\frac{y}{x\cdot\rho^y+y} + \frac{x\cdot\rho^y}{x\cdot\rho^y+y} = 1$, the total possibility is equal to 1.

The Phase 3 can be concluded as follows (shown in Figure 3), where we use $hC_1 \ldots hC_x$ to denote the honest registrants, $dC_1 \ldots dC_y$ to denote the dishonest registrants, and dashed (disconnected) arrows to represent the expectation values in the lottery, i.e., the value of the possibility multiplying the prize $\$(B)$.

$$\begin{aligned}
E \dashrightarrow hC_1 &: \frac{\rho^y\cdot\$(B)}{x\cdot\rho^y+y} && (7)\\
&\vdots\\
E \dashrightarrow hC_x &: \frac{\rho^y\cdot\$(B)}{x\cdot\rho^y+y}\\
E \dashrightarrow dC_1 &: \frac{\$(B)}{x\cdot\rho^y+y}\\
&\vdots\\
E \dashrightarrow dC_y &: \frac{\$(B)}{x\cdot\rho^y+y}
\end{aligned}$$

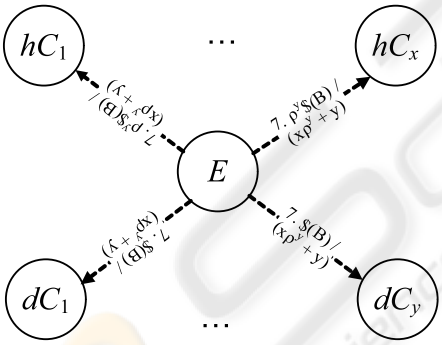

Figure 3: Phase 3: Lottery.

To illustrate the above mechanism in a more clear and intuitive way, we use a simple example as follows. Suppose there are 3 authorized consumers (i.e., $m = 3$), and one of them, say Alice, shares her password to a friend, Bob. All of them register exactly one time to the escrow. Therefore, E will receive 2 honest as well as 2 dishonest registrations (i.e., $x = 2, y = 2$) instead of 3 honest ones. In this case, Alice will get a possibility of $1/10$ to win the prize (suppose $\rho = 2$). In contrast, if she keeps the password private, she can get a higher potability of $1/3$! With respect to Bob, he has an incentive (the same possibility of $1/10$ as Alice) to participate the lottery especially since the registration and lottery are done in an anonymous way. Even Alice colludes with Bob (the same case as if Alice registers twice), they still will get a totally lower possibility of $1/5$ than the rest two honest guys, who will get an increased average possibility of $2/5$ thanks to their sharing.

3 STRATEGIES FOR SETTING PRIZE

As discussed in Section 2, instead of putting an amount of real money $\$(B)$ into E, the provider P can sign and send a *notarized* lottery contract $T(B)$ to E as an alternative. This is because that the amount of $\$(B)$ can usually be defined as a function of the total number of authorized participants m and the price of the secret v (suppose that $\phi_{C1}, \ldots, \phi_{C_m}$ have the same price), and the real money can also be substituted by some other means, such as a free service extension for one or several next periods of τ.

Therefore, we first define a linear prize function as follows:

Function 3.1 (Linear Prize Function)

$$B = \lambda \cdot mv$$

where λ is an coefficient ranging between $(0, 1)$.

As shown in Function 3.1, given the price v, B is defined as a linear increasing function of the total number of authorized registrants m. That is to say, when there are more authorized consumers participating in the lottery, the prize is increasing bigger correspondingly, while the possibility to win the prize is decreasing at the same time. This strategy is welcome to risk seeking consumers who want to get a big prize (e.g., the chance to win one year or longer free access). However, with respect to risk neutral or aversion consumers who prefer a more predictable while relatively lower outcome, another fixed prize function can be defined as follows:

Function 3.2 (Fixed Prize Function)

$$B_f = \lambda \cdot \alpha v$$

where B_f is a fixed amount of prize with respect to each α authorized registrants, and α is a constant. Generally, $1/\lambda \le \alpha \le m$ and $m/\alpha \cdot B_f = B$.

A simple example of Function 3.2 is that, suppose $\lambda = 0.1$ and $\alpha = 1/\lambda = 10$, then for every 10 authorized registrants (suppose they are all honest and do not share their secrets with others), each of them will have a relatively high possibility of $1/10$ to win the prize which is equal to their cost v. In other words, everyone has 10% possibility to enjoy a free access in the next service period.

A "problem" is that the provider P has to pay for the prize, which seems to be a disincentive for P to adopt IBSPS. However, as shown in Function 3.1 and 3.2, if P regards the coefficient λ as a kind of *discount* to encourage the consumers to not share the passwords, P will finally make profit in IBSPS by getting more honest and authorized consumers in return.

For instance, suppose that $\lambda = 0.1$ and $m = 10$, then the provider will simply get more revenue back if more than *one* unauthorized users are forced to subscribe the service legally (because all the authorized consumers would not like to share their passwords by IBSPS), even P has to pay the prize (discount) totally equal to $\$(v)$. The point is that, the provider need only to set λ greater than the estimated rate of unauthorized (shared) consumers, i.e., n/m, so as to make profit in IBSPS.

Moreover, a more tricky strategy for P is to enhance the price at λ, i.e., shifting the cost of prize to each consumer. In this case P will risk nothing since the consumers share the cost of prize by themselves. It is tricky because P can intentionally conceal such details from the consumers (a kind of cheating while widely used in practice).

4 ANALYSES AND CONCLUSIONS

IBSPS is the first work, to our best knowledge, that provides a *positive* incentive for authorized consumers to keep their secrets private rather than to share among friends, which seems to be an open problem by current technical solutions and legal measures.

To our understanding, a positive incentive is better and more popular than a negative one such as the deposit in SPIES (Margolin et al., 2004). This is because with regard to relatively lower sensitive secrets such as the subscription passwords of DRM-based applications, the positive incentive can efficiently *encourage* rather than *threaten* the consumer to protect the secret in a more acceptable way.

Generally, it is too strict to require every (normal) consumer has the ability to detect and prevent any kind of security threatens in time, and it is also difficult to identify the responsibility of password stolen in some complex cases such as caused by virus, security bugs, and inside leaks. Therefore, we cannot put all the responsibilities and risks of password protection on the consumer, which is exactly the main concern and standpoint of IBSPS.

Therefore, compared with the negative incentive methods such as SPIES (Margolin et al., 2004), IBSPS has the following advantages:

- Firstly, unlike SPIES that *shifts* the burden on password protecting directly to the consumers by requiring a relatively big deposit, IBSPS novelly *transforms* such burden into the *benefits* of the consumers, i.e, an extra prize provided by the provider. Thus, IBSPS can encourage the consumers to not share the passwords by their own interests in a more acceptable way.
- Correspondingly, in IBSPS, even in the worst case that a password was stolen due to some unexpected hardware, software, or other management problems, an honest consumer will lose at most some possibility to win the extra prize in addition to the password itself, while need not to endure the potential risk of losing the big deposit as in SPIES. This mechanism is more user-oriented and reasonable compared with SPIES.
- The duplication function in IBSPS can novelly and effectively reward the honest registrants by punishing the dishonest ones, thus it avoids to introduce a charity (fourth party) to share the prize as in SPIES. Consequently, some potential risks caused by the introduction of the charity can also be avoided.

A potential social significance of IBSPS is that, by using IBSPS, the consumers will gradually break away from illegal sharing and foster a good custom to keep their secrets private in DRM applications. And from the point of view of the provider, she is also happy to see that every consumer is honest and authorized, and thus more revenue can be gained in return. The only problem and cost for the provider may be the prize, however, as analyzed in Section 3, such minor cost is worthy to pay as long as there are still some unauthorized (illegal) users who are using the shared passwords. Therefore, IBSPS can be regarded as a kind of win-win game for both the provider and consumers.

It should be figured out that IBSPS may not work in case that simultaneously accessing to a password is not technically prohibited. In this case, a user can share the password with others without giving up any her own utility of the password. This is rather a technical problem of the DRM system than a limitation of IBSPS. However, even in this case IBSPS may still work to some extent if the user does not want to lose her luck to win a big bonus.

Another special case is that, if sharing both the cost and password usage time is a more cost-effective strategy for somebody regardless of the prize, then IBSPS may also fail. However, again, we think this is a pricing problem rather than a limitation of IBSPS, which discloses that there are some users who are not satisfied with the current pricing systems, and thus it is the provider's responsibility to provide more reasonable and flexible pricing and payment methods for those unsatisfied users.

As mentioned in Section 3, a crucial issue of IBSPS is, how much benefit the content provider should invest in order to protect its contents. Evidently, it does not make sense to put more than what would be lost through revenue losses caused by dishonest consumers sharing the contents illegally. More critical study on this issue should be carried out, although we have discussed two simple strategies for the content provider in this article (Section 3).

In this paper, we limit IBSPS to the protection of the secrets such as accounts and passwords in digital subscription services, and we do not extend the analysis directly to the protecting of digital content itself (i.e., purchased music or movie files). This is because so far we found that, unlike password, it is difficult to define the end time of protection of the content. Moreover, content protecting is a topic more related to illegal copying than sharing, though there are some common properties and problems between them. Further studies should be done on this topic, and this is also one of our future works.

As mentioned in Section 1.1, in addition to password and account protection, IBSPS can also be used as an additional layer with some existing DRM techniques and systems to prevent illegal content sharing and distribution. Some other possible applications, such as protecting the domain certificate of authorized domain, are also our future directions.

ACKNOWLEDGEMENTS

This research is supported by 21st COE (Center of Excellence) Program “Verifiable and Evolvable e-Society” of JAIST, a funds by Ministry of Education, Culture, Sports, Science and Technology (MEXT, Japan). It is also conducted as a program for the ”Fostering Talent in Emergent Research Fields” in Special Coordination Funds for Promoting Science and Technology by MEXT of Japan.

REFERENCES

Bao, F., Deng, R. H., and Mao, W. (1998). Efficient and practical fair exchange protocols with off-line ttp. In *1998 IEEE Symposium on Security and Privacy*, pages 77–85, Oakland, CA. IEEE Computer Society.

Bradley, W. B. and Maher, D. P. (2004). The NEMO P2P service orchestration framework. In *Proceedings of The 37th Annual Hawaii International Conference on System Sciences (HICSS-37)*. IEEE.

EC (2002). Digital rights: Background, systems, assessment. European Commission Staff Working Paper. Brussels, 14.02.2002, SEC(2002) 197.

Golle, P., Leyton-Brown, K., Mironov, I., and Lillibrdge, M. (2001). Incentives for sharing in peer-to-peer networks. In *EC’01, 3rd ACM Conference on Electronic Commerce*, pages 264–267, Tampa, Florida, USA. ACM Press New York, NY, USA.

Horne, B., Pinkas, B., and Sander, T. (2001). Escrow services and incentives in peer-to-peer networks. In *EC’01, 3rd ACM conference on Electronic Commerce*, pages 85–94, Tampa, Florida, USA. ACM Press New York, NY, USA.

IBM (2001). IBM response to DVB-CPT call for proposals for content protection & copy management: xCP cluster protocal. Technical report.

Margolin, N. B., Wright, M. K., and Levine, B. N. (2004). Analysis of an incentive-based secrets protection system. In *DRM’04, 4th Internation Workshop on Digital Rights Management*, pages 22–30, Washing, DC, USA. ACM.

Microsoft (2004). A technicall overview of Windows Media DRM 10 for devices. Technical report, Microsoft Corporation.

Mulligan, D. K., Han, J., and Burstein, A. J. (2003). How DRM-based content delivery systems disrupt expectations of “personal use”. In *DRM’03, 3rd International Workshop on Digital Rights Management*, pages 77–89, Washington DC, USA. ACM.

MusicAlly (2005). Napster users sharing passwords to save cash. http://www.theregister.co.uk/2005/04/08/napster_password_sharing/.

OMA (2005). OMA DRM V2.0 Candidate Enabler. http://www.openmobilealliance.org/release_program/drm_v2_0.html.

Zhou, Y.-B., Zhang, Z.-F., Qing, S.-H., and Liu, J. (2004). A new cembs based on rsa signatures and its application in constructing fair exchange protocol. In *EEE’04, 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service*, pages 1–5. IEEE Computer Society.